European Cyber Security Perspectives 2020

kpn

National Cyber Security Centre
Ministry of Justice and Security

Deloitte.

pwc

IDQ

accenture

ANALYZEDATA

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

TNO

Universiteit Leiden
Governance and Global Affairs

Radboud University

TREND MICRO
Securing Your Connected World

paloalto NETWORKS

Xebia Security

NLNETLABS

VU VRIJE UNIVERSITEIT AMSTERDAM

Preface

Dear reader,

This is the moment to look back at 2019 and overthink what happened in the last months in the dynamic world of cyber security. What kind of huge incidents or data leaks reached the front of the newspapers? Interesting researches. New risks or technologies impacting our landscape? Or were there any important changes in legislation that is influencing cyber security policy.

We tend to look at examples that have a direct effect on our business or happened to similar companies close by. But since we live in an interconnected and fully digital world it is just as interesting to see what is happening in a completely different environment or other region in the world.

New Orleans declared a state of emergency after a cyber-attack forced a shutdown of all the city governments computers. Staff had to resort to pen and paper as they tried to keep the services in the city running. This is a warning to other governments and companies of what might happen if you do not invest continuously in the security of your company or even country. It also makes clear that there's no alternative anymore for our digital way of working.

On a geopolitical level we see a large increase in, what can be called, a digital warfare. Instead of real bombs, in some cases cyber-attacks were used to hit infra structures in a country. Which shows that, as many experts predicted, offensive cyberattacks have become part of the arms arsenal of nation states and investing in cyber defence has become paramount to defend from state supported attacks.

Closer to home a ransomware attack caused a problem for the University of Maastricht which made them to postpone exams because students could not reach the university portals during the Christmas break. Presumably the University paid their attackers a considerate amount. Which of course started a discussion around the business model of the cyber attackers and the change of focus they have on gaining for bigger targets. In parallel to this incident it becomes more and more clear that we really need to join forces to create a serious defence against cyber criminals. Of course supported by a close partnership between public and commercial parties.

This year's edition holds four articles on Quantum research and we see an increasing support for these researches from companies and governments in the Netherlands and Europe.

We would like to thank all authors who have contributed to the 7th edition of the European Cyber Security Perspectives.

Enjoy reading and wish you a secure 2020!

On behalf of KPN,

Paul Slootmaker
Chief Information Security Officer

Marcel van Oirschot
Executive Vice President Security

Colofon

European Cyber Security Perspectives 2020

Volume 7

KPN CISO
Teleportboulevard 121
1043 EJ Amsterdam

Chief Information Security Officer:
Paul Slootmaker

Editor:
Karin van der Wekke

Contributors:
Nathalie Lokhorst
Carolien Hoogerwaard

Special thanks:
Desislav Dyakov
Stef van Dop

Master decryption key released for FilesLocker ransomware

European Union announces bug bounty program

Hackers are taking over Chromecasts to promote PewDiePie's channel

Quotes contributing partners

Paul Slootmaker

Chief Information Security Officer, KPN

You should not ask yourself if you will be hacked, but how you will respond! Every organisation, public or private, should be response-ready when an incident does occur.
The only way to do this is by continuously testing and exercising your defense and response capabilities.
With your security team, throughout your organisation and together with your partners.

Hans de Vries

Head of the Dutch National Cyber Security Centre (NCSC)

Should we still invest in email? Absolutely! Protecting your email connections ensures that confidential information does not fall into the wrong hands. In the Netherlands, we strongly believe in using open internet standards like STARTTLS and DANE to do this. The National Cyber Security Centre (NCSC) promotes the adoption of these standards by publishing factsheets and by being in close contact with several large vendors of email server software. We are proud of the adoption rates of DANE we already see in the Netherlands. But of course we strive for more, until we have a near-ubiquitous use of DANE!

Niels van Vorle

Partner Cyber Risk Services Deloitte

As we transition to a truly digital society, a risk-based cyber security mindset must become second nature to all of us. The world around us is changing in an ever growing pace and requires us to adjust accordingly. More than ever, we need to have long-term thinking and anticipate future threats, trying to assess related business risks. Some have the perception that we have time and can wait until threats become clearer. However, in many cases the time required for designing and implementing mitigations is so long that starting tomorrow might already be too late. So let's get cracking!

Grégoire Ribordy

CEO ID Quantique

The adoption of quantum cryptography solutions by service providers is essential to secure their network and their customer data for the coming decade.

Floris van den Dool

Senior Security Executive at Accenture Security

To maintain a power balance between the defenders and cybercrime, we (the defenders) need to start out-innovating the adversary and increase our collaboration.

Gerwin Naber

Partner Cyber, Forensics and Privacy, PWC

It is impossible to imagine a day in our lives without the world wide web. The devoted role of the web is continuously evolving, but comes with significant perils, also for society. Emerging technologies and rapid developing regulations are drivers to come to a new equilibrium between global connectivity, state sovereignty and our individual privacy. The previous year has shown significant new cyber security perspectives with societal impact. Where will this take us and our internet next?

Josh Mengerink

CTO AnalyzeData

Imagine if a shopkeeper would secure their shop in the same way that software systems are secured. They would bar their windows, so nobody enters in an unintended way, put a camera on their back door to monitor access attempts by unauthorized personnel. But, as soon as a customer is inside their shop, they assume that everything is fine. This does not seem like a good idea, so why is this still acceptable in so many (cloud) software systems? A vast majority of digital fraud happens after application authentication has already occurred, so monitoring user behavior inside your application is vital!"

Prof. Dr. Tanja Lange

Scientific Director Ei/PSI and Professor Cryptology Eindhoven University of Technology

While large scalable quantum computers are at least a decade away, it is high time to prepare our systems: find out where cryptography is used, what it is used for, and how to replace it with alternatives that will not get broken by quantum computers.

TNO

Linda Krom

Corporate Security Officer, TNO

People need to develop an instinct for what they can and cannot trust in the digital world, just like they do in the real world. As cyber security measures become more advanced, cyber criminals seem to increasingly rely on social engineering or other vectors that aim to exploit human weaknesses. Knowledge and awareness of cyber criminality on the side of users of the digital world is important, but are only useful if users are motivated to use this knowledge in their day-to-day life. At the same time, we cannot expect users to be on guard all the time. This is why we should help people develop and maintain a sound instinct to judge what is trustworthy.

Prof. dr. Bibi van den Berg

Professor Cybersecurity Governance at the Institute of Security and Global Affairs (ISGA), Leiden University, the Netherlands.

Cyber security is often seen as a threat to systems; the IT-infrastructure on which so much of society has been built. As a result, all effort has been devoted to protecting and defending networks against DDoS attacks, hacks and different forms of malware. Fake News and dis- or misinformation, however, relate to content and not to systems. As witnessed during the 2016 U.S. Presidential elections, this threatens ideas and values, not just systems and services. The new challenge for governments and businesses will be to ensure security for the content layer of cyberspace.

January

4

Hackers leak personal data from hundreds of german politicians on Twitter

9

New tool automates phishing attacks that bypass 2FA

Bart Jacobs

Professor Interdisciplinary Hub for Security, Privacy and Data Governance Radboud University

The starting point of almost every security solution is proper authentication.

Rik Ferguson

Vice President Security Research, Trend Micro

The defining challenge facing security operations teams over the coming decade is how to handle data. The preceding decade has been spent in building out the technology stack, the architecture, and the digital infrastructure of the security function in an organisation. We, as an industry, are now faced with the realisation that we don't have the pipeline of motivated individuals entering the cybersecurity workforce, capable of putting their fingers to the keys that configure, control and monitor the solutions we have built, and many well-intentioned initiatives are already underway to address this, quite rightly. An underlying issue though is waiting to rear its head, "What do we do with all the data that these technologies and their operators are generating?" No amount of hiring will mitigate that problem. Without automated event correlation and analysis, the skills problem ceases to be a crisis. It becomes a lifestyle.

Nikesh Arora

CEO Palo Alto Networks

The world is changing into a multi-cloud hybrid world within the next few years and security needs to keep up.

Andrew de la Haije

CEO Xebia Netherlands

Although securing the Software Development Lifecycle (SDLC) is common sense nowadays, it is still often based on classical approaches. This naturally creates security tollgates that slow down development and product release. The next challenge is making security scalable in modern environments. At Xebia, we truly believe that investing in secure coding, automation and a security culture throughout the company, contributes to the overall security posture of your organisation. We focus on creating the right amount of security for your company and products without sacrificing speed.

Benno Overeinder

Managing Director NLnet Labs

With our dependence on a reliable Internet, usable security is of the utmost importance, and I am certainly not the first to mention this. A few recent incidents have shown that our Internet infrastructure is vulnerable, while implementation and deployment of current standards would have prevented the incidents to happen. Open source implementations of open standards to secure our Internet infrastructure have been available for several years, but deployment is lagging behind. With the high-visibility incidents and availability of easy-to-use software to secure our Internet infrastructure, incentives are better aligned along the cost-benefit dimension.

Dr. Marleen Weulen Kranenbarg

Assistant Professor Criminology Vrije Universiteit Amsterdam

In addition to technical solutions, it is important to consider the human factor in cybercrime and cybersecurity. By addressing issues related to human behavior in the digital environment, we can further enhance cybersecurity. Perspectives from social sciences, such as criminology, can shed light on offender characteristics and strategies, and provide ways to stimulate potential victims to take security measures.

Contents

January

10

Reddit locks out users
with poor password
hygiene after spotting
'unusual activity'

Global DNS hijacking
campaign: DNS record
manipulation at scale

Ask your email provider to secure your email connections with DANE

Are you still sending your organisation's secrets unprotected across the internet?

Sanne Kamerling, NCSC-NL

Email is the technology of the future

Email is here to stay. Even though many alternatives have been proposed and implemented in the past decades, email is still extremely popular. Especially in a corporate context, it is hard to imagine getting any work done without your trusted inbox.

Email is worthy of protection, and worthy of your investments. Even if your private use of email has fallen over the past five years, chances are your business will keep depending on email for years to come. Your organisation's users exchange a wide array of sensitive information via email, ranging from intellectual property and strategic information to personally identifying information (PII).

Email functionality is both crucially important and remarkably uniform across deployments. Therefore, many organisations choose to outsource it to a specialized provider. Their expertise and advantages of scale lead to a more cost-effective and secure setup than most organisations could achieve on-premise.

Eavesdropping is easy when your email provider doesn't protect their connections

Most connections to and from email providers can easily be eavesdropped upon. If an email provider sends your email to the email provider of another organisation, an attacker may read the email in transit anywhere between the two providers.
You may be entrusting your organisation's secrets to be safe in email, but the underlying protocol was never designed to secure such sensitive information. The protocol for email traffic, SMTP, dates back to 1982. Essentially, sending email today still works the same way it did in 1982. Today's threats are much more advanced and numerous than in 1982. It's hardly surprising that such an old protocol is not able to protect against them.

Some measures are available to mitigate this situation. Many email providers use STARTTLS to protect their connections to other providers. However, by itself STARTTLS is not an effective measure to counteract eavesdropping. An attacker who is willing to interfere with the connection can still read all emails that are

TA505 Crime gang debuts brand-new servhelper backdoor

January

11 Over 202 million Chinese job seekers' details exposed on the internet

13 Hacker had access to unknown number of Outlook.com accounts

sent over that connection. This is not just a theoretical risk. In 2015, researchers demonstrated that the STARTTLS protection to Google is stripped from more than twenty percent of all emails in seven countries. In certain cases, this percentage reached almost one hundred percent[1]. These emails were therefore sent unprotected across the internet.

End-to-end email encryption with S/MIME or OpenPGP is another measure that is sometimes used. While effective in theory, using these systems proves cumbersome and error-prone in practice. Most users do not bother with them at all, and even expert users only use them occasionally. Any real solution to the problem of email eavesdropping should therefore be transparent to users, in order to ensure that most if not all emails will be sent through protected connections.

Email security is about more than just protecting the connections to- and from your email provider. Two-factor authentication, spoofing protection and antivirus all protect against different threats. However, none of these other measures are of any help when your email is plucked from the wire by an eavesdropping criminal organisation or foreign intelligence agency.

Ask your email provider to protect all its connections with STARTTLS and DANE

The NCSC-NL recommends that you ask your email provider to secure all their connections with STARTTLS and DANE. DANE is an internet standard that, combined with STARTTLS, prevents stripping attacks. If two email providers both use STARTTLS and DANE, an attacker cannot intercept email that is being send between these providers.

Online tests are available to check whether your email provider already protects their connections with STARTTLS and DANE. For full protection, your email provider needs to protect both incoming and outgoing connections. The email test on internet.nl[2] checks whether your provider supports secure incoming connections for your email. The test on HaveDane[3] checks whether your provider supports secure outgoing connections.

Implementing DANE in addition to STARTTLS is relatively cheap. Your email provider needs to publish some information about the way it has secured its incoming connections. For outgoing connections, it needs to modify its servers in order to the information that other email providers have published about the protection on their incoming connections.

There are some hurdles that your email provider may experience when implementing DANE and STARTTLS. For incoming connections, protection with DANE depends on the use of DNSSEC, another security technology. Support for DNSSEC should be considered a hygiene factor, but unfortunately not all email providers have currently implemented it yet. For outgoing connections, the email server software that your email provider uses, needs to support DANE. While the number of email server software vendors that support DANE is growing, support is by no means ubiquitous. We encourage your email provider to contact their vendor if they do not support DANE yet.

DANE is a relatively new standard, and the email ecosystem is slow to move. That is the primary reason the adoption of this standard has not skyrocketed yet. On the other hand, DANE is a mature technology that many organisations already use in production and at scale. For example, it is compulsory for all Dutch government bodies to apply DANE when investing in email systems[4]. DANE's benefits are available to any organisation that takes the trouble to implement it.

What does NCSC-NL do to further the adoption of DANE?

The NCSC-NL published their advice on implementing STARTTLS and DANE in a factsheet[5]. The advice in this factsheet is aimed at people in a technical role with regard to email connection security, such as information security officers or email system administrators. It contains detailed instructions on how to implement DANE in an existing email environment. The factsheet is a valuable resource to share with your email provider and your internal IT department, to help them get a head start in implementing DANE.

Over the past few years, NCSC-NL has organized and participated in many initiatives to further the adoption of email security standards such as DANE. For example, the internet.nl online test is a product of the Dutch Internet Standards Platform, of which the NCSC-NL is a member.

Additionally, the NCSC-NL is in close contact with several large vendors of email server software, to move them to support DANE in their software. This, for many organisations, is still the largest obstacle to take. By working together with these vendors to make this need visible, NCSC-NL hopes to achieve near-ubiquitous use of DANE in the coming years.

[1] Source: Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security, https://dl.acm.org/citation.cfm?id=2815695.

[2] https://internet.nl

[3] https://havedane.net

[4] See https://www.forumstandaardisatie.nl/nieuws/nationaal-beraad-verplicht-starttls-en-dane for more information.

[5] See https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers

U.S. Gov issues urgent warning of DNS hijacking attacks
Malware in Ad-Based images targets Mac users
January
18
21
23
WiFi firmware bug affects laptops, smartphones, routers and gaming devices
New malware found using Google Drive as its command-and-control server

Manifesto - Next Generation PGP

Kai-Chun Ning, Phil Zimmermann, KPN

What is PGP?

Pretty Good Privacy (PGP) is a software suite that provides digital security. With the encryption it provides, PGP can be used to transfer messages confidentially and is often used for email and file encryption. In totalitarian countries where surveillance is prevalent, citizens can make use of PGP to exchange information safely. Journalists often use PGP to communicate with their sources securely in the same manner[1]. In addition to encryption, PGP can also be used to guarantee the authenticity of a message by generating an unforgeable digital signature for it. Similar to a written signature, a digital signature ensures the recipient that the message indeed originates from the claimed source and has not been tampered with. Since its introduction in 1991, PGP has become an essential tool for, amongst others, dissidents, activists, journalists and whistleblowers.

Outdated Standard and Poor Usability

Despite the importance and benefits of PGP, some fundamental design choices hinder its universal adoption and its userbase remains relatively small[2]. When PGP was first introduced in 1991, some security concepts had not been conceived or were still under active research. Consequently, PGP does not possess certain important security standards that are essential today, e.g. forward secrecy and practical group messaging. In particular, the lack of forward secrecy is considered to be a major security deficiency and is not acceptable to many. Besides forward secrecy, by default PGP applies compression before encrypting data, which renders the length of the ciphertext (even more) dependent on the content of the data. This dependency in turn leaks extra information, which has been exploited by researchers in various other cases before, e.g. in TLS, to recover the plaintext[3].

In terms of the choice of cryptographic suite, PGP includes several early cryptographic schemes that are no longer considered secure. The inclusion of those outdated, so-called fossil cryptographic schemes has been proven to be a significant burden for software developers as well as maintainers and provides very little value. Additionally, accidental usage of those cryptographic schemes may lead to a total compromise of confidential information. One such scenario would be when one user in a group email replies with the entire email thread (exchanged so far) included, quoted and encrypted with triple DES[4]. This leakage scenario is still possible even when using the latest PGP software in 2019 due to the requirement of backward

[1] https://www.theguardian.com/pgp
[2] https://pgp.cs.uu.nl/plot/
[3] https://tools.ietf.org/html/rfc7457#section-2.6
[4] https://sweet32.info/

compatibility. To make matters even worse, some of the aforementioned outdated cryptographic schemes (e.g. SHA1) are chosen by default. It is therefore necessary for users to manually configure PGP before usage. Unfortunately, to override the default settings, one would need to go through the lengthy manual of PGP to learn the format of the configuration file and available choices, which can be rather daunting for users who are not technically savvy. In short, improper security practice enforced by the default settings and the lack of a simple user interface makes PGP inaccessible to the general public, even for its very own creator Phil Zimmermann[5].

Trust Model and Key Management

In regards to the accessibility of PGP for average users, one frequently criticized design of PGP is its key management mechanism and trust model. PGP relies on a so-called "Web of Trust" to establish the authenticity of a public key. A Web of Trust removes the need of public key infrastructure (PKI) and certificate authorities (CA) that are commonly used to establish the authenticity of a key like in X.509 based systems. Instead of depending on a centralized CA for the verification of a public key, which is a single point of failure, PGP determines whether or not the key is authentic by the amount of trust that is demonstrated by "other" PGP users in a Web of Trust. In essence, if more than a certain number of other users who are trusted by one particular PGP user claim that the key is authentic, then the key is considered valid and is accepted by this user. This idea, however, has one critical drawback. A Web of Trust transforms the problem of establishing the authenticity of a key from a technical issue into a social one, as a Web of Trust can only function if other PGP users are able to make adequate judgments when vouching for the authenticity of keys. PGP tries to assist users in doing so by labeling keys with a trust level based on the amount of trust (untrusted, marginal, complete, and ultimate). Nonetheless, the procedure remains heavily dependent on human factors as the meaning of those four trust levels cannot be universally established nor scientifically defined. The definition of trust levels even reduces the usability of PGP, since now PGP users must learn the whole complex mechanism behind a Web of Trust in order to be able to assign trust labels properly. The problem of establishing the authenticity of a key therefore is not solved by the introduction of a Web of Trust and is arguably further complicated. In response, many PGP users simply held key signing parties where they physically meet up at one location to safely sign and vouch for each other's' keys.

Furthermore, even if a PGP user manages to label keys with the appropriate trust level, the endorsed keys remain local to this specific user and the user would still need to distribute the endorsed public keys. PGP tackles this problem by setting up a small number of "trusted key servers". Users may upload their endorsement of other users' keys or their own public keys to any of the servers. To prevent the censorship of any of the keys or endorsement thereof, those key servers were designed to never delete either a public key or any information about a key (including its endorsements). The key servers synchronize with each other periodically to maintain one single global database of public keys and together they function as a distribution hub where other PGP users can download those keys.

Despite the various advantages mentioned above, the addition of the key servers together with the rather inefficient design of the key serialization format opens up the avenue to devastating denial of service attacks[6][7]. In short, by maliciously attaching tens of thousands of endorsements (signatures) on a target public key and uploading it to the key servers, an attacker would be able to render any PGP program unusable when the victim imports the poisoned public key into their system, which effectively denies the usage of the target key.

In addition, since a key and its relevant information can never be deleted from the key servers, the so-called revocation certificate was introduced[8]. By uploading the revocation certificate of a key, the actual owner can render their key invalid, thereby retire the key. However, since by design anyone in possession of the private key can revoke the corresponding public key, one cannot distinguish a revocation certificate from the real owner and an attacker who has compromised the private key. Consequently, other PGP users may refuse to trust the revocation certificate and continue to make use of the revoked key. The fact that a revocation certificate may not originate from the legitimate key owner further inhibits the adoption of PGP.

Key ID Spoofing

To facilitate downloading keys from the key servers, PGP provides several approaches to searching for a particular key. One of them is the "key ID", which is simply the lowest 32 or 64 bits of the hash value of a public key. Regrettably though, the introduction of the key ID paved a new avenue to key impersonation attacks. Due to the short length of the key IDs, an attacker can generate different public keys with an identical key ID efficiently. For example, it has been

[5] https://www.vice.com/en_us/article/vvbw9a/even-the-inventor-of-pgp-doesnt-use-pgp

[6] https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f

[7] https://tech.michaelaltfield.net/2019/07/14/mitigating-poisoned-pgp-certificates/

[8] https://tools.ietf.org/html/rfc4880#section-5.2.1

EU considers
proposals to exclude
Chinese firms from
5G network

January

30

NIST reveals
26 algorithms advancing
to the Post-Quantum
Crypto 'Semifinals'

reported that a 32-bit key ID collision of a public key can be found within merely 4 seconds[9].

Quantum Resistance

At last, with the advent of quantum computing, the public cryptographic schemes adopted by PGP (in particular RSA and elliptic curves) would all become fundamentally broken. A complete replacement of the existing asymmetric cryptographic schemes is therefore necessary. To mitigate this imminent threat, several families of the so-called Post-Quantum cryptography (PQC), which are asymmetric Cryptographic schemes that are resistant to quantum attacks, would need to be carefully examined and tailored, after which proper replacement must be selected to meet the various requirements of PGP.

Conclusion

To sum up, the existing standard of PGP presents various challenges that must be addressed:

1. lack of forward secrecy
2. lack of efficient group messaging/email mechanism
3. fossil cryptographic schemes in the standard
4. improper default security settings, e.g. compression before encryption
5. poor usability
6. problematic trust model and key management
7. rather naive design of the key revocation mechanism
8. insecure design of key IDs
9. asymmetric cryptographic schemes that would soon become broken in the face of attackers who have access to quantum computers

In spite of all those issues, PGP is still arguably the best choice in regard to secure digital communication. For example, the famous NSA whistleblower Edward Snowden made use of PGP to contact journalists[10]. At KPN CISO, we believe that those issues, while daunting, can be addressed and solved. Together with the creator of PGP, Phil Zimmermann, KPN CISO has plans set in motion to work on the next generation PGP standard. In addition to the eradication of all the aforementioned issues, we envision the new PGP standard to be secure, relieved of its historic burden, open-source, completely free, and available to people in need just like the first PGP edition that was released back in 1991.

[9] https://evil32.com/

[10] https://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/

New Mac malware targets cookies to steal from cryptocurrency wallets

February 1

Libreoffice (CVE-2018-16858) - Remote Code Execution via macro/event execution

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Operational technology systems and the threats of cyber attacks

Angeli Hoekstra, PwC

A famous and scary example of the far-reaching effects of cyber attacks impacting operational technology systems (OT systems) is Stuxnet, a malicious computer worm. Stuxnet attacks forced a change in the centrifuge rotor speed of uranium enrichment centrifuges in Iran around 2010. It increased the spin rate of specific centrifuges for a few seconds. It waited 27 days and then reduced the spin rate of these centrifuges for a few seconds. By doing this it damaged the centrifuge systems and caused major damages to the Iranian uranium enrichment facilities. Furthermore, it caused damage to a number of other systems in other countries that utilised similar centrifuges. What made it especially alarming was that Stuxnet damaged the safety systems as well. It is terrifying that malware is actually capable of doing this, since it can create serious accidents and threaten human lives. In this article I will discuss the threats cyber attacks can cause to OT systems and I will show what companies can do to better protect themselves.

Black out in Ukraine

More recently we have seen incidents in Ukraine where malware influenced the power grid and interfered with the supply of electricity. A computer virus attacked one of the transmission stations and opened every circuit breaker in this station. It caused a complete blackout. Fortunately it didn't take long to get the system back into operation. This limited the damage caused by the attack. Clearly, incidents like this may have a disastrous effect on the functioning of society.

February
3
4
5

Phishing attacks against Facebook / Google via Google Translate

First hacker convicted for SIM swapping gets 10 years in prison for stealing millions

Metro Bank is the first bank that disclosed SS7 attacks against its customers

Chaos

I worked in South Africa for a number of years and I have experienced what happens when the electricity supply is disturbed for a longer period of time and the traffic lights stop working. It resulted in a complete congestion of roads and total chaos. There is a domino effect when the electricity system is not working. It impacts hospitals, train systems, telecommunication systems, office building systems (such as elevators, security, and air conditioning), manufacturing systems and air traffic systems. If not prepared with an alternative power supply (which later on was installed in South Africa by businesses and consumers of electricity individually), a whole country comes to a standstill and it also may result in loss of life. Thinking of the Netherlands, this brings to mind the water management systems. If they shut down, part of the country could be flooded.

A form of cyber warfare

It appears that many of the more sophisticated OT cyber attacks are initiated by nation states. It is a form of cyber warfare that is directed at operational systems of specific facilities and in the end may have dramatic consequences for the safety of large groups of people. The above examples affect countries on a national scale. But in recent years, private businesses and their operational technology (OT) have also been disrupted by malware that damages their operational systems. An interesting PwC report on this subject is *The Global State of Information Security® Survey 2018 - 'Strengthening digital society against cyber shocks'.*

Business impact

For businesses, cyber security breaches can have far-reaching material and immaterial consequences. At PwC's global OT Cyber Experience Centre, we have looked into a number of these cyber attacks and their impact on OT systems of companies. We observed that in some cases the malware had already been present in systems for years, only to become active when circumstances are perfect. This malware either intended to damage systems for a specific consequential purpose, or to threat with damage and demand a ransom. This can then of course also have consequences for the reputation of a business and the sense of trust in their products or services.

Distrust in the supply chain

The emergence of cyber crime and cyber attacks has caused distrust in the supply chain. Companies ask themselves: which component of which supplier can we rely on to be safe without having to worry about embedded malware in its systems? Businesses and consumers wonder about the safety and cyber resilience of digital components they buy from their suppliers. This has become a point of growing attention for businesses.

OT security assessments

PwC has found that most companies are aware of the importance of cyber security for their IT systems. On the other hand, many do not know that a lack of OT security also poses a serious threat to their business. Performing an assessment of the OT environment to get a clear picture of the vulnerabilities in the OT environment is critical. During an assessment different aspects can be reviewed. For example, the workforce and the security culture of a company, third party risk management to establish the security of the supply chain and for example by screening third parties. But also to review preventative measures, such as anti-virus measures, password management, patch management and network segregation.

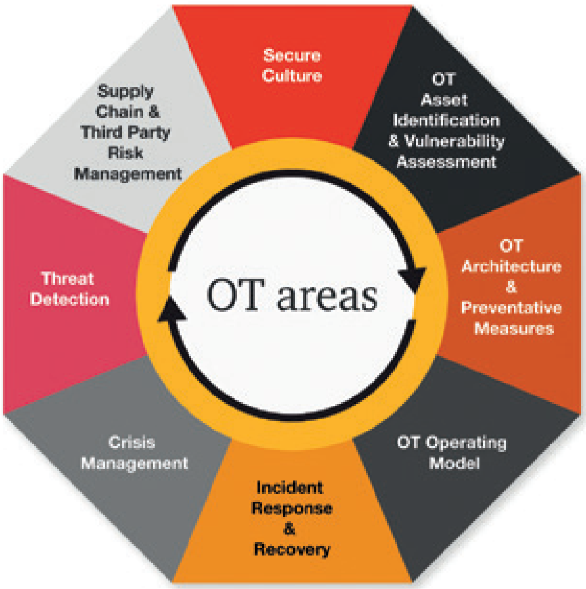

Secure Culture
OT Asset Identification & Vulnerability Assessment
OT Architecture & Preventative Measures
OT Operating Model
Incident Response & Recovery
Crisis Management
Threat Detection
Supply Chain & Third Party Risk Management
OT areas

Figure 1: Overview of OT area's

Incident response and crisis management

However implementing the necessary security measures in OT environments is difficult. Often systems are old and need to be up and running 24/7 and implementing a patch is not feasible. Because of this, a focus on detection and incident response measures is critical. The quicker a company can detect a change in the environment which is not authorised or shows abnormal behaviour, the quicker it can respond and limit the impact of a cyber attack. Incident response and crisis management are critical factors to mitigate risks.

Different threats for different companies

The threats companies and their OT systems are facing vary per company. Companies should ask themselves a number of questions. Where might attacks come from? What type of IT and OT systems do we have?

New MacOS zero-day allows theft of user passwords

February

6

APT10 targeted Norwegian MSP and US companies in sustained cyberespionage campaign

Android phones can get hacked just by looking at a PNG Image

What are the consequences when our OT systems are damaged? Where are we in the supply chain? And there are also other factors a company should consider. For instance, does a company have publicly accessible OT systems used by contractors to do maintenance on the OT systems? Maybe the remote connectivity of these systems is insecure or maybe these systems are easily accessible physically. Companies should also check if they are missing vital security updates.

How to improve the protection of your OT systems?

So what can you do to improve the cyber resilience and the protection of your OT systems? First of all, you need to determine how to increase preventive measures without disrupting your production processes. Are you setting up new facilities, like a new factory? In that case you can design and build prevention, detection and response mechanisms into the facility right from the start of the design process. However, most facilities are not built from scratch and are in use for years with numerous improvements. In that case you need to focus on understanding your design base, your OT assets, and determine your detection and response measurements based on your installed configuration.

Security operations centre

A good step your company could take is to build a hybrid security operations centre. Such a centre can collect different data from different sources and can help identify security incidents in an early stage and even prevent them. The centre can for example gather physical security data and combine the data with IT-related and OT-related security data.

A more advanced option is to build a ‘digital twin’. You can teach the digital twin what the ‘normal’ state of your operations is and that discrepancies from this normal state can be viewed as possible security alerts and not just for example as maintenance alerts (for which a digital twin is normally used). You can also consider building testing labs to test the security and behaviour of specific operational components before implementing them into production. Some of these measures could very well be established together with partners and stakeholders from the sector in which your company operates.

The human factor

Finally, it is important to consider the human factor if you want to improve the OT security of your company and create a secure culture. Often it is the intervention of people that malware exploits and which causes security breaches that otherwise could have been prevented.

First steps to take

So what can you do if you are uncertain about the OT security in your organisation?

It depends on your situation. However, with existing facilities as well as in many other situations: start with doing a quick scan to determine the current situation and its vulnerabilities and risks. This creates clarity. And based on the findings, determine the solution architecture, measurements and roadmap that are required to improve.

February

7

Parents could see other users' privates after cloud migration

8

Australian MP's told to reset their passwords amid hack attack fears

Friction for Privacy

Why privacy by design needs user experience design

Bart Jacobs, Hanna Schraffenberger,
Privacy by Design Foundation and iHub, Radboud University

IRMA is an open source identity platform that is run by the not-for-profit Privacy by Design foundation in The Netherlands. It grew out of academic research at Radboud University Nijmegen – and originally at IBM Research at Zurich in the 1990s. IRMA is now clearly gaining momentum and is being integrated in various ways, especially in healthcare, (local) government, and also in commercial areas such as insurance. The techniques underlying IRMA have been developed with privacy protection as explicit goal. This article explores the impact of this privacy focus on the user experience (UX) and on the ongoing (re)design of the interface of the IRMA app. The authors are both closely involved in the development of IRMA.

What is IRMA?

I Reveal My Attributes (IRMA) is like a Swiss army knife for identity. It offers attribute-based authentication and signing, while encryption with IRMA is in a prototype phase. Here we concentrate on authentication, that is on proving who you are, especially in an online environment.

When first installed, the IRMA app is an empty wallet. The user can subsequently fill it with personal attributes, such as name, date of birth, address, email, mobile phone number, etc. These attributes come from multiple trusted sources and are stored in the user's IRMA app with a digital signature (of the source), so that integrity and authenticity of attributes are guaranteed.

The privacy-preserving character of IRMA depends on two main features in its technical design.

- A user can *selectively* disclose attributes. For instance, in order to watch a certain movie or play a game online, the user discloses only the attribute that he/she is older than 16, or older than 18, and nothing else. This is fully in line with the GDPR's data minimization requirements. We call it *contextual authentication*: a website asks the user to reveal certain attributes, appropriate and necessary for the relevant service, and the user can agree in his/her own IRMA app to the request and disclose these attributes (or not).

- Attributes of an IRMA user are stored *exclusively* in the IRMA app on the user's phone, and nowhere else. When a user discloses (or receives) attributes, data are exchanged directly between the app and the service provider (as verifier, or as issuer, of attributes). There are no intermediate third-parties acting as privacy hotspot, like with Facebook Login or with iDIN (the joint authentication service of banks in The Netherlands). This means that the Privacy by Design foundation that is running IRMA cannot – and does not want to – register where people are getting or showing their attributes or what their values are.

This strong (technical) focus on privacy is all very nice, but is it also the "killing" feature for the wide-scale adoption of IRMA? In our experience, it is not. Instead, the combination of the following five aspects contributes most to adoption: (1) functionality: does it allow users to do what needs to be done; (2) trusted data: can the app be filled with valuable attributes; (3) privacy protection: does it protect against excessive data disclosure; (4) low costs: users should not have to pay at all, and other stakeholders should pay minimally; (5) user experience: is the app pleasant, efficient and intuitive to work with. The development of IRMA has originally focused on the first points. Now that IRMA is no longer an academic research project and is being used in several live projects, our focus has shifted: providing a great user experience without sacrificing privacy has become one of our top priorities. In this article, we explore the interaction between UX design and privacy-protection.

Designing for privacy

A first observation to keep in mind is that an authentication app like IRMA is only a *means*, not a goal in itself. It allows users to log in and to do the things that they are really interested in, namely buying or selling something online, watching a movie, etc. Developers and designers need to be modest in what they can demand from users, since the attention and patience that users will have for authentication are limited.

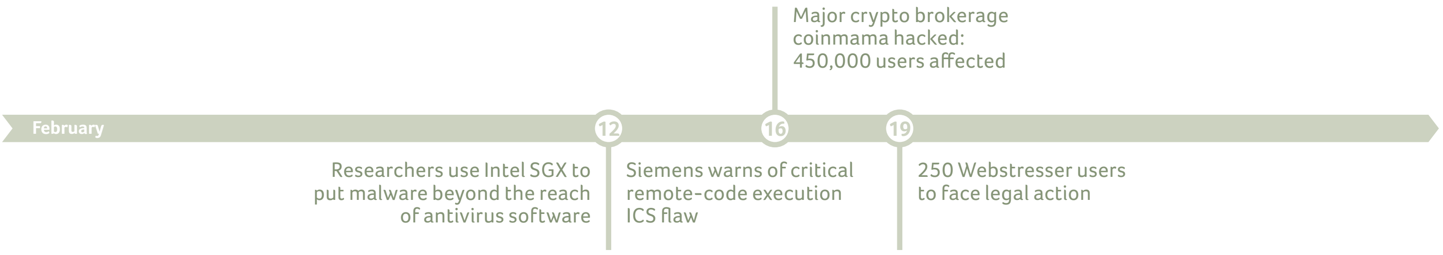
Our second, key point is that there is a dilemma when designing for privacy in authentication: In order to be widely adopted, the app needs to provide people with a smooth user experience and offer users an easy, efficient, intuitive way to disclose their attributes in order to get access. However, to support people in protecting their privacy, the user experience cannot be too smooth and intuitive, since that could make it too easy for people to use the app without really thinking about which information they are releasing and to whom.

Such a tension between user experience on the one hand and privacy on the other hand is not unique to IRMA. Since the introduction of the GDPR, it is hardly possible to visit any website without facing a cookie consent statement, which likely annoys the user and slows them down, but also provides them with at least some form of control over their browsing data.

One might think that we can learn from such consent examples. However, they rather illustrate precisely what we want to stay clear of: the use of design nudges to trick users into doing something which is mostly in the interest of the *website* rather than in their own interest, namely accepting rather than rejecting (tracking) cookies. This widely-spread design mechanism in user interfaces is called a “dark pattern”. It steers people into directions that they typically don't wish to go. Dark patterns come in many forms. A popular example is visually highlighting the choice to agree with something (e.g., to share data for additional “services”) while graying out the option to disagree. Also popular are pre-selecting “agree” as a default, or placing “obstructions”, e.g., allowing users to agree to something with just one click but forcing them to go through a complicated settings menu to disagree.

At first sight, IRMA uses similar design nudges, in particular to keep users in the right flow for authentication: when asked to disclose the necessary information, the option to reveal the requested attributes is highlighted in a striking color, whereas the option to deny the request receives no particular emphasis. However, unlike dark patterns, the intention in IRMA is not to trick people, in the interests of IRMA, but to help them achieve *their own* authentication goal.

Of course, this does not mean that people should blindly agree to IRMA disclosure requests from websites. The GDPR does not allow excessive requests, since it requires data minimization. In this regard, people are protected by the law. But purely technically speaking, requestors can ask for any attributes that they desire, such as a passport number for the usage of a movie service. Since Data Protection Authorities (DPA) are not continuously monitoring the proportionality of every possible attribute request of websites, users also have their own responsibility to recognize potentially inappropriate requests (and to notify the DPA in case of over-asking).



Major crypto brokerage coinmama hacked: 450,000 users affected

Researchers use Intel SGX to put malware beyond the reach of antivirus software

Siemens warns of critical remote-code execution ICS flaw

250 Webstresser users to face legal action

Technology can help users with this challenge, but UX design can play a big role, too. From a privacy-perspective, a proper design triggers users to think critically about each new disclosure, makes them consider whether the request is appropriate and whether all requested attributes are necessary for the relevant service.

Deliberate friction

Unfortunately, relatively little is known about how to design for slow and deliberate decision-making, unlike for fast and non-reflective flows. With IRMA, we are currently exploring different options. One approach would be to alert and slow down the user upon first disclosure of attributes to a new website, for instance with a pop-up text: “You have not visited this site before; are you sure that you wish to disclose these-and-these attributes? Is it clear and fair what the site will do with your personal data? Have you checked the website’s privacy policy?” Subsequently, this choice could be recorded in the app, so that later disclosures to this same website can be handled more quickly. Similarly, a color-code could indicate that a request involves an especially sensitive attribute, such as a citizen registration number (called BSN in The Netherlands). While such design choices will not guarantee that people will carefully consider every single choice, they might help them to stop and think when it counts the most. Another addition that we foresee is a button that allows users to complain directly to the DPA about excessive attribute requests. Ideally, such a button will not only allow users to report abuse easily, but also will foster reflection about the information requests they face. Also, more patronizing strategies are possible. For instance, the app could pause, with a countdown timer, and confront users with a forced time-out reserved for reflection before allowing any choice to proceed. What these ideas have in common, is that when effective, they will cause friction rather than a smooth flow. They will cost users time and mental effort – things that UX design usually tries to reduce[1].

The design mechanisms that we are developing for IRMA are meant to protect people from agreeing too easily to excessive attribute requests. They are like speed bumps and traffic signs on dangerous roads: they slow people down and demand attention for safety. We see it as a duty of care: IRMA is based on value-driven design and its design for privacy requires some slow-downs. A duty of care is especially relevant in situations with a significant knowledge asymmetry – which is often the case with digital technology. As part of this careful approach, also additional regulatory and technical means are being considered within the IRMA project to further protect user’s privacy: for instance, certificates could be made compulsory for verifiers when requesting especially sensitive attributes like passport photos and certain registration numbers.

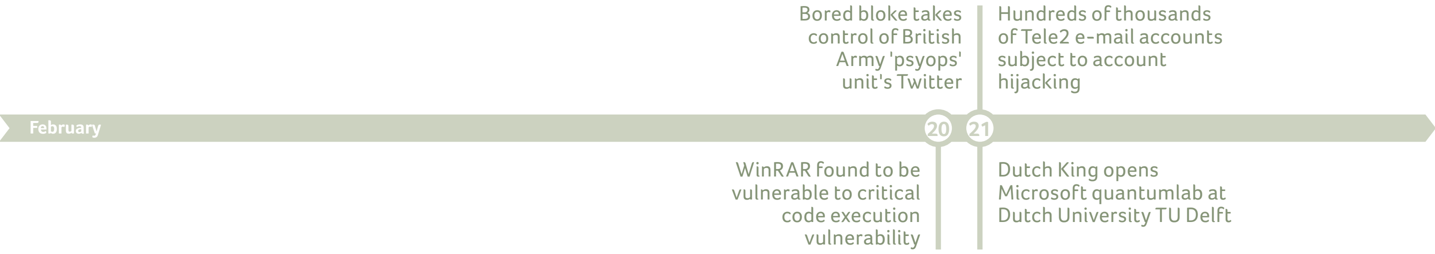
The design of IRMA is a continuous effort. However, some things have become clear already: first, IRMA needs to encourage slow and careful decision-making. Second, IRMA also needs to provide a fast route through the process, in those cases where the same attributes are disclosed to the same party each and every day. Time for deliberation is precious, and users should not be forced to ponder over the same choice every time.

In the end, determining how to resolve tensions between opposing goals requires experience in practice and tests with users, in order to see what actually happens when people’s authentication data is placed in their own hands. What we have observed in tests so far is that young users typically navigate through the app quickly, try out buttons and learn about the app by observing what their actions do, whereas older users generally take time to understand what is happening, to access and read accompanying information, and to make sure to only tab a button once they know what it does.

Concluding remarks

What others can take from our experience is threefold: first, in order to make sure privacy- enhancing technologies effectively enhance people's privacy, these technologies need to be adopted, which requires a smooth user experience. Second, UX design for privacy differs from general UX design. Designers usually strive for interfaces that are intuitive, efficient and a joy to use. When aiming for privacy, other goals are relevant too, which ultimately might cause the experience to be less efficient, pleasant and smooth. Third, privacy-preserving characteristics in a system’s technical design often put people in control over their data. People, however, do not necessarily use this control to actually protect their privacy – possibly even the opposite. User experience design can affect how people handle such control, either by stimulating users to give up information without thinking (e.g. via dark patterns), or by supporting them to reflect, by informing them, and by helping users protect their privacy themselves. All three insights boil down to one conclusion: privacy by design must include careful UX design.

[1] For a broader and more theoretical perspective on how to design for privacy- decisions, with many relevant references, we refer to Terpstra, A., Schouten, A. P., de Rooij, A., & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. First Monday, 24(7). Available at https://firstmonday.org/ojs/index.php/fm/article/view/9358/8051.



Bored bloke takes control of British Army 'psyops' unit's Twitter

Hundreds of thousands of Tele2 e-mail accounts subject to account hijacking

WinRAR found to be vulnerable to critical code execution vulnerability

Dutch King opens Microsoft quantumlab at Dutch University TU Delft

Strengthening the digital security of the supply chain

Sander Peters, KPN

Companies are cooperating ever more intensively with partners, suppliers, subsidiaries and the like. "While introducing scalability, cost-effectiveness and increasing efficiency by outsourcing more and more these days, supply chains also make companies more vulnerable", warns Sander Peters, Head of Security Research at KPN Security. "Cooperation increases the risk of a cyberattack." How do you stop this ecosystem from breaching your security?

The National Coordinator for Security and Counterterrorism (NCTV) has been warning about it for several years: supply chains expands the attack surface of organisations. Attackers are becoming increasingly successful in getting to a target's infrastructure and its data via third parties such as a partners or suppliers.

NotPetya and CCleaner

Criminals make use of inherent vulnerabilities to attack the supply chain. The NotPetya cyberattack in 2017 is a good example of this. It involved the spread of ransomware via legitimate updates from M.E.Doc, a Ukrainian supplier of accounting software. This enabled the actor behind NotPetya to completely paralyze major companies such as Maersk.
Another yet impressive example is the breach of the Cleaner distribution servers in April 2017, where Chinese hackers hacked the Piriform infrastructure via a teamviewer account and successfully injected malware into the system-cleaning software Ccleaner, thereby infecting millions of its users. One of the most peculiar aspects of this situation is that it all happened before the Avast acquisition in July resulting in a PR fallout all throughout 2017 and 2018 for the new owner when the hack became public in September 2017.

Third party risk

Like the NCTV, Sander Peters of KPN Security also sees a clear rise in third-party risks. He feels there are several reasons for that rise. "If I were a state actor, such as the hacking groups APT10 and APT41 that are linked to the Chinese government, I would also target the MSPs and other service providers. By using those large central service providers or global hubs you can access the infrastructures of major parties unnoticed. Additionally, the infrastructures are so large and complex that detecting and erasing all the remnants of a successful hack is extremely hard."

"On top of that, good IT people and hackers tend to be either naturally lazy or superefficient", Peters jokes. "If good security makes it tougher to penetrate an organisation directly, they simply go in search of supply chain vulnerabilities. And it's easier to attack a supplier

February

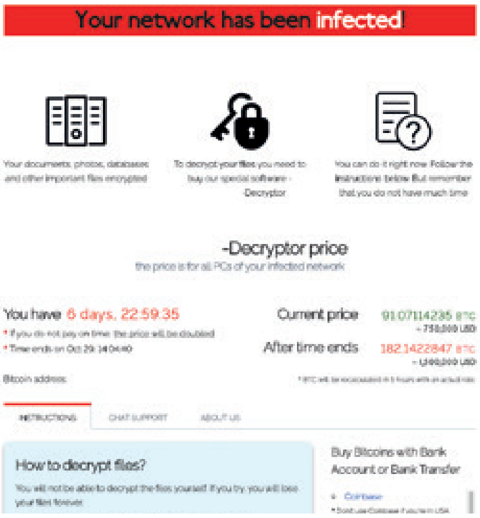
22

ICANN warns for large-scale attacks on the Internet infrastructure

Millions of websites threatened by highly critical code-execution bug in Drupal

28

Terrorists and politicians exposed by Dow Jones data leak that has a line to several organisations in the same sector than to attack those organisations individually.”


Your network has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

-Decryptor price

the price is for all PCs of your infected network

You have 6 days, 22:59:35

* If you do not pay on time the price will be doubled

* Time ends on Oct 29, 14:04:40

Current price 91.07114235 BTC ≈ 750,000 USD

After time ends 182.1422847 BTC ≈ 1,500,000 USD

Bitcoin address:

* BTC will be recalculated in 5 hours with an actual rate

INSTRUCTIONS CHAT SUPPORT ABOUT US

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

Buy Bitcoins with Bank Account or Bank Transfer

- Coinbase

* Don't use Coinbase if you're in USA

Figure 1: REvil ‘ransom’ -demand on their website

Ransomware via MSP

Peters and his team can see the same trend happening in ransomware attacks. “Previously, individual systems got infected via e-mail or web-visits, after which a payment of 300-700 euros was demanded." Cybercriminals are now aiming higher. “That is shown by one of our latest investigations tracking the REvil ransomware and its affiliates. This ransomware family is offered as ransomware-as- a-service, where the makers of REvil themselves receive between 30% and 40% of every payment. This lowers the threshold for carrying out such attacks.”

“The affiliates using the REvil ransomware as a service (RaaS) are skilled and are adapting their approach to the victim’s organisation using specialized campaigns. These campaigns usually start with old school phishing or exploitation of externally accessible functionality as a first step to gain control over the entire network. Our team has found victims of infections at government bodies and healthcare institutions all over the world. In the last few months we saw campaigns focusing on specialized software used by MSPs, like remote access management tooling. Affiliates set a specific ransom for each campaign, varying from 777 dollars to as much as 1,500,000 dollars. It can be determined from the amount of the ransom whether the attack is opportunistic or targeted. Especially in the latter case, the attackers generally knows how much an organisation can pay.”

Grip on external risks

For Peters, the current reality is that the majority of security breaches result from vulnerabilities in the ecosystem. However, security budgets are spent almost entirely on protecting in-house infrastructure and data. According to the Head of Security Research the amount of budget and attention spent on security practices of partners and suppliers should be reconsidered.

“Organisations need to focus not only on protecting their own data and infrastructure but also on the security within the rest of its ecosystem,” Peters stresses. He has some tips for companies that want to get a better grip on the risks inherent to the supply chain:

1. Check and double-check

It is customary to perform a financial and/or legal check on new suppliers. “A cybersecurity check has to become a given”, Peters believes. “An in-depth investigation needs to be carried out to understand how the supplier’s security has been set up and whether the personnel have been screened.”

“But also consider conducting a pentest or a vulnerability scan of the new partner,” adds Peters. “Or perform a security rating.” That rating is a continuous, objective measurement of the digital security of the organisation and of the entire business chain viewed from the outside. The scores give a good initial indication of the current level of security.

2. Accept risks

It is never possible to exclude all risks. “State actors, for example, have billions at their disposal, and plenty of time. So it isn’t really fair to hold a partner with considerably fewer resources accountable for a hack carried out by a state actor. You need to know what your risks are, which risks have to be mitigated and which can be accepted, bearing in mind public opinion and/or the shareholders.”

3. Stay alert

Have the media reported a hack? “Organisations then need to ask themselves whether this attack or something similar could happen to them too,” says Peters. For instance, red flags should be raised when companies and its partners are using software that has been exploited in a public hack. “At KPN Security this is our natural response, but it ought to be the default reaction of every organisation.”

4. Cooperate

“As far as I am concerned, cooperation is key in combating supply chain hacks,” Peters concludes. Cooperation increases the attack surface of the organisation but is also needed to limit the risks. “Explain to your partners why security is so important for both parties, look at how you can make a coordinated response to threats, and grow together to a higher maturity level. And, if needed, ask for the help of your security partner that can help both parties connect the dots.”

March

1
Data tracking Chrome flaw triggered by viewing PDFs

5
Data tracking Chrome flaw triggered by viewing PDFs

7
800 Million e-mail addresses leaked by online e-mail verification service

The end of digital trust is near. How calibrated trust can help us

Dr. Remco Wijn, Drs. Caroline van der Weerdt, Dr. Rick van der Kleij, Dr. Heather Young, TNO

Trust is paramount for creating social and business relations, adopting technology, cooperating and creating economic value. With an increasingly digital economy, no wonder the importance of digital trust is advocated by so many scholars and businesses alike. However, contrary to purported common wisdom, we propose that actual trust is not created through communicating one's trustworthiness, and should not be an isolated goal in itself. Rather, real trustworthiness comes from actively practicing fair and transparent policies and conduct, the establishment and maintenance of which rests with both the trustor (e.g., a customer) and the trustee (e.g., a supplier). In this paper, we introduce the concept of calibrated trust, and how it relates to the need for increased customer involvement.

Concepts of digital trust

Digital trust is considered the “new gold” for organisations and crucial for the development of the digital economy (NLdigital, 2019). It is even considered by some to be a prerequisite for doing business (Buijs and Vermeulen, 2016). Digital trust could “stimulate 2.8 percent additional growth for large organisations, potentially creating value estimated at 5.2 trillion dollars for society as a whole” (Abbosh & Bissell, 2019). Statements as these logically motivate organisations to ask how they can gain trust among their customers, leading to suggestions that “With the right people, the right means and flexibility you can reach the ultimate goal of communicating trustworthiness”, or: “Digital

Citrix hacked by password-spraying attackers
March
8
9
11
Citrix investigating unauthorized access to internal network
TLS 64bit-ish serial numbers mass revocation

trust is not just about cybersecurity, but also ethics, privacy and reliability" (Naber, 2019), or: digital trust is "a strong focus on security combined with transparency on the use of customers' data" (Buijs and Vermeulen, 2016).

Although such statements are largely true, the problem is that they often suggest that trust is a goal in and of itself or a means to create economic value. It ignores the end user's (or the customer's) role and behaviour in the digital environment. Moreover, a focus on winning trust underappreciates the needs, deliberations and goals of individual customers, and the functioning of trust itself. We argue that this approach stands in the way of cybersecure behaviour at the customer end, and therefore in the way of a durable trust basis.

Digital trust in practice

Let's take a moment to think about what happens when we trust. Suppose someone is exploring the domain of smart home appliances. The consumer starts by installing a smart door lock with which one can see who is at the front door and unlock the front door using an application on a mobile device. A consumer may be wary that hackers could find ways to intercept the communication between the mobile device and the door lock or find other ways to control the lock. The lock vendor tells the customer that a particular lock uses first class software and protocols, which cannot be intercepted or hacked. The vendor gains the customer's trust and the lock is sold.

What the vendor did not focus on, however, are other vulnerabilities that may pose a risk to the door lock, such as the need to change the password or to install software updates. Because the consumer trusts the device, basic cyber hygiene measures, such as updating the software, are neglected, leaving the device vulnerable. If the customer's home network is compromised, for instance through another weakly secured device or vulnerabilities in outdated software, and the front door is hacked, this may leave the consumer not only victimized but also untrusting of the vendor, manufacturer, the lock, and digital smart home solutions as a whole. Extending this line of reasoning: too much trust may harm the development of the digital economy and perhaps even society as a whole.

In this example, the customer trusted the lock manufacturer to build a sound and secure lock and the predictability with which it does its job. The customer trusted the vendor to be knowledgeable about home appliances and security, to sell the customer a product in his best interest, and his integrity to give complete an accurate advice. Thus, trust, which we define as a willingness to depend on another, is a result of beliefs about the competence, benevolence, integrity, and predictability of the other on whom one chooses to rely (McKnight & Chervany, 2001).

Some trusting beliefs seem primarily functionally based (i.e., competence and predictability). These beliefs are often influenced by assurance cues such as a modern, well-functioning, or normal appearing website, and security heuristics such as security information displayed in the address bar of browsers (Cheshire, 2011; Li, Hess, & Valacich, 2008). However, such measures do not influence trusting beliefs regarding benevolence and integrity which seem primarily intrinsic and value-based (Krauter & Faullant, 2008). Studies on online banking, for example, show that security measures and perceived security do not influence consumer trust. According to these studies, trust is more influenced by privacy perceptions of online bank services (Law, 2007), which relates much more to the core of companies' intrinsic values and identity.

Consequences of trust

Trust enables us to create durable social relationships, to work together toward common goals, to invest in each other, to do business, et cetera. Abbosh and Bissell (2019), among many others, focus on positive commercial and financial effects of trust. However, an elemental part of trust is that it involves uncertainty or risk, such as of not receiving an online purchase (Cheshire, 2011). It also involves the absence of direct control. For example, typically, most societies offer legal safety nets for situations in which trust is violated. But these do not offer a direct way of controlling the behaviour of the other person or organisation, nor will they always be effective. Thus, from the perspective of consumers, trust is a leap of faith to overcome uncertainty with a chance of being duped and without much control to restore any harm done.

And people and institutions do get duped. Instances of misplaced or manipulated trust lead to an average annual costs of EUR12 million per large organisation worldwide (Ponemon Institute, 2019). Other consequences include negative emotional and practical consequences as a result of identity and data theft or abuse, or even physical harm in the case of online trade in counterfeit pharmaceuticals.

Need for calibrated trust through engagement

In light of this leap of faith to overcome uncertainty, we introduce the concept of calibrated trust as a more effective approach to developing enduring digital relations. We colloquially define calibrated trust as healthy distrust. That is, companies and organisations should help consumers understand what they trust, when they trust, and to take ownership of their own cybersecurity whenever possible. It means that companies should not only help customers take the leap of faith, but also help them cope with the uncertainty and risk inherently present in trusting relationships. In order to do this, we posit that organisations should

March

12 MEPs adopt Cybersecurity Act and want EU to counter IT threat from China

13 Open-source 64-ish-bit serial number gen snafu sparks TLS security cert revoke runaround

help consumers gain the capabilities, opportunities and motivation to determine the security of their services and products, and the trustworthiness of individuals and organisations providing those services and products. This means disclosure of possible cybersecurity strengths and weaknesses, coupled with proactive tools for protection and resolve on the customer level. Moreover, it implies partnering with customers, teaching them, tooling them and motivating them to prevent victimization and warrant a positive online experience. This goes beyond customer engagement purely on the experiential level of a product or service; it requires engagement on a far-reaching procedural and functional level. This is not an easy task, and requires a different type of relationship with the customer. However, we believe that adding this layer of customer engagement will in the end induce a better customer experience overall.

Research agenda

Organisations' current practices to establish and maintain digital trust often revolve around their own measures to communicate trustworthiness, but exclude the crucial role of the end user. We posit that companies should partner with end users and customers to focus on introducing calibrated trust within their (digital) portfolio. In a shared research program with Dutch financial institutions, we are presently conducting research on the workings and consequences of this calibration process in relation to security and how real trust is fostered. This research includes questions on how to prevent false perceptions of security, how these perceptions are influenced and how they differ between consumers and per technology, how we can optimally support consumers in making the right security decisions, and how to change (false) perceptions that customers may hold, for instance, through better security design. By answering these questions, together with our business partners, we aim to support the goals of both cyber secure behaviour and economic benefit.

Literature

Abbosh & Bissel (2019). https://www.accenture.com/pl-en/insights/cybersecurity/reinventing-the-internet-digital-economy retrieved on 1-11-2019.

Buijs & Vermeulen (2016). https://www.accenture-insights.nl/nl-nl/artikelen/digital-trust-oracle. Retrieved on 1-11-2019.

Cheshire, C. (2011). Online trust, trustworthiness, or assurance? Daedalus, 140(4), 49–58. doi:10.1162/DAED_a_00114 PMID:22167913

Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: the influence of internet trust. International Journal of bank marketing, 26(7), 483-504.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. European Journal of Criminology, 12(2), 226-241.

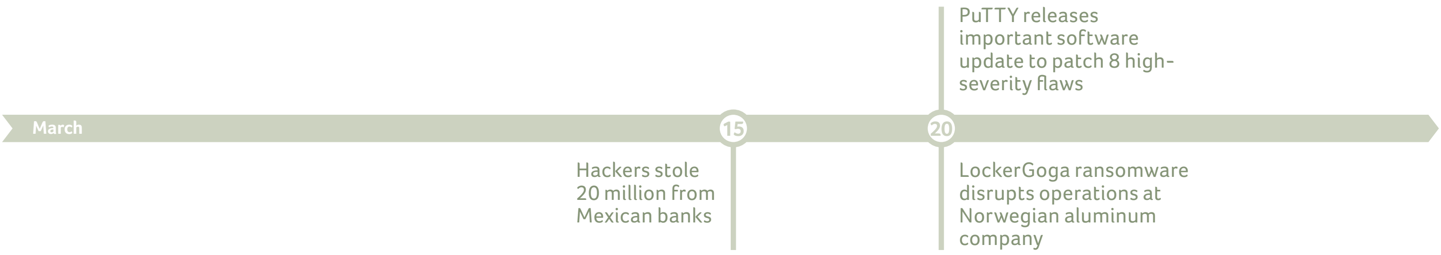
Law, K. (2007). Impact of perceived security on consumer trust in online banking (Doctoral dissertation, Auckland University of Technology).

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

Naber (2019). https://www.pwc.nl/nl/actueel-en-publicaties/themas/digitalisering/bouwen-aan-digitaal-vertrouwen.html retrieved on 1/11/2019.

NLDigital (2019). https://www.nldigital.nl/thema/vertrouwen/ retrieved on 1/11/2019

Ponemon Institute: The cost of cybercrime study (2019). Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 on 1-11-2019.



PuTTY releases important software update to patch 8 high-severity flaws

Hackers stole 20 million from Mexican banks

LockerGoga ransomware disrupts operations at Norwegian aluminum company

Five threats that influence the cyber landscape

New cybercrime operating model among high-profile threat groups

Michael Teichmann, Accenture Security

Cybercrime is not a one-time event. Just as one avenue of income has been blocked, cybercriminals will swiftly move on to another, often more sophisticated means of entry. And even tried and tested methods of attack, such as ransomware, can be subject to change, as threat actors apply the principles but interpret the execution in new and different ways. Deepfakes, disinformation distribution, and supply network attacks are among the most recent cybercrime examples. Security is front and centre of maintaining trust, but with new threats constantly emerging, it is being sorely tested.

New threats ascend the throne

Strong investment in cybersecurity has not been lacking. But despite these investments, the relentless creativity of cybercriminals continues to put pressure on organisations to be defence-ready. Threat intelligence provides the right information to make better business decisions. But the scope of that intelligence is growing. Businesses could start evaluating their cyberpostures from many different perspectives—the cyberposture of suppliers, partners and acquisition targets are just as important as their own organisations to avoid opening up new security gaps or inviting in threat actors who are dormant or active on third-party networks.

“To maintain a power balance between the defenders and cybercrime, we (the defenders) need to start out-innovating the adversary and increase our collaboration,” Floris Van Den Dool, managing director at Accenture Security. “Only with increased sharing of knowledge and platforms, and implementing innovative ideas collaboratively across companies will we be able to balance out an ever-increasing threat landscape and technology sprawl that will see accelerated growth and exponentially impact our challenge as defenders.”

March

21 Brit Police Federation cops to ransomware attack on HQ systems

22 Medtonic's implantable defibrillators vulnerable to life-threatening hacks

26 WinRAR zero-day abused in multiple campaigns

28 Cisco botched patches for its RV32/RV325 routers

A shift in high-profile cybercrime operating models

We see a significant increase in threat actors and groups conducting targeted intrusions for financial gain, also referred to as 'big game hunting'. Despite the arrests of individuals associated with online underground marketplaces, activity among infamous threat actor groups—such as Cobalt Group, FIN7 and Contract Crew—has continued. Accenture Security analysts have also observed the shared use of tools that automate the process of mass-producing malicious documents to spread malware, such as More_Eggs, which is used in both conventional crimeware campaigns and targeted attacks.[1]

The continued activity is associated with relationships forming among 'secure syndicates' that closely collaborate and use the same tools—suggesting a major change in how threat actors work together in the underground economy. With syndicates working together, the lines are even more blurred between threat actor groups, making attribution more difficult.

In addition, we've observed a shift in the way Cobalt Group targets victims to gain access to the victims' supply chain networks. While malware has typically been sent to internet users via phishing emails, we now see an emergence of malware executed through web browsers focused on targeting online merchants and retailers specifically.

accenturesecurity

2019 CYBER THREATSCAPE REPORT

accenturesecurity

5 FACTORS OF THE CYBERTHREAT LANDSCAPE

We see these five factors influencing the current cyberthreat landscape:

1. Compromising geopolitics: New threats emerge from disinformation and technology evolution

Emerging technologies, such as artificial intelligence (AI), present new avenues of expression for potential geopolitical activity, including disinformation. One menacing use of AI is in the creation of 'deepfakes', which are high-quality forged images or videos that could be used for anything from discrediting or blackmailing a political opponent, rival company or extortion target, to causing worldwide panic with a video of a head of state purportedly claiming to have launched a nuclear weapon.

The propagation of synthetic media content, such as deepfakes, is likely to accelerate as fabrication tools become more accessible and widespread. This could spill over into the cyber domain, where both politically and financially motivated actors could leverage deepfakes during target reconnaissance on social networks or social engineering campaigns, for example.[2]

As they focus more on interference with AI modelling, threat actors and groups are likely to deploy adversarial AI, corrupting the ability of machine learning algorithms to interpret system inputs and exercising control over their behaviour. Adversarial AI using deep-learning applications in natural-language processing could enable the manipulation of algorithms that determine sentiment, gather intelligence, or filter for spam and phishing.

[1] Accenture Security. "2019 Cyber Threatscape Report." 2019. https://www.accenture.com/nl-en/insights/security/cyber-threatscape-report.

[2] "Know Your Threat: AI is the New Attack Surface," Accenture, 2019. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf.

April

4
Ongoing DNS hijacking
campaign targeting
consumer routers

11
VPN applications
insecurely store
session cookies

12
Internet Explorer zero-day
lets hackers steal files
from Windows PCs

16
Dutch Telecom provider
starts experiment with
Secure File Transfer

We encourage organisations to combine multiple approaches to help ensure robust, secure AI, especially rate limitation, input validation, robust model structuring and adversarial training. Media sources have named various tools to help detect inauthentic videos.[3][4]

5G enters the security mix

Another watershed technology with the potential to enable massive surveillance and disruption is 5G. This technology's local processing of data means those who control the infrastructure could tamper or spread disinformation to 5G users.[5]

These issues dovetail into national security concerns, as core multinational disagreements persist around the accountability of 5G infrastructure providers and concerns that the control of equipment and software in 5G infrastructure could enable a small group of companies to conduct information operations against a global population of users.

We believe sufficiently advanced AI and Edge systems in control of layer seven application data could dynamically splice deepfakes into streaming content to select users. This technique would likely be used to target VIPs and other decision-makers while they consume news media.

Geopolitical analysis and a strategic-level understanding of the events that motivate cyberthreats to action can help you manage known threats and allocate resources in anticipation of emerging threats. Be vigilant and prepare for the fact that world events are often a target, with phishing lures or distractions taking advantage of and being used to influence outcomes.

2. Cybercriminals adapt, hustle, diversify and are looking more like states

Despite high-profile law enforcement actions against criminal communities and syndicates in 2018, the ability of threat actors to remain operational highlights the significant increase in the maturity and resilience of criminal networks in 2019. Our analysis indicates conventional cybercrime and financially-motivated, targeted attacks will continue to pose a significant threat for individual Internet users and businesses. However, criminal operations will likely continue to shift their tactics to reduce risks of detection and disruptions. They could also attempt to maximize the return on effort in several ways such as: shifting away from partnerships to operating within close-knit syndicates; taking advantage of familiarity with the local environment; increasing the precision of targeting by using legitimate documents to identify likely victims before delivering malware; or selling and buying direct access to networks for ransomware delivery rather than carrying out advanced intrusions.

3. Hybrid motives pose new dangers in ransomware defence and response

Ransomware is increasingly plaguing businesses and government infrastructures, with the number of ransomware attacks more than tripling in just the past two years[6]. Aside from delivery via spam campaigns, analysts have witnessed threat groups Nikolay and GandCrab planting ransomware directly on networks through network access intrusions[7]. Actors are offering to sell remote desktop protocol (RDP) access to corporate networks, which they've likely gained through compromised servers and RDP brute forcing, to those in underground communities.

The ransomware threat will be exacerbated further by the sale of access to corporate networks—through which an attacker can deploy ransomware on a corporate-wide scale—and the potential of ransomware with self-propagating abilities (such as WannaCry) to re-emerge could pose a significant threat to businesses, particularly those with time-critical operations.

While the motives behind such an attack may appear to be financial, targeted ransomware attacks may at times serve hybrid motives, whether financial, ideological, or political. Regardless of motive, while the ransomware threat remains, organisations must ensure they take adequate measures to prepare, prevent, detect, respond, and contain a corporation-wide ransomware attack. Considering the possibility that an apparently financially-motivated ransomware attack may in fact serve other purposes, a ransom payment may not guarantee the restoration of company data; therefore, companies should plan for the recovery of operations, even in the event of a disruptive loss of data.

[3] "Browser Plug-ins that Spot Fake News Show the Difficulty of Tackling the 'Information Apocalypse.'" The Verge, August 23, 2018. https://www.theverge.com/2018/8/23/17383912/fake-news-browser-plug-ins-ai-information-apocalypse.

[4] "AI and Machine Learning Exploit, Deepfakes, Now Harder to Detect." PCMAG, May 13, 2019. https://www.pcmag.com/article/367357/ai-and-machine-learning-exploit-deepfakes-now-harder-to-detect.

[5] Cybersecurity and Infrastructure Security Agency. "Overview of Risks Introduced by 5G Adoption in the United States." July 31, 2019. https://www.dhs.gov/sites/default/files/publications/19_0731_ cisa_5th-generation-mobile-networks-overview_0.pdf.

[6] Accenture Newsroom. "Malware and Malicious Insiders Accounted for One-Third of All Cybercrime Costs Last Year, According to Report from Accenture and Ponemon Institute." March 6, 2019. https://newsroom.accenture.com/news/malware-and-malicious-insiders-accounted-for-one-third-of-all-cybercrime-costs-last-year-according-to-report-from-accenture-and-ponemon-institute.htm.

[7] iDefense Security Intelligence Services. "Account GandCrab Advertises GandCrab Ransomware Version 5.0." September 27, 2018. IntelGraph reporting.

April
21
23
25

Thousands of Oracle WebLogic systems exploitable because of zero day vulnerability

German security office warns of increasing ransomware attacks on firms

Source code of Carbanak trojan found on VirusTotal

4. Improved ecosystem hygiene is pushing threats to the supply chain, turning friends into frenemies

The global interconnectedness of business, the wider adoption of traditional industry cyberthreat countermeasures and improvements to basic cybersecurity hygiene appear to be pushing cyberthreat actors to seek new avenues to compromise organisations, such as targeting their supply chains—including those for software, hardware and the cloud.

Organisations should routinely seek full awareness of their threat profiles and points of supply chain vulnerability. Organisations can try to improve processes that guard against the cybersecurity risks inherent in the landscape of modern global business operations by integrating cyberthreat intelligence into M&As and other strategically important actions, incorporating vendor and factory testing into their processes, and implementing industry-focused regulations and risk assessment standards.

5. Life after meltdown: Vulnerabilities in compute cloud infrastructure demand costly solutions

The discovery of multiple side-channel vulnerabilities in modern CPUs over the last two years could pose a high risk to organisations running their compute infrastructure in the public cloud. Adversaries can use this class of side-channel vulnerabilities to read sensitive data from other hosts on the same physical server. Mitigations are available for most platforms, cloud deployments, and software.

However, most of the mitigations come at a cost of reduced performance, leading to a potential increase of compute costs for enterprises. Understanding the threats posed by CPU vulnerabilities is important to design a proper risk mitigation strategy, which can be vastly different for each organisation.

So, what should you do?

In the past year, cybercriminals have continued to test the resilience of organisations and governments by layering attacks, updating techniques and establishing new, intricate relationships to better disguise their identities. It is no longer enough to plan for attacks or understand what to expect.

Today, organisations must not only take on the disruptive forces that are changing their industries with speed, confidence and continuous innovation, but also remember their most important currency—trust. Security is front and centre of maintaining that trust, but with new threats constantly emerging, it is being sorely tested.

Stay one step ahead of the cyberattackers. Look at security with a wide lens, to include the vulnerabilities of partners and third parties in the scope of their cyberstrategies. Be consistent but flexible in your defence; adapt your approach to meet the latest demands from a rapidly changing world.

IT service provider refuses to pay ransom, hackers publish stolen data online

Viber VOIP app used to steal contact list, impersonate your phone number

Binary Reversing 101

Sebastiaan Groot, KPN

At its simplest, reverse engineering is the act of trying to understand an engineered product by observing and analyzing it, rather than reading a comprehensive piece of associated documentation or having the product explained to you. Take the open and extensively documented main protocol underlying the Domain Name System (DNS) for example and assume its inner workings are a secret. How would you go about understanding the bits and bytes that go over the wire? You would capture some DNS traffic, modify the domain name or record type and resend the request. Having captured both requests, you can compare the differences and document the changes.

This article focuses on binary reverse engineering, the act of trying to understand what an executable does and/or contains simply by observing and analyzing the executable binary itself. Why learn and practice binary reversing? It is an important aspect of malware analysis and vulnerability research. Besides its direct applications, the skills that it teaches are also applicable to other aspects of security research. For whom is this article intended? Some operating system and low-level programming knowledge is useful, but these can be substituted by enthusiasm and curiosity.

How do you go about binary reversing? There is no “one way” or individual toolset that works for every situation. We showcase examples for Linux executable binaries on a 32-bit x86 architecture because of the availability of high-quality free tools, but alternatives exist for almost any environment. Generally, you can divide binary analysis methods into two categories: static and dynamic analysis methods.

Static analysis tools

With static methods you analyze properties of the binary without executing the binary itself. Static analysis methods include inspecting the ELF header (the executable format used in Linux, like PE is used

New exploits for unsecure SAP systems

Hackers found exploiting Oracle WebLogic RCE flaw to spread ransomware

Sophos sees new ransomware MegaCortex being used in the wild

Mystery Git ransomware appears to blank commits, demands Bitcoin to rescue code for Windows) and disassembling the program from raw bytes back to assembly language. The following list names a few static analysis methods that we are going to use in this exercise:

- **readelf**: Shows properties of the ELF header, including target architecture, endianness, sector information and dynamic symbols.
- **objdump**: Disassembles an ELF file, translating the raw bytes to (mostly) readable assembly language.
- **strings**: Extract readable sequences of characters from any file, with support for multiple character encodings.
- **interactive disassemblers:** Feature-rich disassemblers. Analysis tools generally include finding cross-references, automatic detection of strings, code and labeling of function arguments. IDA Pro, Radare2 and Ghidra are examples of interactive disassemblers.

Dynamic analysis tools

With dynamic methods you analyze the binary by executing it in some fashion. The main advantage of dynamic analysis is that you can clearly observe what the binary does during execution. However, you are only able to observe (generally) one execution path through the program in a single execution run. Some dynamic analysis tools that are going to aid us include:

- **strace**: Executes the program and records all system calls that it makes.
- **ltrace**: Executes the program and records all (dynamic) library calls that it makes.
- **gdb**: Executes the program in a debugger. This allows you to halt execution at specified locations and walk through the program step-by-step, examining what it does.

Getting to know your tools

We start this exercise by “reverse engineering” a trivial program to get familiar with some of these tools. You should always use an isolated environment when dealing with unknown programs but setting up such an environment is outside of the scope of the exercise. The programs we will be analyzing are safe to run on your system (source and Makefiles are included), but setting up a separate virtual machine for the purpose of analysis is advisable nonetheless.

Start by installing readelf, **objdump**, **strings**, **strace**, **ltrace**, **gdb** and **radare2** on your Linux distro of choice. Next, download the **basics** program that we are going to analyze from the exercise repository on GitHub[1].

Start by gathering some basic information about the program using **readelf**.

```
$ readelf -h -dyn-syms ./basics
 ELF Header:
   Magic:   7f […]
 […] printf@GLIBC_2.0 (2) [...]
```

From this we can glean a lot of basic information about the binary. The *Class* is *ELF32*, with *Machine* of *Intel 80386*, indicating that this is a 32-bit x86 binary. The *type* is *EXEC (Executable file)*, meaning it is an executable program. Especially useful for more obfuscated binaries is the *Entry point address*, as this tells you where the operating system will start execution of the program once it is properly loaded. The next section of output talks about the *‘.dynsym’* symbol table. The dymsym table includes the names and library versions of external functions that this program can call (and generally only external functions that it needs). For many programs, imported function names already give some indication of the types of behavior that the program might exhibit.

As a quick second step, use **strings** on the binary.

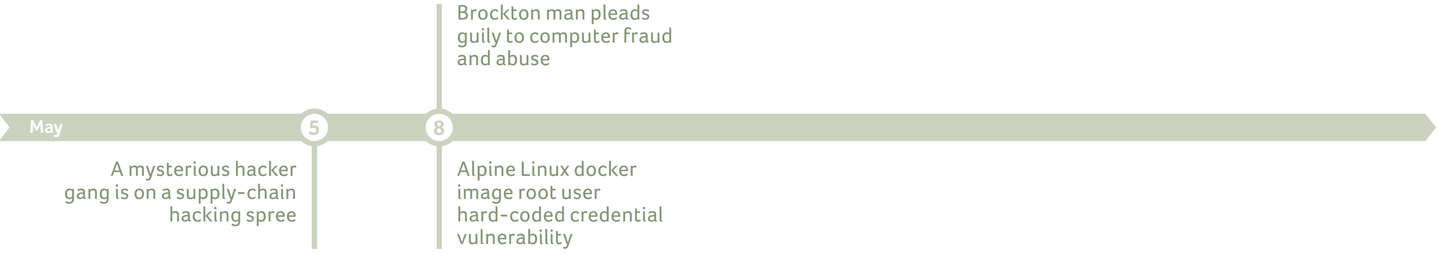
```
$ strings ./basics
[…]
_ITM_registerTMCloneTable
[^_]
AWAITING REVERSING INPUT:
[…]
```

As you can see, most of the output consists of function labels, version numbers and file names. In between this output is the text “AWAITING REVERSING INPUT:”, perhaps hinting towards a prompt that the program will present to users.

At this point we could start disassembling the binary, but analysis of assembly is generally a fairly lengthy process. Let us first see what the program seems to do when we execute it.

```
$ ./basics
AWAITING REVERSING INPUT: test input
tupni tset
```

[1] https://github.com/sebastiaangroot/binary-reversing-101



Brockton man pleads guily to computer fraud and abuse

A mysterious hacker gang is on a supply-chain hacking spree

Alpine Linux docker image root user hard-coded credential vulnerability

It seems to ask for input, after which it answers the user. To see what dynamic library functions the program uses, use **ltrace**.

```
$ ltrace -o ltrace.txt ./basics
AWAITING REVERSING INPUT: test input
tupni tset
$ cat ltrace.txt
__libc_start_main(0x80491b0, 1, […]
printf("AWAITING REVERSING INPUT: ") [...]
gets(0xffc172a0, 0xffc172d0, 3, 0) [...]
strlen("test input") [...]
putc(116, 0xf7f5fce0, 3, 0xffc172a0)
[…]
```

As you can see, the program uses a combination of *printf, gets, strlen* and *putc* to function, and seemingly nothing else. Note that statically compiled libraries are not going to show up here, as **ltrace** has no way of differentiating between statically compiled library functions and native functions of the program itself.

> As a side note, is any of the output of ltrace alarming to you? If so, why is some of this output cause for concern? Can you crash the application with this knowledge? Can you make the application do something it was not designed for?

Similarly, **strace** can record any system calls that a program makes. While system calls are often less descriptive than high-level library functions are, they are necessary for programs to interact with the system. Any output the program generates or information possibly gathered from the system is handled through system calls, making **strace** a very useful tools to quickly understand how a program interacts with the rest of your computer.

```
$ strace -o strace.txt ./basics
[…]
$ cat strace.txt
execve("./basics", ["./basics"], […]
[…]
write(1, "AWAITING REVERSING INPUT: ", 26)
read(0, "test input\n", 1024) = 11
write(1, "tupni tset\n", 11) = 11
exit_group(0)
```

As you can see, **strace** generates quite a lot of output. Most of it is related to loading the binary and setting up its memory layout while loading any dynamic libraries it might need. The first system call truly generated by the program itself is *write*, which writes data to a file descriptor (in this case file descriptor 1, the default for *STDOUT* on Linux). After which it uses *read* to ask for user input via terminal or console and a single call to *write* to respond in kind. But wait, didn't **ltrace** show us that the program made many calls to *putc*? Apparently, the library that implements *putc* does not make a call to the write system call for every call to itself, but rather buffers some data before writing a larger amount of data in a single system call.

We now have a fairly good idea of what the program functionally does, as well as the system calls it uses to achieve this. At this point, we mainly have heavier, more time-consuming analysis tools left. Although absolutely overkill for this trivial binary, we will briefly go over basic functionality of all three: debuggers, disassemblers and finally interactive disassemblers (radare2 in particular).

The debugger of choice that is used in this exercise is **gdb**. By itself it is a simple but easily extensible and scriptable debugger. There are a lot of good plugins available for gdb that makes your life easier as a reverse engineer. The one that I would recommend for this exercise is PEDA[2] for its ease of installation and useful display of your current debugging state. Start by executing **gdb** with the *basics* program, set a breakpoint at the '*main*' function and start execution.

```
$ gdb ./basics
gdb-peda$ break main
Breakpoint 1 at 0x80491b4
gdb-peda$ run
```

If you decided not to use PEDA, you can use the commands *"x/20i $eip"* to disassemble the next twenty instructions from the current instruction pointer and *"info registers"* to print the current register contents.

You can use the command "*step*" to execute the next instruction in the program. This is the most fine-grained method of slowly executing the program one instruction at a time. The command "*next*" works in a similar fashion but treats call instructions (which perform a function call) as a single instruction. Instead of halting on the first instruction of that function call, it performs the entire function call and halts on the first instruction after the function returns. This is useful if you are not interested in the inner workings a certain subroutine but would rather spend your time analyzing the function you are currently examining. Finally, "*continue*" is useful if you want to let the program execute until it hits another breakpoint. For example, you may hit a lengthy loop within the program. Once the loop is identified, you can place a breakpoint on the first instruction after the loop, and call "continue" to quickly let the program execute through the loop.

[2] https://github.com/longld/peda

BlueKeep: Security update to close Remote Desktop Services vulnerability in Windows

Researchers Dutch University (VU) find big leak in Intel processors

Remote desktop services remote code execution vulnerability

May 14

WhatsApp discovers 'targeted' surveillance attack via Zero-Click remote code execution

Intel side channel vulnerability MDS

Keyloggers injected in web trust seal supply chain attack

Hackers access data from more than 460,000 accounts at Uniqlo's online store

What if you want to disassemble the program quickly, but without running the program in a debugger simultaneously? That is what simple disassemblers such as **objdump** are made for. Run **objdump** with the -d flag to automatically disassemble any code that **objdump** recognizes.

```
$ objdump -d ./basics
[…]
080491b0 <main>:
 80491b0:   55          push   %ebp
 80491b1:   89 e5       mov    %esp,%ebp
[…]
```

Just like using a debugger on a program without the accompanying source code, this takes some knowledge of assembly language. Luckily, assembly language is fairly simple in its structure, it is just very verbose and thus takes time to analyze. Start by reading the disassembly of the *main* function and try to identify where the calls to functions that we saw earlier were made. Are you also able to find the *jmp* and *jl* instructions? Those cause the execution flow to jump around within the *main* function. Especially the *jl* instruction (jump if less than) is notable in this program, as it is a conditional jump that decides whether the program should continue executing a certain loop or not.

If we want more of the program analysis of the disassembly to be done for us, we can start looking into interactive disassemblers such as IDA, Ghidra and Radare2. Given the permissive license of Radare2 (GNU LGPLv3) we will use that, but both IDA and Ghidra are worth a look as well.

For the purpose of this exercise, we will limit our use of Radare2 to examining the control-flow graph (CFG). A CFG is a directed graph where the nodes are basic blocks (a sequential set of instructions without jumps) and the edges represent the jumps between basic blocks. CFG's are an incredibly useful visualization of the control-flow through a function and allows you to immediately identify loops and branches. Start by executing **radare2** and telling it to analyze the binary.

```
$ radare2 ./basics
[0x08049090]> aaa
[…]
[0x08049090]> VV @ main
```

The "*aaa*" command tells **radare2** to use many of its binary analysis techniques. This allows **radare2**, among other things, to identify functions and label possible function arguments where it can. The command "*VV @ main*" tells **radare2** to enter visual graph mode, where you can navigate with the "hjkl" or arrow keys to explore the CFG of the *main* function. Pressing *q* twice brings you back to the **radare2** shell.

Radare2, as well as IDA and Ghidra, have a wealth of features to explore besides the CFG view. For a more comprehensive look at Radare2, take a look at the radare2 book on gitbooks[3].

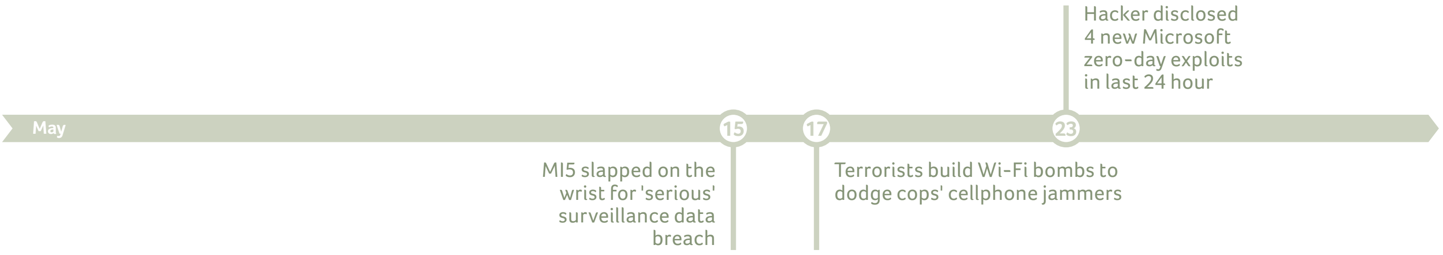
A small challenge

Having briefly familiarized yourself with some of the basic (and not so basic) tools and techniques of binary reverse engineering, I want to invite you to reverse engineer a **password-checker** found in the same repository as the **basics** program[4]. Start with the tools that yield the most results for the least effort. Only start staring at disassembly, CFGs and debuggers once you have a fairly good idea what the program is doing. Feel free to contact me[5] if you have found the solution for the **password-checker** or if you want pointers to more exercise material. Good luck and happy reversing!

[3] https://radare.gitbooks.io/radare2book/

[4] https://github.com/sebastiaangroot/binary-reversing-101

[5] sebastiaan.groot@gmail.com | sebastiaan.groot@kpn.com



Hacker disclosed 4 new Microsoft zero-day exploits in last 24 hour

MI5 slapped on the wrist for 'serious' surveillance data breach

Terrorists build Wi-Fi bombs to dodge cops' cellphone jammers

Post-quantum cryptography: An update on the NIST competition

Andreas Hülsing, Eindhoven University of Technology

The 2nd round of NIST's post-quantum cryptography standardization competition is well underway. After a call for post-quantum systems for public-key encryption and digital signatures published by National Institute of Standards (NIST) in December 2016, the competition started in December 2017 with 69 "complete and proper" submissions. Since then the field has been reduced to 26 proposals (of which 12 are with involvement from the Netherlands).

Round 1

During the first three weeks of the competition, 12 proposals got entirely broken or significantly harmed. During the next three months the frequency of new attacks slowed down significantly, and only 4 further proposals got attacked. In total, five proposals got withdrawn by the authors, and another 13 got rejected by NIST due to a lack of "full confidence in the security of" the proposals. The most common reason for attacks was the use of new, unstudied security assumptions.

The remaining attacks were enabled by overly aggressive parameter choices, and general design flaws. The unharmed proposals follow a common scheme: All of them are variants of previously known designs from the literature. For public-key encryption, the 35 proposals can be grouped into variants of about 9 general designs. For signature schemes, the 13 proposals follow 7 designs. NIST urged teams of similar proposals to merge their submissions, which lead to 4 merged submissions of 9 original proposals. Out of the remaining schemes, NIST picked the most promising candidates out of very similar proposals. This resulted in a final selection of 17 proposals for public-key encryption, and 9 proposals for digital signatures that still cover the same amount of different general designs as the 48 unharmed schemes.

The final list of 26 proposals that moved on to the 2nd round was published in January 2019. It preserved the variety of ideas while reducing the number of targets for security evaluation and implementations.

Round 2

In the 1st round, the main selection criterion was mathematical security of the proposals. At the end of the 1st round, several proposals did not yet have optimized software implementations. With the beginning of the 2nd round, the criteria also include performance in software and hardware. By now, most 2nd round candidates have optimized software implementations and most of them are constant-time, protecting against software-side-channels. Benchmarks are available for all schemes in SUPERCOP[1], libraries with less coverage that support benchmarking are provided by the Open Quantum Safe[2], and the PQCRYPTO[3] projects. For hardware and microcontroller implementations, the situation is moving somewhat slower. The pqm4[4] project provides benchmarks for several of the 2nd round candidates but a complete comparison is still lacking. Results regarding performance on reconfigurable hardware so far are limited to case studies that compare a few schemes.

The road from here

The ongoing 2nd round of the competition is supposed to run till roughly mid-2020. It will be followed by a last, 3rd round that is supposed to result in the publication of draft standards in 2022. In parallel, NIST is planning to adopt stateful hash-based signatures which were excluded from the competition as their API differs from that of regular signatures. A special publication covering XMSS (RFC 8391), and LMS (RFC 8554) are planned for late 2019.

At the 2nd NIST Post Quantum Crypto (PQC) Standardization Workshop, held in August 2019, NIST asked for feedback on the idea to speed-up the process. NIST suggested to already select a few schemes for standardization and continue with a 3rd round for the remaining schemes. This might be interpreted as an expression of confidence in at least a few of the existing proposals. It might also be an expression of industry pressure and the fear of being overtaken by other standardization bodies but this seems less likely as main standardization bodies including IETF and ISO declared the intention to wait for the NIST process to finish. However, the community clearly declared that it considers a 3rd round necessary.

Open questions

The 2nd NIST PQC Standardization Workshop was the time for the community to reflect on the ongoing competition. Devastating new attacks were not found for about a year, performance numbers are known, at least for software, and NIST was considering to take a shortcut from the competition. So, why take another delay of about 1.5 years? Given that large-scale quantum computers will be able to break all encrypted data that gets collected today this might feel like a gamble.
The first and foremost reason for the community opinion was that experience showed that

> "we get one shot at doing this right".

It is extremely unlikely that industry can be convinced to switch cryptographic algorithms twice in a short period of time. Hence, it is important to handle the open questions that came up during the first 1.5 years of the competition in a satisfactory way. Two of them are worth highlighting.

Verifiability of security claims

While it was not strictly required, NIST motivated submitters to support their proposal by a "proof of security". In public-key cryptography, a proof of security is not an absolute security statement but it relates the security of the scheme to the hardness of a mathematical problem. In the best case, it is shown that breaking the cryptographic scheme is as hard as solving the mathematical problem. This allows cryptanalysts to focus on analyzing the mathematical problem which is usually shared between many schemes. The NIST process demonstrated a collection of common pitfalls of this approach.

1. Proofs are written and verified (if at all) by humans who make mistakes. A false proof is no proof.
2. Sometimes, designers fail to relate the security to the most common, and hence well studied, mathematical problems, and resort to make assumptions about less studied mathematical problems. If these problems turn out to be easy, the proven statement is void.
3. Some proofs do not demonstrate a tight relation between the security of the scheme and the hardness of the problem. Instead they prove that breaking the scheme is easier than solving the mathematical problem by at most some factor. If the factor is too large, such non-tight proofs also just prove a void statement for actual parameters.
4. Finally, proofs are given in mathematical models that define the goal and capabilities of an attacker. Some proofs are given in models which do not cover the intended application of the scheme. In this case, the proven statement is void for that application of the scheme.

[1] https://bench.cr.yp.to

[2] https://openquantumsafe.org/

[3] http://libpqcrypto.org/

[4] https://github.com/mupq/pqm4

Nansh0u campaign compromises over 50,000 publicly available databases

Almost a million vulnerable RDP servers exposed on the internet

HiddenWasp seizes control of Linux systems

For most discovered instances of these issues within the NIST process, it was possible to recover a proof of a meaningful statement. However, not all issues are fixed yet and it is unlikely that all mistakes are caught. Especially non-tight proofs are often assumed to be an artifact of the known proof techniques.

Replacing non-tight proofs by tight proofs is subject of ongoing research. In addition, new efforts to support verification are required. Work on modularization of proofs is important to ease manual verification. Another promising approach is the use of computer-verified proofs. However, existing tools are still an area of ongoing research and do not support proofs for a post-quantum setting yet.

Application Integration

The cryptographic building blocks targeted by the NIST competition differ from the ones used today in two ways.

1. Performance: Post-quantum cryptography has worse performance than the public-key schemes used today. Even if some schemes get close to the performance of today's schemes in some metric (e.g., speed), they are off by a lot in others (e.g., size). This also widens the gap between the performance of secret-key and public-key cryptography.
2. API: Today, a cryptographer's duct tape is the Diffie-Hellman key exchange (DH). The properties of DH are so far almost unique: DH allows to compute a shared secret for two parties that know each other's public-key without any interaction. The only (conjectured) post-quantum scheme with this property is CSIDH[5], which was proposed after the start of the competition and is too new to be considered for practical application. Consequently, NIST decided to standardize key encapsulation mechanisms (KEM) instead of key exchange protocols (KE). In principle, KEMs can be used to construct KE at the cost of added interaction.

This change in characteristics requires to redesign applications for the post-quantum setting. On the one hand, it is worth reassessing if all uses of public-key cryptography in an application are strictly necessary or if we can replace some of them by secret-key cryptography. On the other hand, we have to develop new versions of our applications and protocols that can deal with the new sizes and can be instantiated with a KEM instead of DH. This is especially relevant for modern, post-compromise secure communication protocols like the Signal protocol or Wireguard which right now are inherently using DH.

In addition to the changed characteristics, most proposals are still young compared to today's schemes. Hence, it is worthwhile to think about hybrid versions of protocols that make use of a combination of today's schemes and post-quantum cryptographic schemes.

[5] https://csidh.isogeny.org/

June

3 Hell-thcare hackers break into database of 20m medical test biz patients

3 GandCrab ransomware shutters its operations

5

6 A botnet is brute-forcing over 1.5 million RDP servers all over the world

6 Backdoor found in four smartphone models; 20,000 users infected

Dear CISO: Grow with your organisation
Don’t be just the gatekeeper, be an accelerator

Anne-Sophie Teunissen, Jeroen Willemsen, Xebia Security

DevSecOps! Shift left! These are terms you hear on stage, read in articles, and see in the media. Embedding security in your DevOps strategy starts with a strong collaboration between the security team and the engineering teams. After all: security is the responsibility of everybody. So far so good. But what does this mean? What should you do in your organisation? To get security right, we see at least three focus areas that need your attention as a security professional: *risk appetite, security knowledge,* and *security culture*. The recommendations for each of these focus areas will differ depending on where the organisation is in its journey. In this article we look at the focus areas for a start-up, a scale-up and an enterprise.

The Focus Areas

Let’s start with *risk appetite*: there are various definitions for risk appetite, but it basically boils down to: how much risk do you want to accept as an organisation in order to create value. The higher the risk appetite, the more risk you are willing to take to create the value you persuade as an organisation. Risk appetite can vary per area: you can have a very low risk appetite when it comes to public image (e.g. being marketed as a secure partner to collaborate with), but a high risk appetite when it comes to how you craft your products (e.g. work on functions only, and no security checks).

Next up is *security knowledge*, the body of knowledge required to secure the IT of the organisation. It comprises the various fields required to safely develop, deploy and run the IT stack used by the organisation. This includes various activities, such as creating architecture definitions, threat modelling, defensive programming, (continuous) security validation, vulnerability verification, monitoring, and executing compliancy processes.

Last is *security culture*. This goes beyond the security awareness program. It is about taking ownership of the product that the organisation builds, deploys and operates. Ownership comes with a sense of responsibility. This responsibility includes a need for employees to be aware, vigilant, and take security as serious as the risk appetite requires. Another facet of this focus area is trust. For every member of the organisation, the same questions are relevant: do you trust that others take ownership and responsibility for security as well? Do you trust others to have operational excellence? And can you trust others when you share security issues?

Trust and a sense of belonging are closely connected. A well-functioning team, which engineers want to be part of, builds on trust, which then contributes to a culture of feedback and transparency. This greatly benefits the security practice. After all, an open culture helps to identify threats early on and to recognize security incidents faster.

Start-up!

When you are a start-up, there is often one goal: survive and grow. Whether you have a focus on getting a product out and capital in, or on getting your first chunk of market share: you will have a risk appetite which is relatively high. The primary worry is not about detecting and fixing every security vulnerability, it is about showing the value of the product that you are developing. In this stage we recommend focussing on the low-hanging fruit. For starters, get threat modelling off the ground and make sure you can fix your high-risk issues first. Next, create your core security building blocks, such as an authentication & authorization setup, and data encryption controls. Don't spend time on defence-in-depth controls that hardly reduce risks. Once you got the right investors on board to grow, you can start hardening the product more.

Having the necessary security knowledge is key. We often see that the lead-developers and tech-savvy platform engineers have some basic security knowledge. This initially might be enough, but a security knowledgeable colleague can add a lot of value to the team, if they help developing the product further. This makes them the ideal start-up's security champion, who is eager to help the engineers in order to get somewhere fast.

The culture of a successful start-up is often filled with pride and ownership. This means that engineers will want to tackle the security challenges as part of what they do. Equally important is the mutual trust in such case: making sure that people can trust each other's knowledge and that transparency prevails over politics.

We recommend to "first have business to secure, then secure that business". Start with big blocks, and don't mitigate every small risk before the idea behind the start-up comes to fruition. Unless the security of your product is one of the main selling points, of course.

Scale-up!

When you are a scale-up, the main goal is: get more sustainable. Grow features, show your value, get more customers, challenge and take-over the market. Given that you are now present and visible in the market and have more to lose, your risk-appetite might decrease. What are you willing to risk? How will this impact your growth? Risk appetite will vary given the sector you operate in and the investors you operate with. But in the end, you will have to keep taking risks to continue growth. Those risks should not get too big though, so it is time to further invest in your risk management processes to keep an overview of all the information risks. Unlike for start-ups, it becomes key to focus on lower risk issues as well. Given the increase of the amount of IT components in the organisation, simplifying life-cycle management activities is key. This means that teams will have to follow sane rules of creating and maintaining IT components without too many manual interventions or inherent high risks.

While your organisation grows, so does the challenge of getting the right spread of security knowledge across your organisation. At this point you might want to consider investing in automation and standardisation of best practices.

Often a cure-all is hoped for by creating a security team. The security team should focus on helping the engineers forward: spread the knowledge, train people, raise security champions, and support engineering teams to become more self-sustainable. This enables them to do secure development, do threat modelling, and maintain a security pipeline. Is something high risk? Support in every step of the way when it comes to designing and implementing security controls. Don't be "just" the gatekeeper, be an accelerator. Obviously, at some point you will need to invest in some form of an oversight function. But in the early phases of your scale-up it is more important to grow a security community and start an educational program.

One underestimated challenge when it comes to the security culture, is getting the scale-up through the growth spurt. Throughout this process you need to make sure that teams don't lose their sense of ownership, so that they will take the end-to-end responsibility for the security of the product seriously. Given this growth spurt, mutual trust can be under pressure as well. For instance, senior teams might wonder whether the newly introduced engineering teams take care of the quality of the products equally well. Another example can be found in "us" versus "them" situations, between the engineering teams and the security team.

We recommend investing in creating a secure base for the product the organisation makes. Automate your security testing, foster champions, share knowledge, and make sure that teams experience ownership.

Enterprise & Government

When you are an enterprise *or* government organisation, more is at stake, because you are a well-established name in the market. Similarly, the stakes rise when you have a big responsibility for society as an

June
19
20
21

Google and Cloudfare test post quantum cryptography for TLS

Critical actively exploited WebLogic flaw patched CVE-2019-2729

KPN and QuTech join forces to make quantum internet a reality organisation. You may have more to lose if something goes wrong, so the risk appetite of your organisation lowers in comparison to the scale-up. This also has an impact on how you handle security but does not mean a culture of *better safe than sorry* is the ideal approach. Making a set of heavy-duty security controls mandatory for every part of the organisation does not always make sense. For example, requiring a pentest on every change of a static website hosting the lunch menu of the canteen. The trick is to strike a balance. Your organisation especially benefits from identifying information risks in the IT-stack and methods such as threat modelling are still of great value. It helps engineering teams to apply enough security. Enough security evolves around questions such as "Do I need to solve this vulnerability?" and "What is the risk if not doing so?". And, it eventually gives the second line (and third line) of defence insight on whether decisions are in line with the existing risk appetite.

When organisations get bigger, it is tempting to let security knowledge become a thing of the security team. It is quite difficult to bring the right level of security knowledge to an ever growing and changing workforce. Wouldn't it be convenient if a centralized team of security specialists has all the knowledge to help out the rest of the organisation? The answer is no. The danger which rises here, is that a centralized security team cannot keep up with the engineering teams, and therefore slows down the development process. Instead, invest in role-based security awareness and knowledge, from developers to product owners to helpdesk employees.

As for the security culture: when evolving to a reality where the security team is primarily responsible, the ivory tower is lurking. This creates the friction between security and engineering teams that so many organisations currently experience. Our advice would be: learn from the scale-up. Create an environment where the engineering teams have enough security capabilities – with or without the support of local information security specialists – and the centralized security team is able to advise on risk mitigation and at the same time perform their reporting role as a second line of defence.

We recommend investing in the trust between the security team(s) and engineering teams. And, at the same time keep building on creating a secure base.

While your organisation grows, you will go through various transformations and adopt new processes as well as new technologies. Each of these will change your way of working. Each of these changes offers an opportunity for you as a CISO / security professional to grow and strengthen your bond with the organisation. This can help you to tackle security the best way possible: together.

June
24
25
26
27

Raspberry Pi used to steal data from NASA lab

New Silex malware is bricking IoT devices, has scary plans

Account takeover vulnerability found in popular EA games origin platform

Welcome Spelevo: New exploit kit full of old tricks

Securing Internet Routing with RPKI

Alex Band, NLnet Labs

The protocols that make the core of the Internet work have proven to be incredibly robust and scale very well, so over the last decades there has never been a need to radically change them. The result is that the Internet we use today is largely based on technologies designed between the 70s and the early 90s of the last century; a time when security wasn't really on anyone's mind.

When looking up a domain name using the Domain Name System (DNS), there's no real certainty that the IP address you receive in return is the correct one. When packets are routed along the Internet using the Border Gateway Protocol (BGP), there's no way to know for sure they are coming from a legitimate origin or haven't been hijacked along the way.

We could consider changing the protocols that make up the core of the Internet to new ones that have security built in, but making this happen is like rebuilding an airplane while it's flying. That's why operators and researchers generally propose to add a security layer on top the existing protocol, allowing for gradual adoption. For the DNS, this has resulted in DNSSEC, which ensures that the IP address you receive in response to your query has not been tampered with by adding a digital signature.

To understand how routing can be secured, we first need to take a step back and look at the numbers that make the system work...

Connecting the Numbers

The global routing system of the Internet consists of a number of functionally independent networks called autonomous systems (ASs), which are each identified by a unique AS Number. From these networks, they route IPv4 and IPv6 address blocks.

The Internet Assigned Numbers Authority (IANA) has authority over all number spaces used in the Internet, including IP address space and AS Numbers.

July

3 First-ever malware strain spotted abusing new DoH (DNS of HTTPS) protocol

4 Sodinokibi ransomware exploits windows bug to elevate privileges

11 Magecart group compromises 17,000 domains by overwriting Amazon S3 buckets

11 Sea Turtle hackers head to the Mediterranean, snag Greece's TLD registrar as a souvenir

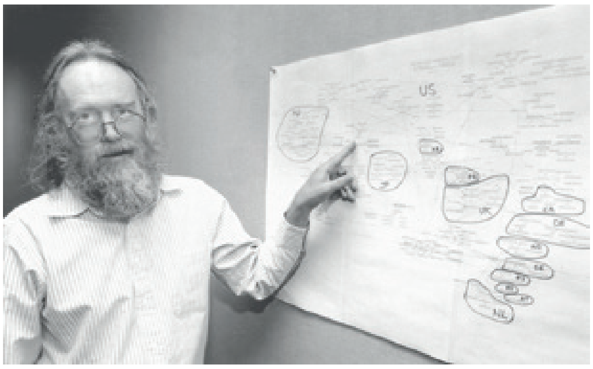


Figure 1: John Postel in 1994, with a map of Internet top-level domains

The IANA function started out with just one man, John Postel, but was eventually formalised in an organisation which allocates public Internet address space to five Regional Internet Registries (RIRs). In turn, these RIRs allocate to National or Local Internet Registries (NIRs and LIRs), who then assign to customers and end-users.

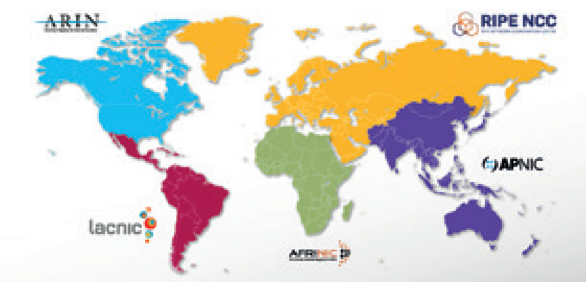


Figure 2: The service regions of the five Regional Internet Registries

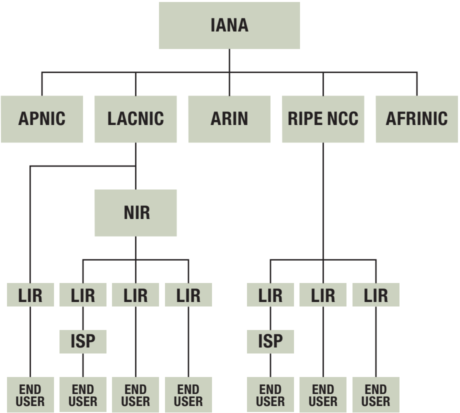


Figure 3: Internet number resource allocation hierarchy

This hierarchy ensures globally unique registration of Internet numbers, so that anyone can verify that for example the RIPE NCC attests that KPN has the right to use the AS Number 286 and one of their IP ranges is 134.222.0.0 – 134.222.255.255. This registration data is a great starting point to establish who is authorised to route specific address space on the Internet.

Internet Routing

The Border Gateway Protocol (BGP) is used to exchange routing information between autonomous systems. The current version, BGP4, has been in use on the Internet since 1995. Globally, there are now more than 66,000 active autonomous systems that announce around 800,000 IP ranges, also known as prefixes.

When a network operator configures their border routers, they specify which IP address blocks to originate and announce to their peers. There is no authentication or authorisation embedded within BGP, which means they can announce any prefix, also one they don't have the right to originate.

As a result, routing incidents occur every day, if only because the numbers on the keyboard are really close together. While several decades ago outages and redirections were often accidental, in recent years they have become more malicious in nature. Some notable events Pakistan's attempt to block YouTube access within their country, which resulted in taking down YouTube entirely in 2008, and more recently, the almost 1,300 addresses for Amazon Route 53 that got rerouted for two hours in order to steal cryptocurrency, in 2018.

Since the 1990s, network operators have employed the Internet Routing Registry (IRR) to establish a tighter coupling between what operators intend to route, and what is actually seen in BGP. The IRR is a distributed set of databases and some, but certainly not all of them, are operated by the authoritative Regional Internet Registries.

The result is that out of all the information on routing intent that is published, it is difficult to determine what is legitimate, authentic data and what isn't. This sparked the development of the new standards in the Secure Inter-Domain Routing (SIDR) Working Group of the Internet Engineering Task Force (IETF). These efforts resulted in what is now standardised as Resource Public Key Infrastructure (RPKI).

First GDPR fine in the Netherlands imposed: EUR 460,000

July

15

Meet Extenbro, a new DNS-changer Trojan protecting adware

16

Phishers target Office 365 admins with fake admin alerts

Route Origin Validation with RPKI

Resource Public Key Infrastructure (RPKI) proves the association between specific IP address blocks or ASNs and the holders of those Internet number resources. The certificates are proof of the resource holder's right of use of their resources and can be validated cryptographically.

Most importantly, the certificate structure in RPKI mirrors the way in which Internet number resources are distributed. The RIRs act as a trusted Certificate Authority (CA) and issue certificates to resource holders. Certificate Authorities verify that the public key in the generated certificate is the public key of the identified party.

RPKI provides a set of building blocks allowing for various levels of protection of the routing system. The initial goal is to provide route origin validation, offering a steppingstone to providing validation of the entire path in the future. Now, the legitimate holder of a block of IP addresses can make an authoritative, signed statement about which autonomous system is authorised to originate their prefix in BGP. These statements are called Route Origin Authorisations (ROAs).

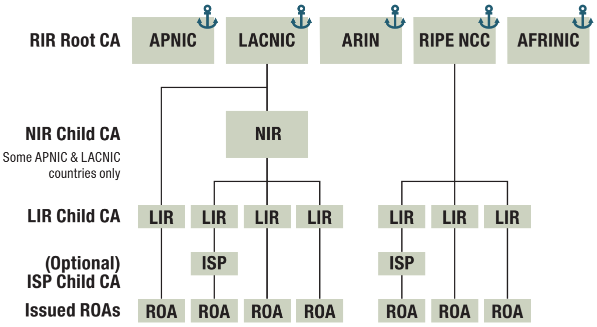


Figure 4: RPKI Certificate Authority hierarchy

When a network operator creates a ROA for a certain combination of origin AS and prefix, this will have an effect on the RPKI validity of one or more route announcements. Once a ROA is validated, the resulting object contains an IP prefix, a maximum prefix length, and an origin AS number.

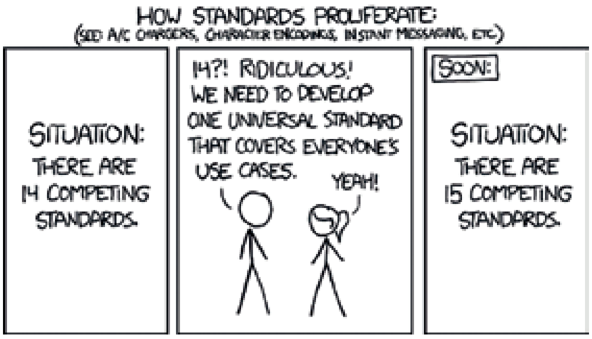
When comparing these statements to route announcements seen in BGP, you can have three possible outcomes:

- **Valid**
  - The route announcement matches with a ROA that was published by the holder of the IP address block.
- **Invalid**
  - The prefix is announced from an unauthorised AS, or the announcement is more specific than is allowed by the ROA.
- **NotFound**
  - The prefix in this announcement is not, or only partially covered by a ROA.

Based on these three states, other network operators can now reliably set up filters to only accept traffic from legitimate, authorised origins. But is that really happening?

RPKI in the Real World

Since the 1990s we've known that we were going to run out of IPv4 addresses, giving us more than enough time to transition to an alternative numbering scheme. We knew there was a problem and just look where we are now with IPv6 adoption...



HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Figure 5: https://xkcd.com/927/

In this light, the Internet community was curious to see how RPKI would be adopted, because it suffers from a chicken-and-egg problem: why set up filters based on RPKI when there are no ROAs, and why set up ROAs when nobody is using RPKI-based filtering. Then there's also cryptography involved in RPKI... Can't we just fix the IRR and call it a day?

Critical flaws found in VxWorks RTOS that powers over 2 billion devices

July 17 18 29

Dutch police arrest suspected hacker behind Rubella and Dryad malware

Slack resets passwords for users who hadn't changed it since 2015 breach

To see how RPKI could be done successfully, perhaps the adoption of free Let's Encrypt HTTPS certificates is a good example: make it as painless and cheap as possible for people to adopt it and offer a tangible benefit.

The five RIRs started offering a free, hosted RPKI service for their members in January of 2011. The strategy was to take away the crypto burden from the users, so that they could just focus on creating ROAs to declare their routing intent. The reasoning was that once there was a large enough pool of high quality, well-maintained data, the value of using it for filtering would emerge automatically.

In the last two years, this strategy started paying dividends when, after a high-profile hijack of Amazon Route 53, cloud provider Cloudflare threw their weight behind RPKI by announcing that they would start dropping routes with an RPKI invalid state. Soon after, AT&T and Telia Carrier announced they were doing the same. Around the same time, a variety of smaller and larger operators in the Netherlands, including SURFnet and KPN, started to aggressively adopt RPKI based origin validation, making them global front runners in the use of the technology.

In November of 2019, the RIPE NCC passed a milestone of reaching 10,000 issued RPKI certificates, well over 40% of their membership in just 8 years. In Internet terms, that is a massive adoption rate, which can be attributed to a one-click setup of a CA, painless ROA management and relentless training and outreach.

NLnet Labs has been able to contribute to this technology by developing a free, open source software toolset for managing and publishing ROAs, as well as software to validate RPKI data and push the processed information to routers. In addition, various research projects have emerged from these efforts, helping the Internet community get a better understanding of the real-world impact of the technology.

RPKI has well and truly taken off and Internet routing is getting more secure every day.

DHS warns small airplanes
vulnerable to flight data
manipulation attacks

July 30 31

Google researchers
disclose vulnerabilities for
'interactionless' iOS attacks

Reducing risk by resolving conflicts between security and DevOps

Laurens van Dijk, Sergey Panfilov, KPN

New software development methodologies have significantly increased the frequency and reduced the latency of software delivery over the past few years. The most advanced practitioners are capable to deliver changes to a production environment within the hour, dozens of times per day[1]. This unprecedented speed of software delivery creates both challenges and opportunities for traditional approaches to information security. In this article, we'd like to offer some insights and advice on the incorporation of security as a component into software development processes.

Agile software development and DevOps

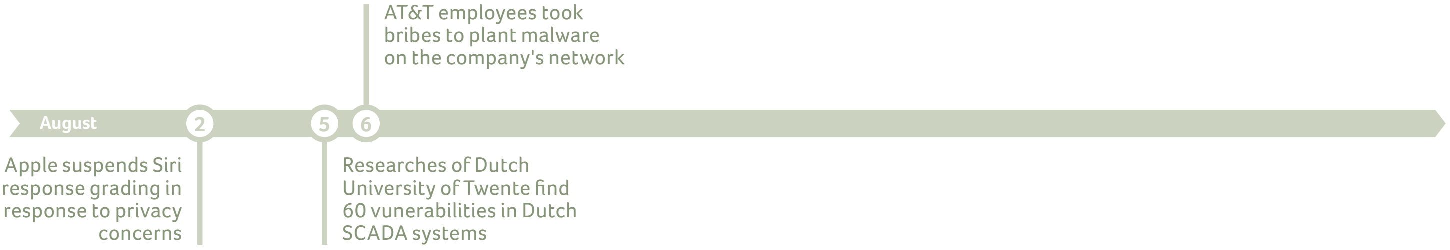
Agile software development has gained tremendous popularity since publication of the Agile manifesto in 2001 and is widely considered as mainstream nowadays[2]. It addresses the rigidity and difficulties in adapting to external changes halfway through a project, associated with the waterfall approach to software development. This paradigm for development of software is characterized by the focus on delivery of the valuable and working software to the customers in short iterations, embracing changes in business requirements at any stage of development process, encourages close collaboration of the people involved in development of the software[3].

However, development teams working according to Agile ran into another problem: Operations teams, traditionally responsible for delivery and maintenance of software, could not keep up with the pace of software production by Agile development teams. DevOps takes off where Agile stops and extends the core principles of Agile to the tasks that would traditionally be performed

[1] Forsgren, N., Smith, D., Humble, J., Frazelle, J. (2019). 2019 Accelerate State of DevOps Report.

[2] Martin Fowler, The State of Agile Software in 2018, https://martinfowler.com/articles/agile-aus-2018.html

[3] Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J. & Thomas, D. (2001). Manifesto for Agile Software Development


August
2
5
6
AT&T employees took bribes to plant malware on the company's network
Apple suspends Siri response grading in response to privacy concerns
Researches of Dutch University of Twente find 60 vunerabilities in Dutch SCADA systems

by operations teams separated from development teams. By integrating and automating operational tasks in the Software Development Lifecycle, DevOps enables agile delivery of software.

The conflict between Information Security and DevOps

The original focus of DevOps has been mainly on development and operations tasks, leaving out many information security aspects important to software development. That work is usually performed by a separate (information) security team. A traditional approach to information security relies on the use of security policies, manual processes for verification of compliance, and incident response. Quite like how traditional operations teams are often unable to keep up with the speed of Agile development teams, these traditional security teams are now finding themselves unable to keep up with the rapid speed at which a well-functioning DevOps-team can deliver software.

It first starts with the security policies getting out of date faster, due to the rate of changes in business- and technology landscapes. These policies then become a bottleneck for introduction of new technology solutions to support new business requirements. The use of 'quality gates' with a manual verification of compliance to the policies before release of new software leads to an increasing backlog of projects waiting for security tests. Security testing in the later stages of software development often reveals blocking vulnerability findings, preventing release of software changes, because of the unexpected work related to mitigating these security vulnerabilities. All these issues increase the lead time to the market and negatively affect the business of a company.

Improving security adaptation in DevOps

Integration of security within DevOps is the logical next step in DevOps evolution. This is acknowledged in the 2019 State of DevOps report by Puppet[4].

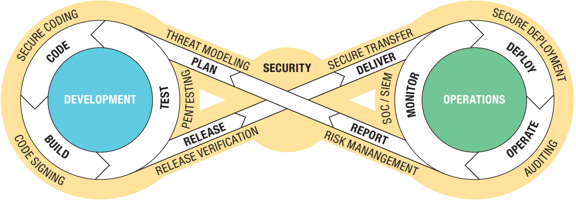


Figure 1: Secure DevOps lifecycle

Figure 1: shows the DevOps lifecycle with integrated security.

The lifecycle begins with collaboration of security and development teams on threat models during the planning phase. Threat modelling at the early stage gives an opportunity for implementation of solutions, which are truly secure by design. It helps to determine relevant security policies and plan implementation of required security controls, written as security requirements. Threat modelling may also reveal the gaps in security policies, which need to be addressed in order to be able to proceed with chosen software design. That requires the change in governance of security policies, so it becomes Agile as software development processes.

Security requirements (functional and non-functional) created at design stage need to be prioritised as part of the product backlog, so they are taken into development. That gives an opportunity for implementation of automated verification of security policy compliance, using "Compliance as a Code" principles and integrating automated security tests in software development pipeline at the "code" and "build" stages. Other security tools, such as Static Application Security Testing (SAST) analysers and vulnerability scanners, can help to discover vulnerabilities at the early development stages and improve the security posture of software being developed.

Integration of security tools in the development and automated security testing provides new control mechanisms for security experts, who can focus on evaluation of automated security tests and review changes only in high-risk areas of the code. That does not mean there is no place for manual security testing anymore. The role of penetration testing in DevOps needs to change from a mandatory release tailgate to continuous security testing performed in parallel to DevOps lifecycle management and focused on the most important security aspects.

Conclusion

Using an Agile or DevOps methodology in software development at your company can result in a greater rate of software delivery and rapid value creation. However, methodologies such as DevOps create challenges for organisations and security specialists used to a traditional way of managing information security. A large fraction of software development teams at KPN have been migrating to working according to Agile/DevOps. The next important near-future goal for KPN will be enabling DevOps teams to also incorporate security in their workflows. Incorporating security as part of the development process will allow us to simultaneously deliver value to customers at a rapid pace, while also increasing the security level of our products to an even higher standard.

[4] Mann, A., Brown, A., Stahnke, M., Kersten, N. 2019 State of DevOps Report, https://puppet.com/resources/report/state-of-devops-report/

Windows 10 security
alert: Vulnerabilities
found in over 40 drivers

August 7 8 10

Microsoft contractors
are listening in on Skype
translation calls

Researcher finds security
bugs in exposed
Boeing 787 software

Will quantum computers break the Bitcoin blockchain?

Itam Barmes, Bram Bosch, Deloitte

Quantum computers hold promise to break practically all public-key cryptography that is used today. Since Google announced its achievement of "quantum supremacy", there have been many claims predicting the demise of currently used cryptography in general, and Bitcoin in particular. In this article we will explain how serious the threat is and what can be done about it.

The main focus of this article will be to answer the following questions:

1. How many Bitcoins could be stolen now if sufficiently large quantum computers were available?
2. What can one do to mitigate the risk of Bitcoins being stolen by an adversary with a quantum computer?
3. Is the Bitcoin blockchain inherently resilient to quantum attacks now and in the future?

Quantum computers and cryptography

In asymmetric cryptography, a private-public key pair is generated in such a manner that the two keys have a mathematical relation between them. As the name suggests, the private key is kept as secret, while the public key is made publicly available. The security of asymmetric cryptography is based on the fact that the public key can be derived from the private key, but not the other way around. All known (classical) algorithms to derive the private key from the public key require an astronomical amount of time to perform such a computation and are therefore not practical. However, in 1994, the mathematician Peter Shor published a quantum algorithm that can break the security assumption of asymmetric cryptography. Anyone with a sufficiently large quantum computer could use this algorithm to derive a private key from its corresponding public key.

Bitcoin 101

Bitcoin is a decentralized system for transferring value. Unlike the banking system where it is the responsibility of a bank to provide customers with a bank account, a Bitcoin user is responsible for generating their own (random) address. By means of a simple procedure, the user's computer calculates a random private-public key pair and a Bitcoin address that is mathematically

New HTTP/2 flaws expose unpatched web servers to DoS attacksv

August

13

Microsoft warns of two new 'wormable' flaws in Windows Remote Desktop Services

New Bluetooth KNOB attack lets attackers manipulate traffic

> In the Bitcoin network, the decision of which transactions are accepted into the network is ultimately left to the so-called miners.

related to these keys. The use of the private key is required in order to perform transactions from this address.

Moving Bitcoins from one address to another is called a transaction. Such a transaction is similar to sending money from one bank account to another. In Bitcoin, the sender must authorize their transaction by providing a digital signature that proves they own the address where the funds are stored. Remember: someone with an operational quantum computer who has your public key could falsify this signature, and therefore potentially spend anyone's Bitcoins.

In the Bitcoin network, the decision of which transactions are accepted into the network is ultimately left to the so-called *miners*. Miners compete in a race to process the next batch of transactions, also called a *block*. Whoever wins the race, is allowed to construct the next block, awarding them new coins as they do so. Bitcoin blocks are linked to each other in a sequential manner. Together, they form a chain of blocks, also called the "blockchain".

The victorious miner who creates a new block, is free to include whichever transaction they wish. Other miners express their agreement by building on top of blocks they agree with. In case of a disagreement, they will build on the most recently accepted block. In other words, if a rogue miner attempts to construct an invalid block, honest miners will ignore the invalid block and build on top of the most recent valid block instead.

Address types

When discussing Bitcoin transactions, we need to distinguish between two address types (there are more than 2 address types, but they are less relevant for the present discussion). In the first type the address to which the Bitcoins are transferred is the exact value of the public key. Such a transaction is called 'pay to public key' (p2pk). Bitcoins stored in such addresses are inherently vulnerable to a quantum attack as an adversary could derive the private key from the address and then transfer the Bitcoins to their own address.

In the second type of transaction, the address of the recipient is composed of a hash of the public key. The first and most popular implementation of this is called 'pay to public key hash' (p2pkh). As a hash is a one-way cryptographic function, the public key is not directly revealed by the address. The public key is only revealed at the moment when the owner wishes to initiate a transaction. This means that as long as funds have never been transferred from a p2pkh address, the public key of that address is not known. Thus, the private key cannot be derived using a quantum computer. However, if funds have ever been transferred from a specific p2pkh address (no matter what amount), the public key is revealed. From that moment on, this address is marked "used" and should ideally not be used again to receive new coins. In fact, many wallets are programmed to avoid address reuse as best they can. Avoiding the reuse of addresses is considered best practice for Bitcoin users, but you would be surprised how many people do not take this advice to heart. More on that in the following chapter.

How many Bitcoins could be stolen now if sufficiently large quantum computers were available?

Imagine that someone manages to build a quantum computer today and is therefore able to derive private keys. How many Bitcoins will be in danger?

To answer this question, we analysed the entire Bitcoin blockchain to identify which coins are vulnerable to a quantum attack. As explained in the previous section, all coins in p2pk addresses and reused p2pkh addresses are vulnerable to such an attack. Our analysis reveals that there are circa 2 million Bitcoins in p2pk addresses. These Bitcoins have not been moved for many years, and it is a reasonable assumption that these coins were generated through mining during the first year of Bitcoin's existence. Furthermore, there are about 2.5

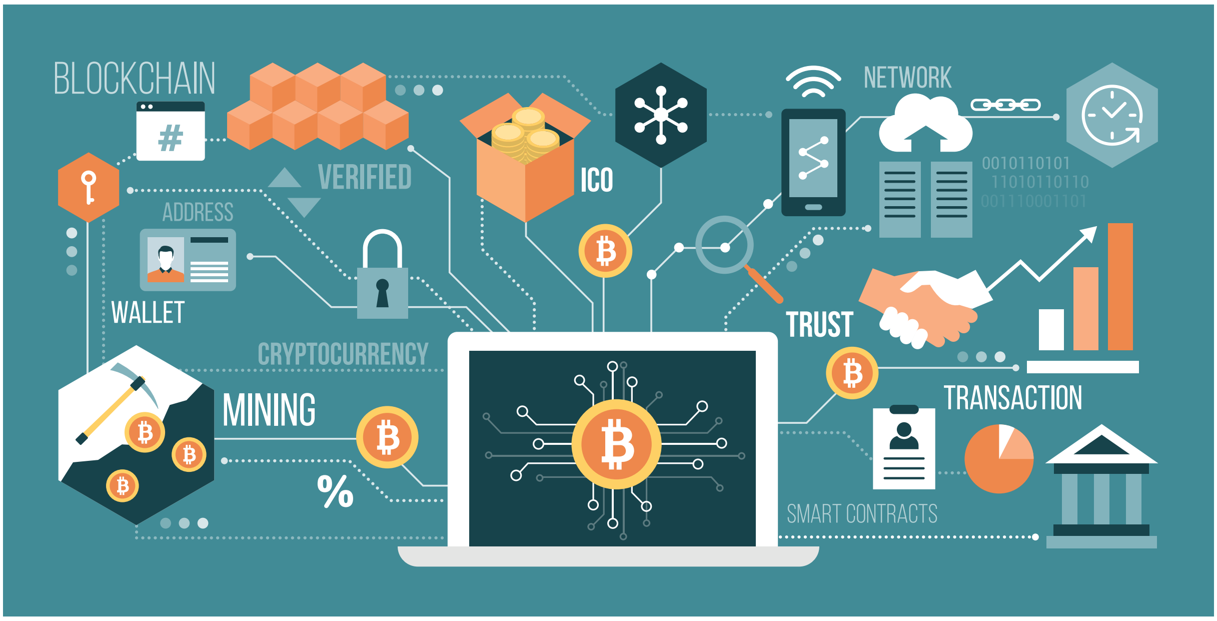
August

16 Confidential company documents exposed in public sandboxes

20 Nearly two dozen Texas towns targeted by tiresome ransomware

20 Severe flaws in Kubernetes expose all servers to DoS Attacks

21 Proof of concept available for arbitrary file disclosure in pulse connect



million Bitcoins in reused p2pkh addresses. Together this means that about 25% of all Bitcoins in circulation can be stolen by an adversary with a quantum computer. At the current price this is over 35 billion USD! Talk about an incentive to build such a machine.

What can one do to mitigate the risk of Bitcoins being stolen by an adversary with a quantum computer?

In the previous section we explained that p2pk and reused p2pkh addresses are vulnerable to quantum attacks. However, p2pkh addresses that have never been used to spend Bitcoins are safe, as their public keys are not yet public. This means that if you transfer your Bitcoins to a new p2pkh address, then Shor's algorithm will be ineffective against them.

The issue with this approach is that many owners of vulnerable Bitcoins have lost their private keys. These coins cannot be transferred and are waiting to be taken by the first person who manages to build a sufficiently large quantum computer. A way to address this issue is to come to a consensus within the Bitcoin community and provide an ultimatum for people to move their coins to a safe address. After a predefined period, coins in unsafe addresses would become unusable (technically, this means that miner will ignore transactions coming from these addresses). Such a drastic step needs to be considered carefully before implemented, not to mention the complexity of achieving consensus about such a sensitive issue.

Is the Bitcoin blockchain inherently resilient to quantum attacks now and in the future?

Let's assume for a minute that all owners of vulnerable Bitcoins transfer their funds to safe addresses (everyone who lost their private key 'magically' finds them). Does that mean that the Bitcoin blockchain is no longer vulnerable to quantum attacks? The answer to this question is actually not that simple. The prerequisite of being "quantum safe" is that the public key associated with this address is not public. But as we explained above, the moment you want to transfer coins from such a "safe" address, you also reveal the public key, making the address vulnerable. From that moment until your transaction is "mined", an attacker who possesses a quantum computer gets a window of opportunity to steal your coins. In such an attack, the adversary will first derive your private key from the public key and then initiate a competing transaction to their own address. They will try to get priority over the original transaction by offering a higher mining fee.

In the Bitcoin blockchain it currently takes about 10 minutes for transactions to be mined (unless the network is congested – which has happened frequently in the past). As long as it takes a quantum computer longer to derive the private key of a specific public key then the network should be safe against a quantum attack. Current scientific estimations predict that a quantum computer will take about 8 hours to derive a typical Bitcoin private key (https://arxiv.org/abs/1905.09749), which means that Bitcoin should be, in principle, resistant to quantum attacks (as long as you do not reuse addresses). However, as the field of quantum computers is still in its infancy, it is unclear how fast such a quantum computer could become in the future. If a quantum computer will ever get closer to the 10 minutes mark to derive a private key from its public key, then the Bitcoin blockchain will be inherently broken.

Closing remarks

Quantum computers are posing a serious challenge to the security of the Bitcoin blockchain. Presently, about 25% of the Bitcoins in circulation are vulnerable to a quantum attack. If you have Bitcoins in a vulnerable address and believe that progress in quantum computing is more advanced than publicly known, then you should probably transfer your coins to a new p2pkh address (don't forget to make a secure backup of your private key).

In case your own Bitcoins are safe in a new p2pkh address, you might still be impacted if many people will not (or cannot) take the same protection measures. In a situation where a large number of Bitcoins is stolen, the price will most likely crash and the confidence in the technology will be lost.

Even if everyone takes the same protection measures, quantum computers might eventually become so fast that they will undermine the Bitcoin transaction process. In this case the security of the Bitcoin blockchain will be fundamentally broken. The only solution in this case is to transition to a new type of cryptography called 'post-quantum cryptography', which is considered to be inherently resistant to quantum attacks. These types of algorithms present other challenges to the usability of blockchains and are being investigated by cryptographers around the world. We anticipate that future research into post-quantum cryptography will eventually bring the necessary change to build robust and future-proof blockchain applications.

PDF editor biz breached,
users' passwords among
stolen data

August 29 30

Google adds all
Android apps with
+100m installs to its
bug bounty program

Interdisciplinarity 2.0

What cyber security needs is true interdisciplinarity rather than the multidisciplinarity that is currently the norm.

Els de Busser, Tommy van Steen, Leiden University

Traditionally, cyber security has been considered to be an IT problem. The IT department, being located in the basement as often jokingly pointed out by cyber security specialists, was put in charge of 'sorting out' all problems relating to the computer systems of companies. Whether these were hardware problems, software bugs, or cyber security challenges did not matter, no differentiation between problems (and therefore the party responsible for the solution) occurred.

While this worked well at the time, the growing complexity of computer systems and the ever-expanding nature of cyberspace creates new issues and threats on a daily basis. As a result, the classic 'let the IT department sort it out' approach is now considered obsolete. In recent years, the call for more diverse skillsets for cyber security specialists and the conglomeration of various academic fields and backgrounds to battle the cyber security challenges of the 21st century has amplified.

In this call for more diverse skillsets, any debate seems to focus on interdisciplinarity, and the importance of bringing different fields together to work on complex cyber security dilemmas. Indeed, besides the IT-trained cyber security experts, there now are people from nearly all academic fields involved in cyber security. Judicial scholars working on the implementation of GDPR to regulate online data mining, liability questions and numerous forms of cybercrime, psychologists working on methods to battle fake news and social engineering, and international relations experts discussing how to govern the internet across borders are only a snapshot of the variety of fields working to improve the world's cyber security. Clearly, this is an improvement of the traditional view of cyber security as merely an IT problem, and it is much needed as cyberspace and the possibilities, both in positive and negative ways, of interacting online are expanding at an exponential level. However, it is not the interdisciplinarity that we are looking for, or more importantly, that we so direly need. In practice, the way various fields jumped on the cyber security topic is merely a multidisciplinary approach, where different

September

3 Popular web comic XKCD shuts down forum after hack

5 FunkyBot malware intercepts Android texts, 2FA codes

fields work on the same topic, but not together. This multidisciplinary approach to cyber security is mainly a siloed approach where scholars and practitioners from different field stay within their field to assess - and find solutions to – cyber security problems. This way, the judicial scholars often lack technical knowledge of computer systems, psychologists do not recognise the possibility of shaping online behaviour through legislation, and international relations experts ignore the intricacies of human nature.

If we have merely adopted a multidisciplinary approach rather than an interdisciplinary approach, what is the difference between these two and why would it matter? In a truly interdisciplinary approach to cyber security, experts from all relevant fields start gaining expert knowledge in other fields as well. So rather than being (just) a judicial scholar, a psychologist, or an international relations expert, each of these experts takes the time, and puts in the effort, to learn about the other fields as well. Not only gaining knowledge about the different viewpoints of these fields, but also receiving training in their field's specialists' skills to solve cyber security problems. The goal here is not to create a full 'symbiosis' where experts have equal expertise in their first field as in their second, third or even fourth field. That approach would not be feasible and in fact it would reduce the quality of the specialists as they would turn into generalists with basic knowledge about many fields. Instead, it means getting a general, clear understanding of other fields to the level that you can communicate with experts of the other fields, understand (potential) problems, and make an informed decision in jointly solving problems in addition to your own primary field.

It is essential to recognize that we all have a so-called disciplinary comfort zone. Mostly this is the first discipline we were trained in. It is a first shaping of thoughts and opinions and it is human to rely on what we know. Even those who develop further and graduate with a double degree will feel more comfortable in one discipline over the other. That discipline we feel most comfortable in tends to function as a pair of glasses through which we look at other disciplines. A pair of disciplinary glasses we may never be able to take off. This does not necessarily exclude interdisciplinarity though: one can acknowledge the disciplinary comfort zone and at the same time learn the basics of another discipline in order to gain a better understanding of cyber security questions and solutions. The software developer who never talks to the legal department of her organisation may spend numerous hours building a programme that contains inherently illegal functions that create liability issues. If she also does not engage in a conversation with psychologists, that same software may do the opposite of encouraging the users' cyber secure behaviour.

What is needed for implementing such integrated approach to cyber security? Obviously, a first step is creating awareness that this approach works, ideally with both the strategic-governance level and the operational level of organisations. That means dropping the assumption that anything starting with "cyber" is by definition an IT-dominant issue, and recognizing how multifaceted the cyber security context really is. That also means having an open mind towards unfamiliar disciplines: a willingness to recognize that your own disciplinary comfort zone is simply insufficient to solve these complex problems.

Once the mind is aware and open towards looking at other disciplines, the second step is learning from those other disciplines and using that knowledge for the benefit of a genuine joint approach. There is no need to spend years studying the complete range of a new field. What suffices is gaining understanding on how the other discipline deals with cyber security issues and then integrate it with your own where needed. This simplified explanation sounds straightforward but two important obstacles may block this integration: we call them territoriality and appropriation. Territoriality refers to the recognition that an unfamiliar discipline may help you in developing solutions for a cyber security related question, but still remaining on your own turf due to an assumed inferiority of the other discipline. You may do some reading on the other discipline, you may even find it interesting, but you still rely only on your disciplinary comfort zone to solve the problem. This is an amplified and narrow-minded version of the aforementioned disciplinary glasses. By appropriation we mean that in learning about an unfamiliar discipline, one takes it at face value. Without much in-depth study or reflection, you adopt some superficial features of the other discipline – such as terminology or methodology – and copy/paste them into your own, ignoring their context. Both territoriality and appropriation rely on a feeling of superiority of the own discipline. Genuine interdisciplinarity is the opposite. It means being able to recognize your disciplinary comfort zone while at the same time embracing unfamiliar disciplines as equal partners in a cooperative effort towards solving a complex issue. What is needed is the joining of different – at first sight unrelated – disciplines in function of the common goal, solving cyber security issues.

Training experts interdisciplinary, with a focus on creating awareness of knowledge and methods of other fields, and battling the risks of territoriality and appropriation, enables the cybersecurity specialists of the future to actually work together instead of merely divide the problem into a technical, judicial, behavioural and political aspect and asking field experts for solutions to each aspect. True interdisciplinarity is more than the sum of its parts and is required to avoid effective solutions falling between the cracks of the various fields involved in cyber security. It is by adopting an interdisciplinary approach that different fields can truly start working together, rather than just alongside each other, on battling the challenges in cyber security.

September

6

Metasploit team releases BlueKeep exploit

Flaws in over half a million GPS trackers expose children location data

7

Millions of Exim servers vulnerable to root-granting exploit

Identity is the foundation of security

Mathijs Valk, KPN

Security professionals spend the majority of their working hours repelling attacks and many measures are taken for that purpose. They tend to assign digital identity a secondary role because of this, even though proper identity management is the foundation of any security setup. There needs to be certainty that someone who accesses your digital systems actually is who they say they are and are authorized to do what they are doing. Hackers have free rein if they can misuse a digital identity effectively.

There is a strong need for further integration of security and identity. The focus currently lies on traditional methods of network security, while identity management is often treated as a separate domain. In reality, those traditional networks will cease to exist in the future. Even in the new reality, it is impossible to organize security without solid identity management. Digital boundaries are becoming blurred, so identity management is increasingly becoming the starting point for good security.

The wall and moat have disappeared

This point is best illustrated by comparing the current situation with how ICT networks were secured in the 1980's. To keep criminals at arm's length, specialists built thick walls around their networks. Requirements changed with the advent of the Internet, as administrators needed to facilitate the communication of their networks with the outside world. They created holes and entrances in their walls to allow for external systems to connect to the internal infrastructure. To thwart unauthorized access, they applied security controls to those openings. Among other things, this enabled them to give partners secure access to data and applications.

But these walls are starting to crumble, with cloud computing and digital transformation accelerating the process. The cloud means that data and applications are placed off the user's security network, on the computer systems of third parties. An increasing number of companies no longer have their 'own network', effectively meaning that the walls have disappeared. What remains is people interacting in the cloud. People who interchange data, carry out transactions and require access to systems and

September

10 Sustes malware attacking systems using Exim vulnerability

11 D-Link network gear flaw leaves passwords open for potentially whole world to see

11 VU Amsterdam researchers develop new attacks on Intel processors

> Identity can also have value to the organisation as a whole. It could play a role in protecting customer privacy or make the quality control of the supply chain more effective.

resources. You can grant such access only if you know who you are dealing with and what authorizations they have -or should have- within a system.

Unlawful access and fraud

The press regularly reports on incidents where inadequate attention to identity management resulted in security breaches. Recently, one Dutch Hospital received negative publicity for its flawed identity and access management. Unauthorized staff members accessed the electronic health record of reality star Samantha de Jong. An in-house investigation showed that around 2,800 doctors and nurses had access to all the data of all the patients who had ever been in the hospital. The Dutch Data Protection Authority called it a “serious issue” and imposed a fine on the hospital.

The consequences of CEO fraud draw regular attention as well, and this form of cybercrime could be seen as an extreme example of identity fraud. Here a person pretends to be someone else in an attempt to steal money. The hacker might, for instance, assume the identity of the managing director of the company and instruct staff members to transfer money to a bank account. There are many examples where unsuspecting victims comply with such requests.

It is also prevalent in more traditional hacking, where the attackers are after the rights of a ‘superuser’, for example, the CEO or a system administrator. Those rights allow them to move unhindered through a computer network and provide access to the company’s valuable data.

Security begins with identity

Proper organisation of identity management can limit the impact of such attacks. The first step to ascertain whether a user’s actions on a system are unauthorized, is to determine whether that user should have access in the first place. After that, the question is whether that person has the authorizations required for the activities that they are carrying out. Any such rights also need to be revocable.
Digital resilience is vital and does not only involve traditional security solutions. It also needs a broad choice from an extensive identity portfolio. Innovative identity technologies, such as self-sovereign identity, are getting more traction in for example digital government portals in the Netherlands. Access to these services is secured using the eHerkenning authentication system, allowing government bodies to deactivate their obsolete access systems and improving the level of security.

Additional security layers are Public Key Infrastructure (PKI), allowing for strong authentication, and Identity & Access Management, used to arrange authorizations such as the granting of rights and the setup of special accounts for specific users. This prevents identities and accounts from being misused.

Focus on value

To be able to deploy these solutions effectively, organisations must work towards an integral vision on digital identities. They need to ensure that the rationale for an identity project is not focused solely on – for example – compliance simply because the law so requires. It should also be much more than just a reaction to incidents. The actual risks of the organisation are relevant as well. One question would be: which roles in the organisation do I consider particularly risky and what rights do I grant in such cases?

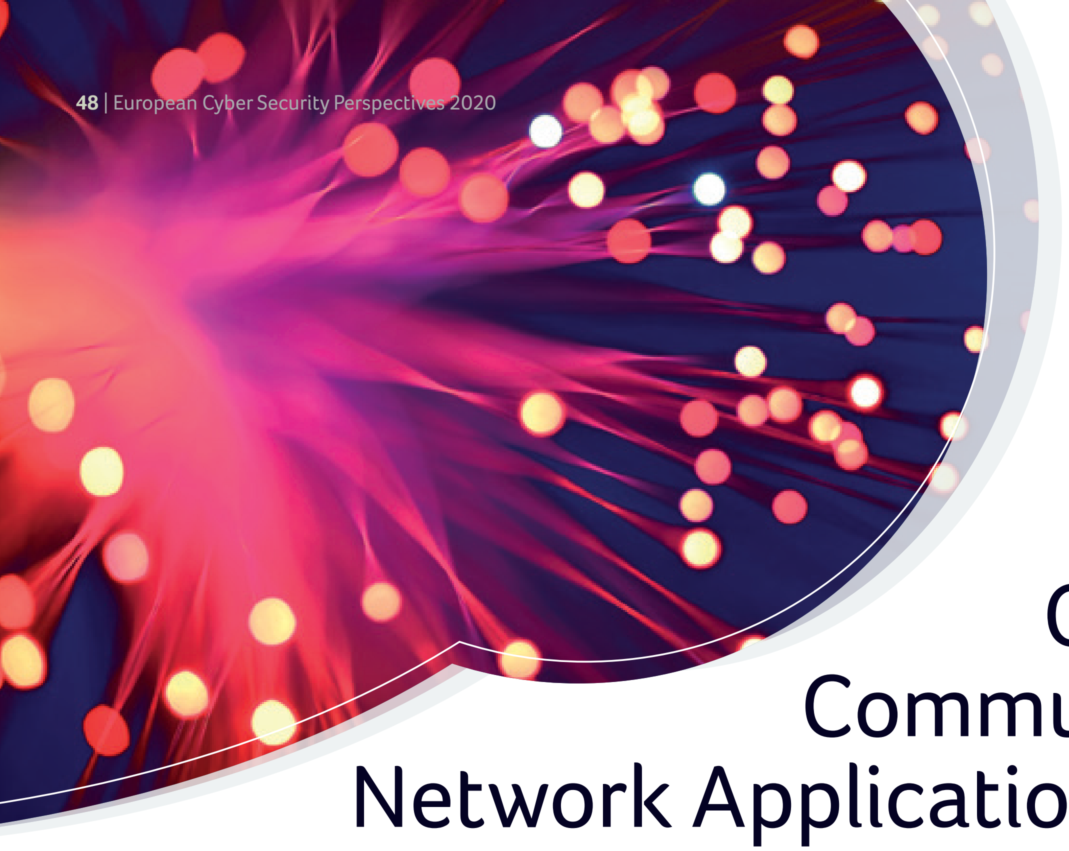
However, identity can also have value to the organisation as a whole. It could play a role in protecting customer privacy or make the quality control of the supply chain more effective. This allows for better protection of the privacy of customers or more effective controls on the quality of the supply chain. Identity then has suddenly become a distinguishing factor.

September

12 iOS lock screen can be bypassed to access address book in iOS 13Beta

13 Infosec duo cuffed after physically breaking into courthouse during IT security assessment

13 Mystery database left open turns out to be at heart of huge Groupon ticket fraud ring



Quantum Communication Network Applications Today and Tomorrow

Jean-Sébastien Pegon & Bruno Huttner, IDQuantique

Quantum Key Distribution: a recognized answer to Quantum Computer security threats

It is now well known that quantum computers will break most internet security solutions relying on public key cryptography, such as RSA, ECC or Diffie-Hellman. Various announcements from governmental organisations (NSA, NASA, EU, ...), standards bodies such as NIST[1], ETSI or ITU, and private companies working on quantum computers (IBM, Google,...) have made the threat absolutely clear: encryption breaches would generate a systemic failure. Classical or post quantum cryptography solutions are based on assumptions about the ease of solving complex problems (NP Hard), knowing the computational power available at a given point of time. In contrast Quantum Key Distribution[2] (QKD) is recognized as an Information Theoretically Secure (ITS) answer to the threat to security posed by quantum computers.

> Quantum cryptography is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. A more accurate name for it is Quantum Key Distribution (QKD). It works by sending photons, which are "quantum particles" of light, across an optical link. The Heisenberg Uncertainty Principle stipulates that in quantum physics observation causes perturbation. This is used to verify the security of the distributed keys and prevents the risk of eavesdropping.

> Contrary to classical physics, quantum physics is fundamentally random. It is the only theory within the fabric of modern physics that integrates randomness. Quantum Random Number Generators (QRNG) use these quantum-random properties to generate truly random numbers. Moreover, the high availability of randomness from a QRNG ensures instant inexhaustible entropy to avoid delays in transaction processing. The key generation of QKD systems is also enriched thanks to QRNGs.

QKD has been deployed by many organisations, primarily to protect data integrity or long lifetime data by using quantum keys to harden current encryption solutions. More recently telecom service providers have started to assess how this technology could be integrated in large scale backbone networks, not only to encrypt data but also to improve the security of the distributed control and management network. This article proposes an overview of the possible telecom use cases and the foreseen next steps to ease the integration of quantum cryptography in data and mobile networks.

QKD securing datacenter interconnection (DCI) or site to site connectivity

DCI requires secured high bandwidth connectivity and low latency. Hence using symmetric Layer 1 encryption

[1] https://csrc.nist.gov/events/2015/workshop-on-cybersecurity-in-a-post-quantum-world

[2] https://www.idquantique.com/quantum-safe-security/overview/qkd-technology/

September

16 Password-revealing bug fixed in password manager LastPass

23 Emergency Internet Explorer patch amid in-the-wild attacks

24 DeadlyKiss malware targets telecommunications providers

24 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day

25 Microsoft rushes out fix for Internet Explorer zero-day

such as AES-256 combined with QKD makes perfect sense, since a link of 100 Gbps can be encrypted using quantum keys in just a few microseconds with minimum bandwidth overhead[3]. It is the perfect first line of defence for all data streams at a reasonable cost per bit. Most network vendors propose this Layer 1 encryption solutions in their portfolio.

Since ETSI proposed a standard interface[4] (REST API) to exchange keys between QKD nodes and key consumer layers such as encryption equipment, the first common use case is to enhance DCI security thanks to quantum keys. The quantum key XOR with the standard session key generates a super session key, which is used by the network encryption equipment. Thus, the network security certification remains valid and it is even improved thanks to the ITS nature of QKD.

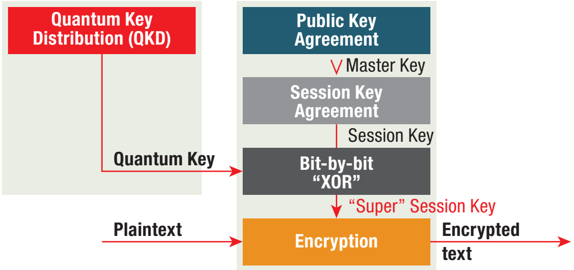


Figure 1: Dual Key Agreement

One QKD equipment can be connected to many (up to 80) consumer agents, therefore the cost of a QKD link can be "shared" by several data applications while avoiding to rely on RSA/ECC or DH for the key exchange. This solution, recognized by the industry, is available on the market and is rolled out in production environments.

The need for Quantum Communication Networks beyond site to site connectivity

The secured datacenter interconnection use case is current certainly an important commercial application of QKD. The next step is to secure large telecom networks with hundreds of nodes. QKD needs to be integrated in existing designs as an overlay solution with minimum impact on deployed networks, including their provisioning and monitoring. It is now possible to connect QKD nodes to each other while mapping existing topologies. The concept of Quantum Communication Network becomes a reality and enables the distribution of keys beyond standard distances (~100 km) and beyond basic point-to-point architectures. Thanks to an efficient Key Management System (KMS), keys can be routed and used by distant nodes connected to each other through QKD nodes or trusted repeaters. It opens the door to broader applications, for instance in Software Defined Networks (SDN) and mobile transport optical networks.

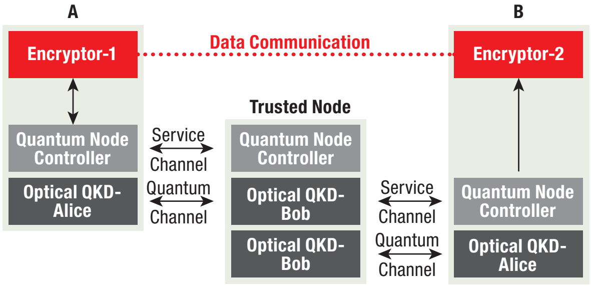


Figure 2: Trusted Node overview

QKD integrated in an SDN architecture

The digital transformation of the economy and enterprises has changed our day to day life. It is also impacting legacy IP services, such as MPLS-based solutions. This transformation for network service providers is enabled by SDN and Network Function Virtualization (NFV). SDN is an overlay technology optimizing the use of private MPLS-based and internet-based connectivity. Therefore, it improves the network resource usage based on application performance requirements. SDN allows network operators to use web-based interfaces frequently relying on Application Programming Interfaces (APIs) to order, configure and operate real-time network carrier nodes and services. SDN is also used by enterprise customers to smoothly configure internet services or cloud connectivity. It provides agility and speed of execution, thanks to automatic setup. It leads to significant productivity improvements and over the top business models.

However, this creates new security challenges since data is carried over the internet in order to reach hybrid clouds, mixing public and private hosted services. SDN is orchestrated centrally exchanging critical configuration messages to remote nodes. QKD technology on one hand can improve the security of SDN control and management planes but also needs to be integrated and remotely managed by SDN controllers to benefit from the same agility and configuration processes as new network architectures. Major carriers are already looking at using QKD integrated in SDN networks to improve the security level and prevent new attack vectors.
SDN control plane uses standard network security protocols such as SSH, TLS or IPSec, which can be combined with QKD. The DH session key can be XOR with a Quantum key provided by the QKD node[5]. Existing security certifications of the SDN network remain valid, but the security of the key exchange

[3] https://www.idquantique.com/testing-begins-on-uks-ultra-secure-quantum-network-link-using-the-equipment-of-id-quantique/

[4] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

[5] Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Thomas Szyrkowiec, Achim Autenrieth, Momtchil Peev, Diego Lopez, and Vicente Martin "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks" https://ieeexplore.ieee.org/document/8064559

becomes quantum-safe thanks to QKD and QRNG. To speed up the adoption of QKD in SDN networks, new interfaces need to be defined and standardized. The good news is that there is already some activity within ETSI and ITU defining SDN interfaces to QKD equipment. This ongoing standardization is an important step towards large scale implementations and vendor interoperability. It is also planned to demonstrate its implementation in 2020 through a European Testbed project called "OpenQKD" involving 38 European partners including major Telecom Service Providers[6].

QKD securing 4G/5G Backhaul

As 5G mobile networks are being rolled out to boost B2B digital transformation in various critical sectors such as e-Health, autonomous vehicles, or smart Cities/Factories/Buildings, the risk of cyberattacks has never been greater or the attack surface wider. Therefore, the level of security expected increases compared to previous mobile network generations which were not designed to transport critical data and are certainly not quantum-safe. Like SDN, 5G standard uses TLS or IPSec protocols presenting identified security weaknesses in the key exchange protocol based on RSA, ECC or Diffie-Hellman.

The mobile community have started to look at the impact of quantum computing attacks on 5G networks. The standardization workgroups and assessment have started. But knowing on one hand the delay between the approval of standards and its actual implementation, and on the other hand the lifetime of a mobile generation (approximately 20 years considering 2G is still available in many countries), mobile providers should certainly start their own assessment and piloting solutions in 2020.

The demand for enhanced mobile security for critical applications should allow mobile service providers to justify their investment. Some applied research papers[7] explain how QKD was successfully implemented in 5G mobile testbeds or networks. South Korea is already pioneering QKD deployment in 5G production networks. QRNG is also used to improve the entropy of the RAND function used for the Mobile Authentication protocol[8].

5G technology, thanks to network slicing, opens new opportunities while offering differentiated services and pricing per user or IoT devices. End-to-end multi-layer security is one of the performance criteria between various profile of devices. Some of the applications of the B2B sectors relies on robotics or video analytics, which are both demanding in terms of performance (high data rate and low latency) and security. Since quantum cryptography offers universal security without degrading the performance, it is a perfect fit for critical industry use cases.

We observe that some B2B customers are ready to pay more to benefit from premium performance and long-term security ensuring forward secrecy and data integrity of critical applications. The investment in QKD technology and networks is justified to address these demanding use cases. Furthermore, Quantum Key Distribution can be offered only on selected network legs, for example between an edge computing node and the customer location using 5G IoT. As quantum computers mature, the volume of customers interested by quantum-safe security solutions will continue to increase justifying long-term investment to expand the solution to the entire network. Finally, quantum-safe security applied today to 4G or 5G is a service differentiator compared to other providers or wireless technologies.

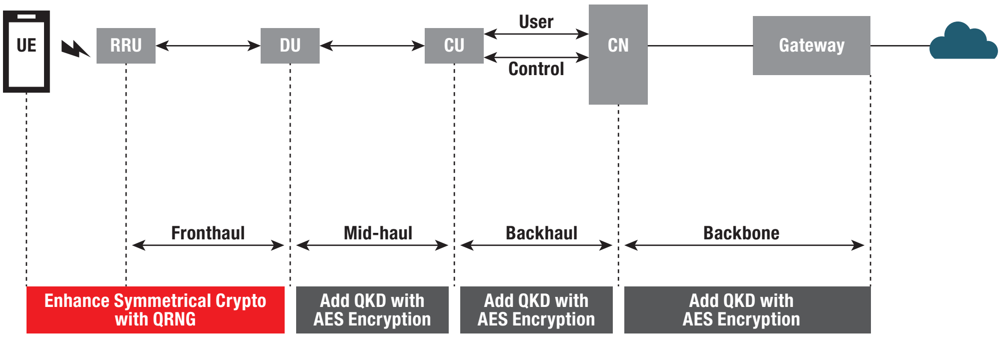

UE
RRU
DU
CU
User
Control
CN
Gateway
Fronthaul
Mid-haul
Backhaul
Backbone
Enhance Symmetrical Crypto with QRNG
Add QKD with AES Encryption
Add QKD with AES Encryption
Add QKD with AES Encryption

Figure 3: 5G architecture overview with Quantum Technologies

[6] https://openqkd.eu/

[7] R. Nejabati, R. Wang, A. Bravalheri, A. Muqaddas, N. Uniyal, T. Diallo, R. S. Tessinari, R. S. Guimaraes, S. Moazzeni, E. Hugues-Salas, G. T. Kanellos and D. Simeonidou " First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining over Flexi-WDM Optical Networks https://ieeexplore.ieee.org/document/8696286

[8] https://www.idquantique.com/quantum-safe-security/applications/telecommunications

Evolving from Incident Response to Threat Intelligence

Arnim Eijkhoudt, KPN

Threat Intelligence (TI) is the industry term for describing the practice of leveraging knowledge about your adversaries, technology and company exposure[1] to make informed decisions about security situations and improving the company's overall security posture. TI is frequently considered to be a separate activity or discipline at CERTs. With this article we aim to demonstrate that with a holistic approach to TI, a security organisation can improve their processes, move to proactively addressing security risk, reduce their costs by minimizing exposure and streamline their traditional CERT/incident handling processes.

Basic Threat Intelligence practices

TI commonly revolves around the processing and sharing of Indicators of Compromise (IoCs). IoCs are static pieces of technical information that describe the properties of a given threat, such as IP addresses, domain names, cryptographical hashes, email addresses, etc. TI analysts review the information, looking for coherence/correlation between the IoCs and threats. While these are great initial steps to get started with TI, combining and embracing threat intelligence and automation can bring much greater benefits. Horizontal and vertical integration of the two can be a powerful way of cost reduction through automatization, efficiency improvements, bridging gaps with risk management, red-/purple-teaming and incident handling.

Case Study: From Incident Handling to Threat Handling

KPN-CERT actively started using a Threat Intel Platform (TIP) in production in early 2016. Initially, the systems and processes ran parallel to our existing Incident Handling and ticketing systems, and it quickly proved to be instrumental in investigating and resolving a long-term fraud campaign. However, much of the initial TI work was done manually, and most of the information resided with dedicated analysts: determining which incidents to ingest into the TIP, searching for and enriching from additional sources, correlating information and processing the information for further use outside the TIP.

[1] Exposure can be any risk or vulnerability, known or unknown, technical or not

October

3

Dutch police break up bulletproof hosting outfit and kill Mirai botnet

Egypt used Google Play in spy campaign targeting its own citizens, researchers say

Multiple D-Link routers found vulnerable to unauthenticated remote code execution

Minerva attack can recover private keys from smart cards cryptographic libraries

With the addition of more and more information feeds, this accelerated the equivalent of SOC 'alert fatigue' for the TI analysts: information pollution/false positives and the resulting inability to filter out irrelevant information. For these and other reasons, it was therefore neither a sustainable nor scalable way to continue.

Back to the Drawing Board: Going 'all-in' on Threat Intelligence

In 2017, KPN-CERT decided to reposition its TIP and to restructure the existing processes around Threat Intel practices. Clear goals were set to aim for the TI maturity level of 'Exposure Management'. This meant that TI would be repositioned as the overall way of working, with Incident Handling being a specific part of the overall TI process. Part of this transition would be the explicit focus on Site Reliability Engineering (SRE) principles. Every team member is expected to look critically at their work processes, and to develop and deploy automation tooling to eliminate manual work. This directly reduces overhead costs and the chance for human error as well. The strong focus on SRE closely aligns with the emergence and evolution of open TI protocols, standards and technologies such as STIX/TAXII, MITRE's ATT&CK, OASIS, COCOA, etc. as well as the overall vision at KPN-CISO.

Challenges

Transforming your organisation's processes means making a significant initial investment. It can be a difficult 'sell', especially if the results only come at a later stage. Firstly, the expenditure of time and effort is significant, although it is also somewhat dependent on the existing culture and agility of the organisation. Secondly, by embracing these standards, technologies and the principles of SRE and TI, there is also the implicit choice for using those open standards and technologies while choosing for and deploying solutions that are compatible with these.

Nevertheless, the total cost of ownership (TCO) and subsequent cost reduction has shown to significantly outweigh those initial investments. For KPN-CERT, it has simplified everything from day-to-day incident handling to case investigations. In that sense, it is a 'gift that keeps giving'. It will continue to simplify the future interconnection of systems and exchange of TI data, cooperation with industry partners, CERTs, government and NGO's organisations, etc.

Reaping the benefits at KPN

Interoperability and development

Investing development time into a middleware library continues to pay dividends. One of the first things KPN-CERT developed, was a middleware library for interoperability with its TIP. This middleware makes it easy and quick to develop new integrations, because there is a consistent API that abstracts the communication with the TIP. Development, prototyping and deployment of integrations now happen in the span of days or a few weeks, rather than multiple months or years. It also enables the transformation and exchange of data between other types of systems, further simplifying and enabling interoperability. Good examples are simple scripts that can take TIP data and transform these into rulesets for popular IDS[2]. Lastly, it prevents being dependent on the TIP or other service providers for providing and maintaining interoperability or the interpretation and/or transformation of TI between the systems.

Integrations and optimizing processes

At the outset, integrating ticketing systems into our TIP was one of the primary goals, making the Incident Handling part of the overall TI process and automatically allowing for correlation of information in tickets/incidents with other TI in the TIP[3]. This not only enables our incident handlers and TI analysts to automatically share data, but it also forms the basis for moving from handling separate (and sometimes seemingly isolated or unrelated) incidents to detecting recurring problems and persistent threats in an automated manner.

However, critically examining the systems that exist in your organisation can provide a wealth of other potential enrichment sources or threat intel as well. Good examples can be the development of integrations with asset management systems, so that information about affected systems can immediately be enriched with ownership information, software/services running, previous incidents, change or request tickets, etc. This can even be taken further and to logical conclusions, e.g. by the automated parsing of vulnerability feeds and combining this with the asset management, vulnerability scanning information and emerging threat data from the TI analysts to determine real-time security exposure.

[2] https://github.com/KPN-CISO/EIQ-to-IDS - Transforming EclecticIQ JSON into Snort rulesets

[3] KPN-CERT has achieved this by creating (and publishing) integrations with common ticketing systems, such as OTRS and ServiceNow

Unpatched Android flaw exploited by attackers, impacts Pixel, Samsung, Xiaomi devices

Ransomware victim hacks attacker and releases decryption keys

FBI warns of major ransomware attacks as criminals go "big-game hunting"

KPN-CERT has also developed many other integrations, such as the Kathe enricher[4], which provides the detection of malware families and strains through the use of ssdeep[5] hashes. This effectively reduces cost by limiting the time spent reverse-engineering malware samples and by letting TI analysts define Courses of Action for families of malware, rather than having to deal with malware samples on an individual basis.

Bridging the gaps between TI, management and operations

By moving towards the TI maturity level of Exposure Management through these principles of automation, integration and interoperability, TI analysts can more easily determine the company's exposure to security threats. The ability to determine the risks that the company faces, trends over time, emerging threats, etc. and to be able to do so in (largely) automated ways also improves reporting on operational to tactical levels. This, in turn, allows your TI team to more effectively report to and liaise with your Risk Auditors, Board of Directors and other decision makers in the company. Understanding and effectively reporting on risks will facilitate better focus and decision-making, truly improving your company's security posture.

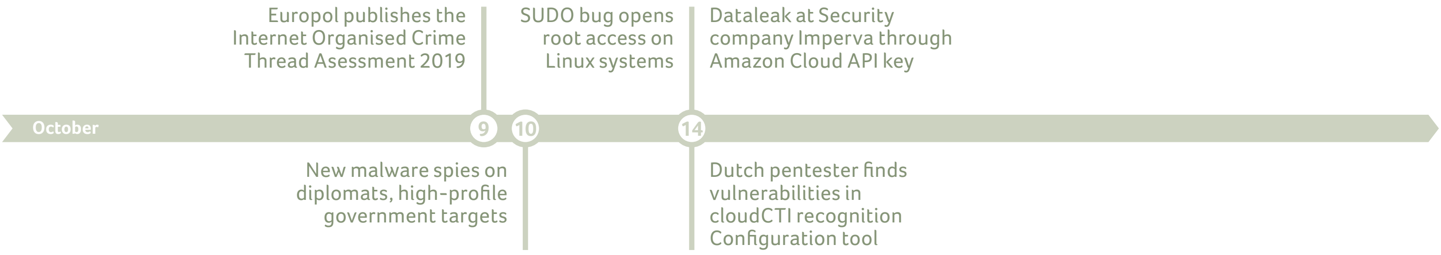
Final words

Perhaps you are just starting with TI or already in the later stages. Either way, KPN invites you to join forces with us in collectively fighting cybersecurity threats around the world, by embracing Threat Intelligence, intelligence sharing and supporting the open standards and protocols to do so. Threat Actors rarely work in a vacuum and rarely limit themselves to a single industry, so why should we?!

You can connect with us by sending an e-mail to cert@kpn-cert.nl

[4] https://github.com/avuko/kathe - Analyzing malware families through ssdeep hashing

[5] https://ssdeep-project.github.io/ssdeep/index.html


Europol publishes the Internet Organised Crime Thread Asessment 2019
SUDO bug opens root access on Linux systems
Dataleak at Security company Imperva through Amazon Cloud API key
October
9
10
14
New malware spies on diplomats, high-profile government targets
Dutch pentester finds vulnerabilities in cloudCTI recognition Configuration tool

Cyber security needs to change in order to be successful in today's world

Fred Streefland, Palo Alto Networks

Today's world isn't the same as it was in the last century. This isn't a surprise obviously, but it has significant consequences to the way that we manage cyber security, which we experienced especially in the last few years. Technological developments go extremely fast and thousands of devices are linked to the Internet each day ('Internet of Things'). These IoT devices provide lots of opportunities, because they often fulfil an essential function or are placed in our critical infrastructure. But they are also causing a significant risk, because they fulfil an essential function or are placed in our critical infrastructure but can also communicate between each other without human intervention. Since IoT devices are often not made with security in mind, they are vulnerable and increase the attack surface significantly.

Besides these developments, organisations themselves also have become more complex. Through this instrumented and interconnected world, their data isn't only in the on-premise computers of their own datacentre in their headquarters, but their data is everywhere, and their employees have become mobile workers with the company data installed on their mobile devices or in public clouds. The old-fashioned perimeter security doesn't work anymore in today's complex world.

The 'move to the cloud' is another challenge that causes organisations to transform. Organisations are required to become agile and scalable by using cloud computing. In recent years, it has become clear that organisations that use public cloud for their products and services are more agile than organisations that decided to stay on-premise. The transformation to public cloud infrastructures provides a significant competitive advantage against the on-premise organisations. Since security is a main prerequisite for this move to the cloud, it's an important aspect for organisations.

Cooperation is key

So, let's dive more into this security aspect. Until some years ago, mainly specialized companies came up with solutions to the cyber problems and challenges of the time. For every problem there was a different solution (read: 'product'), with the result that thousands of different products arose, all of which found their way into the market. As a result, the current cyber security landscape has arisen, with organisations running on average more than 30-40 different cyber security products in their organisation, which do not communicate with each other and are certainly not integrated into one overview image.

So, although not all organisations have a good cybersecurity posture yet, I do see some positive developments in the cyber domain that do work. Cooperation is one of them. Several cyber companies acknowledged this some years ago and they found the Cyber Threat Alliance (CTA), a not-for-profit organisation that brings together the main cyber security companies in the world and 'encourages' them to share threat intelligence with each other.

This cooperation in the private sector is successful, but the cooperation between the public and private sector still needs improvement. The 'bad guys' are working together and if we want to become successful as a society, then we'll need to do this as well. Public-private collaboration is especially essential, because cyber security is not confined to either domain, and both domains are also complementary to each other. We can learn a lot from each other if we are willing to really share and dare to delegate.

A great example of working together is the recently signed Memorandum of Understanding, signed by both Palo Alto Networks and Europol. We are expanding our collaborative efforts in combating cybercrime and want to work together to make cyberspace safer for citizens, businesses, and governments. The Memorandum includes the exchange of threat intelligence data and details of cybercrime trends, as well as technical expertise and best practices.

In addition to a real collaboration, it is also very important that the public sector must dare to invest, because 'the cheapest security solution' certainly does not work in the cyber security world. The bad guys have no budget restrictions and use all the resources they can afford. In addition, they have no game rules to privacy or compliance, which we do have (especially in the financial and public sector domains).

Adopting a Zero Trust approach

In my humble opinion, we now have two actions that we need to take as a society if we want to become successful within the cyber security domain. These two actions are:

1. Stop with the current point products and 'price fighting solutions'-approach;
2. Apply a Zero Trust strategy: so always use a risk assessment as the foundation for the cyber security plan and dare to invest.

From my conversations with CISOs from international organisations and governments, as well as my own experiences, I believe that this is the only way for successful cyber security.

It will not be surprising, but each organisation (public and private) that is serious about their cyber security needs to adopt a Zero Trust strategy in combination with a thorough risk assessment as the basis for the cyber security plan.

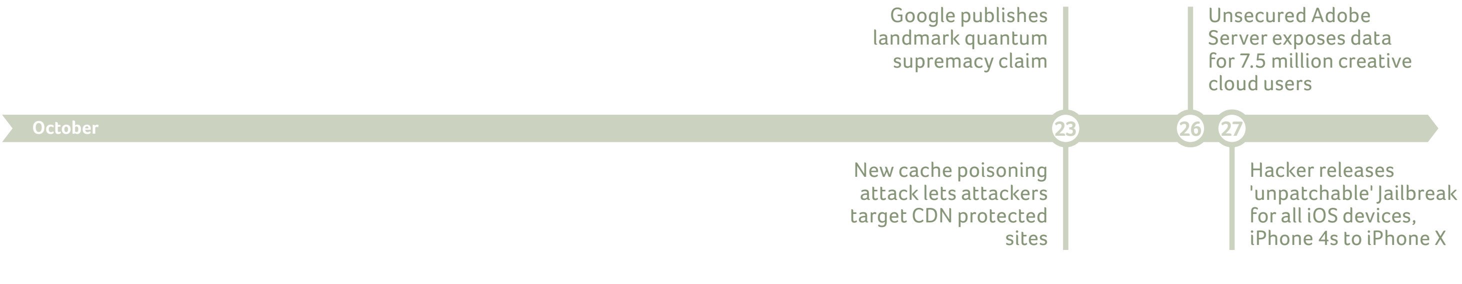
Zero Trust is a strategy, based on an untrusted world, where the security is based on the crown jewels of the organisation, the most valued assets and the security is arranged from the inside out (instead of looking at the threat first). The threat is a given, because we live in an untrusted world and to secure the crown jewels of the organisation, everything needs to be logged and monitored. Visibility into the entire IT landscape of the organisation is therefore a prerequisite, which is not a simple task in the current complex world and with the current complex organisations but is required.

Everyone in the organisation must ask themselves the questions: What are my crown jewels? Where are my crown jewels? And who has access to my crown jewels (and who shouldn't)? These questions should be posed by every European tender for security solutions. A risk assessment is fundamental to a good and effective cyber security plan, because it starts with it.

My definition of cyber security reads: *Cyber security means to mitigate the risks for the core business, so that the business can do its business.* Cyber security is therefore not more than managing risks for the business, which make the previous mentioned questions about the crown jewels essential.

Conclusion

Fortunately, there are organisations that take cyber security seriously and dare to invest. They adopt Zero Trust and start cyber security plans with profound risk assessments. These organisations are the organisations that we don't see in the media reports about hack incidents or ransomware infections. Unfortunately, there are only a few of them and I still see far too many organisations, who are going through the old way. Ask yourself if your company is cyber secure enough.


October

23 Google publishes landmark quantum supremacy claim

23 New cache poisoning attack lets attackers target CDN protected sites

26 Unsecured Adobe Server exposes data for 7.5 million creative cloud users

27 Hacker releases 'unpatchable' Jailbreak for all iOS devices, iPhone 4s to iPhone X

Insider threat: Trust, but verify

Troy Verberckmoes, VU University Amsterdam, Nadine Bijlenga, KPN

Trusted insiders pose a threat to our organisations because they have access to opportunities which outsiders do not. There is no shortage of examples showing the potential impact of incidents with insiders: the alleged conspiracy to steal McAfee's trade secrets[1], AT&T employees who took bribes to plant malware on the company's network[2] and an ex-employee blackmailing his former employer KPN with stolen customer data[3]. Why do some employees turn bad while others do not? And what could companies do to reduce the risk of insider threat?

Lures and a lack of credible oversight

The American CERT National Insider Threat Centre distinguishes four categories of intentional (non-violent) insider threat: Intellectual property theft, IT sabotage, fraud and espionage.[4] The motivation and modus operandi of malicious insiders are diverse. Just like other threat actors in the security landscape, their motivation goes from curiosity and ideology to gaining financial benefits and geopolitical motives.

Insiders can also be influenced by outsiders with their own motivations. This was for example the case in Iran: the stringent physical security measures alone were not sufficient to protect the nuclear facility against the infamous Stuxnet attack[5]. The attack succeeded because of a recruited insider who collected crucial information and eventually deployed the virus. In general, twenty percent of cybersecurity incidents and fifteen percent of data breaches originated from employees within the company[6].

[1] https://www.cyberscoop.com/mcafee-lawsuit-tanium-employees-secret-sauce/

[2] https://www.zdnet.com/google-amp/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network

[3] https://nos.nl/artikel/2253366-celstraffen-geeist-tegen-afpersers-kpn.html

[4] CERT National Insider Threat Center. (2018). Common Sense Guide to Mitigating Insider Threats, Sixth Edition. Pittsburgh, PA: Carnegie Mellon University.

[5] https://www.volkskrant.nl/nieuws-achtergrond/aivd-speelde-cruciale-rol-bij-sabotage-kernprogramma-iran~ba24df9f/

[6] https://www.verizon.com/about/news/verizon-refocuses-cyber-investigations-spotlight-world-insider-threats

From the perspective of employees, an opportunity is a prerequisite to commit a malicious act. According to the organisational opportunity theory[7], opportunities arise in environments where lures are combined with a lack of credible oversight. Lures arise when:

1. someone has privileges that can lead to unjustified access to (technical) sources, or;
2. someone has access to certain (technical) resources that he or she can use for personal gain to the detriment of another individual or organisation.

A lack of credible oversight exists in situations where there is:

1. a lack of capacity of external parties (both within and outside the organisation) to pay attention to the behavior of individuals/organisations, and/or;
2. a lack of capacity of those external parties to impose negative consequences when they see misconduct.

What does this mean for the risk that malicious insiders pose to organisations? The work environment provides many lures, often with a lack of credible oversight.

Why most people stay on the right path

If so many opportunities for insider threats exist within the workplace environment, why is it relatively rare for an insider incident to happen within a company? An explanation can be found with the use of the subjective utility theory of crime[8]. This theory indicates that individuals within organisations make subjective estimates of the certainty and seriousness of formal and informal sanctions, the benefits of organisational crime and the costs of compliance and the certainty and importance of the loss of self-esteem.

Fortunately, this means that for most employees, a malicious act against their employer won't even cross their minds. It simply goes against their own morals. The costs of such an act will therefore result in a loss of self-esteem so high, that the benefits of the crime can never be enough. If loss of self-esteem is not an issue, employees will still not necessarily consider committing a malicious act because they will estimate the benefits of organisational crime and the costs of compliance both to be low. Finally, there is a very small percentage left who actually might consider committing a malicious act. Of these people, some will not follow through even then, because they estimate the risk of formal and informal sanctions to be too high.

Insider Threat Risk

Even though most employees can be trusted, a single malicious insider could inflict serious damage to a company due to the opportunities they potentially have. While most organisations invest in cybersecurity, they are often mainly focused on external threats. It is therefore understandable that ninety percent of organisations feel vulnerable to insider threat. The majority of organisations have identified at least one insider attack against their own organisation in the past year, of which more than one third have even experienced six or more incidents[9]. Sixty-four percent of the organisations found company information publicly accessible on the internet and fifty-six percent of the organisations reported potential theft of data by departing or new employees[10].

Since malicious insiders have legitimate access to systems as well as knowledge of these systems, the victim organisation might never realize what happened to them. It is very likely that our organisations often misattribute damage to external factors, because they only occasionally discover that the true cause can be traced back to an insider. Therefore, these statistics are most probably the result of underreporting.

This begs the question how companies can prevent such a thing. There is no such thing as one hundred percent solid security, but there are a lot of opportunities where the defenses against insider threats can be improved. For this, the situational crime prevention theory[11] can be used as a starting point. This theory indicates that you must address five dimensions within opportunities to raise the costs of criminal behavior and lower the benefits:

1. the efforts to carry out the act must be increased
2. the associated risks of discovery before committing the crime must be increased
3. the expected rewards of the offense must be lowered
4. situational circumstances that can encourage the crime must be removed
5. the excuses that perpetrators can use to justify their actions must be removed

For companies the best way to start addressing these five dimensions is to start working on an insider threat program.

An integrated approach

An Insider Threat Program is an organisation-wide program which defines roles and responsibilities over all departments and has a well-established and clear vision. An insider threat program is of added value because it uses an integrated approach to analyze and mitigate risks from both malicious and unintentional insiders. Also, when an incident does occur, the

[7] Shover, N., & Hochstetler, A. (2005). Choosing white-collar crime. Cambridge: Cambridge University Press.

[8] Nagin, D., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. Law & Society, 27(1), 467-496.

[9] https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf

[10] https://www.thehaguesecuritydelta.com/media/com_hsd/report/154/document/2017-Insider-Threat-Intelligence-Report.pdf

[11] Cornish, D., & Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. Criminology, 25(4), 933-948.

November

20 Companies pledge support for the Hack_Right Program

1

NordVPN users' passwords exposed in mass credential-stuffing attacks

11

Magento urges users to apply security update for RCE bug established collaboration ensures an immediate and organized response. In regards to sharing and collecting information, privacy and confidentiality must be taken into account.

To build a solid basis, companies need to find out what their critical assets are, include insider threat risks in enterprise-wide assessments and clearly document and consistently enforce policies and controls. To reduce insider threat risks, the employee lifecycle needs to be addressed within the whole supply chain[12] [13]. This includes setting up a screening process for critical positions and developing a comprehensive employment termination procedure, but this also includes anticipation of stressful situations such as reorganisations, and creating awareness for insider threat risks. Disgruntled employees are more inclined to cross the line. Therefore, it is important to also focus on the adoption of positive incentives to align the workforce with the organisation. This can improve workplace engagement, perceived organisational support and interpersonal development at work for all employees.

In addition, clear access controls are important to prevent, detect and respond to insider incidents. It is important to implement strict password and account management policies. To enforce separation of duties, the doctrine of least privileges and to monitor the behavior of privileged users. Finally, quick wins can be made by taking measures to close doors to unauthorized data exfiltration.

Conclusion

Implementing an insider threat program addresses all the dimensions of the situational crime prevention theory which mitigates the opportunities of insider incidents significantly. Implementing clear access and authorization controls, for example, will increase the effort needed to commit the crime. Associated risks will be increased by transparency and communication of the implementation of the program. Increased collaboration between all departments and personnel result in less lures and better credible oversight, removing many opportunities for malicious insiders in the first place, which lowers the expected rewards of any offense. Attention to the individual level prevents employees from becoming disgruntled, which removes many situational circumstances encouraging the crime. Finally, by clearly documenting and enforcing policies, many of the excuses that perpetrators can use to justify their actions can be removed.

[12] CERT National Insider Threat Center. (2018). Common Sense Guide to Mitigating Insider Threats, Sixth Edition. Pittsburgh, PA: Carnegie Mellon University.

[13] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

November

12

YouTube BitCoin videos pushing predator info-stealing trojan

13

TPM-FAIL timing attack allows extraction of private keys from some TPM chips

Anomaly detection 101: Hunting the unknown

Bram Cappers, Joey van de Pasch, Dennis Cappers, Josh Mengerink, AnalyzeData

Intrusion detection is a hot topic in the world of cyber security. Especially with artificial intelligence and machine learning as the new buzzwords it can be difficult for outsiders to know what to expect from them. In this article we aim to explain the fundamental basics of anomaly detection. In particular we discuss the strengths and limitations of such techniques, how far we can go towards full automation, and what you should keep in mind when using anomaly detection.

The main goal of many intrusion (or anomaly) detection systems is to discover activity in data (a.k.a. events) that stands "out of the ordinary" or is strange/unexpected. Of course we can get very philosophical about what the true definition of an anomaly is, but let us focus on some examples in practice. In practice, events are commonly found in areas such as healthcare, finance, security, telco, mobility and many more. Examples where intrusion detection turned out to be valuable for the latter two will be discussed later. First it is important to understand that there exist three types of anomalies that we can discover in data, namely: point, contextual, and collective anomalies.

Point anomalies are outliers that are strange with respect to your entire data collection. Imagine you have a login history of an employee Bob and Bob always logs in to the company from the office in the Netherlands. If Bob after 5 minutes would suddenly login from Uganda, this is strange with respect to his entire history.

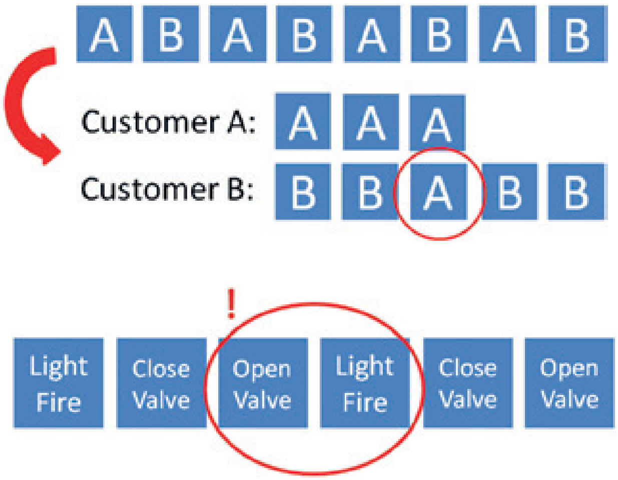


Figure: 1 (top image) Contextual anomalies become visible when inspecting data from a different point of view. (Bottom) Collective anomalies are caused by the presence of groups of events.

Contextual anomalies are outliers that are strange with respect to a subpart of the data. Suppose Bob accesses contracts A and B in the following order: ABABABAB… although the order of the events seems fairly regular, if we would group the data for instance on the customers for which Bob is accessing these contracts we can see that he usually accesses contract A when working with customer A and contract B for customer B. The access of contract B for customer A however is uncommon and is considered anomalous with respect to that customer.

Although point anomalies are relatively easy to discover, the main challenge for fully automated solutions is to find the right split for the detection of contextual anomalies. If we have a dataset with a 100 columns, there are 2^{100} data splits possible for which we can find anomalies! How should an algorithm know which (combination of features) are more interesting than others? This is where human insights become vital.

Finally, collective anomalies are outliers that are not strange by themselves, but can be strange if they happen together. In a combustion engine for example events such as “open gas valve” and “light fire” are not uncommon, but the order in which they happen matters a lot.

Challenges:

The contextual anomaly problem shows that discovering anomalies in general is not difficult at all. We can always find a viewpoint from where data can be seen as abnormal. We need to assist automated techniques with domain knowledge in order to avoid generating too many alerts. Besides context in practice there are many other challenges to tackle before we can reliably discover anomalies of interest.

Data bias: In order for anomaly detection to work, we need to have a notion of what is regular behaviour of a system. This requires a “training” phase where the system absorbs all the activity that for instance Bob is doing in order to get a better understanding of his daily way of working. This is under the assumption that the data observed during the training period is representative for Bob’s profile. If the training period is too short, we have too little data points to draw a reasonable conclusion (i.e., overgeneralization). A too long period, however, increases the risk that any abnormal behaviour is also captured in the “profile” of normal behaviour.

In the past companies such as HP[1] and Google[2] discovered this the hard way. HP for instance designed webcam tracking software such that your head always stays centered on screen if you move away from the camera. The algorithm was carefully designed and trained on a lot of data. What they did not know was that the training data hindsight contained more examples of light-skinned people than of dark-skinned people. As such, the webcam feature did not work when an African American showed his face in the camera. After this discovery, the computers were referred to as “racist” computers.

False positives: As with all technology, anomaly detection is not perfect. Although it is perfectly valid for Bob to login from the United States when he is on a business trip, the system may not recognize this as normal. Such an event may be unfairly marked as an outlier and is also referred to as a false positive. Analogously there exists the class of false negatives: the number of times the anomaly detection does not trigger on something it should have.

In security there is typically an imbalance between the amount of normal and anomalous traffic. 99.9% of the traffic is legitimate whereas 0.1% could be an indicator of compromise. Too many false alarms makes the system obsolete as you basically shift the problem from manually digging in the data to find anomalies into digging in the alarms to find the real ones. Minimizing the false positive rate without missing too many true anomalies is therefore crucial in order to be useful in practice. Even in systems with a 1% false positive rate, results can be impractical when dealing with thousands of events per second.

Concept drift: Suppose that our employee Bob gets promoted to a function where he for instance needs to travel a lot to the United States. The profile that we once built for the user has become outdated and should not lead to false positives. Although throwing away his old profile is always an option, be aware that this can be costly if data is scarce or training phases are long.

[1] https://www.wired.com/2009/12/hp-notebooks-racist/

[2] https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai

November

22 FBI warns of cyber attacks targeting US Automotive Industry

25 RIPE NCC runs out of IPv4 blocks

What can we do?

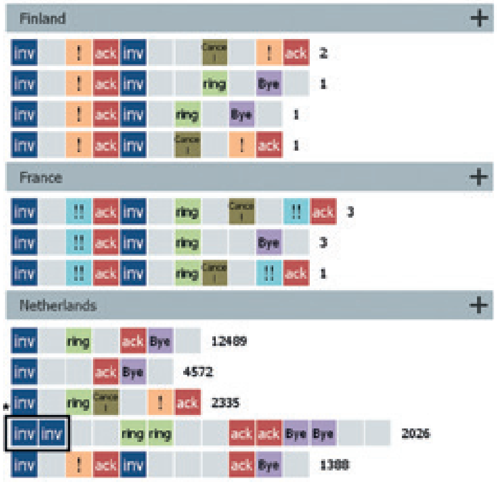

Finland
inv ! ack inv Cance ! ack 2
inv ! ack inv ring Bye 1
inv ! ack inv ring Bye 1
inv ! ack inv Cance ! ack 1
France
inv !! ack inv ring Cance !! ack 3
inv !! ack inv ring Bye 3
inv !! ack inv ring Cance !! ack 1
Netherlands
inv ring ack Bye 12489
inv ack Bye 4572
inv ring Cance ! ack 2335
inv inv ring ring ack ack Bye Bye 2026
inv ! ack inv ack Bye 1388

Figure 2: The discovery of a bad proxy server while checking the validity of phone call handshaking.

As a human we are aware of activity inside our company and have knowledge that is often not taken into account by the anomaly detection algorithms. Knowing for instance that the shutdown of a server happened for maintenance purposes can seriously alter the way anomalies are interpreted. One way to tackle the contextual anomaly problem is therefore to start defining behavioural patterns of which you are certain are desired/undesired and guide anomaly detection techniques into the areas that are unknown. We have applied this strategy in several domains, including Voice Over IP telco fraud and the discovery of illegal waste dumping in an international IEEE data challenge.

In Voice Over IP traffic there is a certain expected pattern when trying to make a phone call: The sender first sends an invite (INV), the recipient must acknowledge (ACK) after which the call starts and is either ended with a BYE or CANCEL. By visualizing the steps in a phone call as a sequence of blocks we could see which patterns were more present than others. This enables us to prioritize certain features over others and tailor anomaly detection algorithms to patterns we did not expect at first but became relevant after we have discovered them. The result was the discovery of a bad proxy server that was forwarding the phone calls to a malicious server (Figure 2).

Figure 3 shows a use case where we studied vehicle travel patterns in a wild life preserve. By colouring the data based on properties that were of interest (e.g., entering the park, visiting a camping etc.), anomaly detection techniques in turn could use this information to discover that certain vehicles were accessing areas for which they were not allowed. It was the combination of driving in restricted areas while not being authorized personnel that was causing the anomalies to be interesting.

We hope to have shown you how anomaly detection can be applied within some specific areas together with the different challenges that have to be faced. We as humans are still invaluable when it comes to spotting new anomalies and building models of expectation. Detection techniques can be significantly improved by enabling users to incorporate their insights in these techniques. In the end finding anomalies is not difficult. Finding the ones that matter is the challenge.

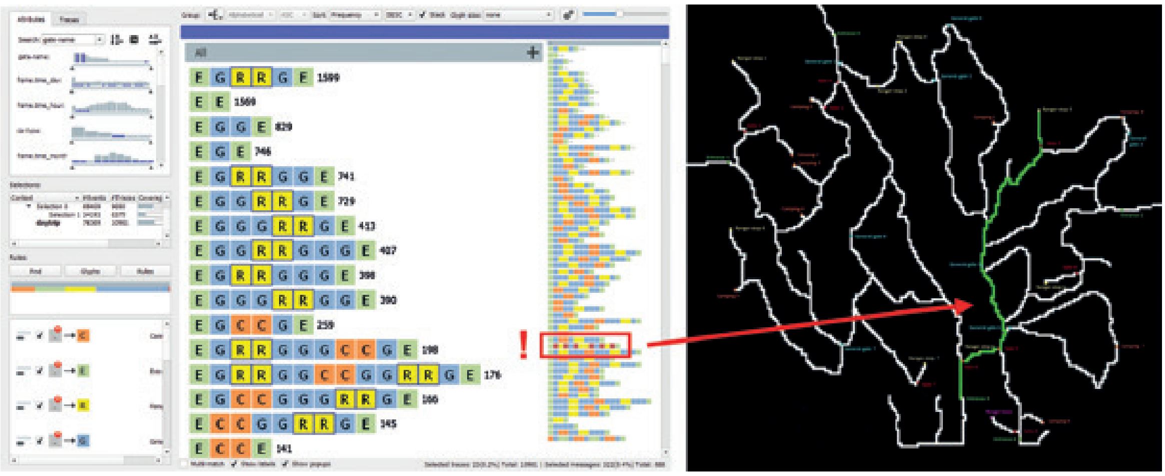


Figure 3: The discovery of a truck dumping chemical waste in the Lekagul wild life preserve.

Hacker steals 44 million euros in crypto coins from the Korean crypto exchange

November 26 27

T-Mobile data breach affects more than 1 million US customers

The sky has already fallen
(you just haven't seen the alert yet)

Rik Ferguson, Trend Micro

With today's ever-evolving threat landscape, it's not enough to just have advanced security protecting your users and infrastructure, you need capabilities in place to help you respond rapidly to threats that may breach your defences. Despite having layers of advanced protection, there is no such thing as 100 percent prevention, it only takes a single threat to make it through for your organisation to be 100 percent at risk. To avoid serious and widespread damage, your goal needs to be; prevent as much as you can, and detect and respond quickly if a threat does break through.

Many organisations today use multiple, separate security layers to detect threats across their endpoints, servers, network, email and cloud infrastructure, leading to siloed threat information and an overload of threats with little means to correlate and prioritize them. Investigating threats across all these disparate solutions makes for a very piecemeal and manual investigation process that can miss threats altogether due to lack of visibility and correlation. Many detection and response solutions only look at endpoints—and therefore miss threats that enter through user emails, the network, and servers—resulting in a very limited view of the breach and provides an inadequate response. To have a true picture of threats affecting your entire organisation it's important to have native integration into detection and response functions across email, server, network, cloud workloads, as well as the endpoint.

Detection and response are vital security requirements for all organisations, but the truth is most organisations are resource and skillset constrained. Modern detection and response currently require a significant amount of time and dedicated expert resources that most organisations don't have.

Of course, the much-touted "Cybersecurity Skills Shortage" isn't news to anyone, or it shouldn't be. For seven or more years, journalists, industry analysts and practitioners have been opining about it *one way* or *another*. Analyses and opinions vary on how we have reached this impasse, my own being that this is a largely self-inflicted crisis caused by proscriptive hiring practices and unreasonable job requirements. Whatever the reason, the outcome remains the same. We have too few people doing too much work, with too many tools and too few meaningful resources.

November 28

Cloudy biz Datrix locks down phishing attack in 15 mins after fat thumb triggers email badness

The typical Security Operations Centre (SOC) of today is drowning in a huge volume of alerts. In the financial world for example 60% of banks routinely deal with 100,000+ alerts every day, 17% of them *reporting* 300,000+ security alerts, according to research carried out by Ovum, and this pattern is repeated across industry verticals.

There is no way that the typical Security Operations Centre is staffed to the levels required to be able to triage these alerts, meaning that a large proportion of them are simply never actioned (read ignored). Of those that do eventually see a pair of eyes it hardly seems worth the effort. An *EMA report* all the way back in 2017 found that analysts were spending around half an hour investigating each incident with much of the time being spent either downgrading alerts marked as critical (46%) or otherwise reprioritising (52%) and identifying false positives (31%). In fact, if you do the maths on those numbers, it is abundantly clear that no SOC will ever be staffed to the levels required to deal with such a volume of information. Twenty-five minutes of work per alert, for 100,000 alerts is equal to 41,667 hours of work in every 24-hour period. So, any enterprise dealing with that volume of alerts would need a SOC team of 5208 people, just to keep up with the triage!

This deluge of information, coupled with a focus on small, repetitive and often manual tasks are critical components contributing to fatigue, boredom, and a feeling of powerlessness in the workplace. A *recent survey carried out by Trend Micro* revealed that IT teams are under significant pressure, with some of the challenges cited including prioritizing emerging threats (47%) and keeping track of a fractured security environment (43%). The survey showed that they are feeling the weight of this responsibility, with many (34%) stating that the burden they are under has led their job satisfaction to decrease over the past 12 months. It's not just the SOC analysts either, in that same survey one third of IT executives told us that they felt completely isolated in their role.

Workplace pressure at these levels is simply not sustainable, fatigue leads to neglect, neglect to mistakes, and mistakes lead to burnout, further reducing the available talent pool and dissuading others from ever entering into the industry, it's a vicious circle.

This security event flood is exacerbated by the fact that the majority of organisations rely on large numbers of specialised and disconnected tools. Many of the alerts that analysts are dealing with are often different views of the same object, or duplicate notifications from discrete security tools. The Ovum report I mentioned above notes that almost half their respondents (47%) told them that only one in five events is actually related to a unique security event. So hey, looking on the bright side, maybe you only need just over a thousand people in that SOC team after all!

In fact, Security Operations Centers are drowning in threat data, all the while thirsting for meaningful threat intelligence.

Water, water everywhere
and all the boards did shrink,
Water, water everywhere
nor any drop to drink.

This uncomfortable reality is one of the major driving forces behind the emergence and rapid adoption of XDR. As opposed to the simpler Endpoint Detection and Response (EDR), XDR collects and correlates data across email, endpoint, servers, cloud workloads, and networks, enabling visibility and analysis that is difficult or impossible to achieve otherwise. With more context, events that seem benign on their own suddenly become meaningful indicators of compromise, and you can quickly contain the impact, minimizing the severity and scope.

A recent blog post by my friend and colleague Greg Young laid out his reasoning on *"Why XDR is a big deal and is different from SIEM and Platforms"* and a truly mature XDR technology, with feature rich APIs, collecting, correlating, triaging, reporting and perhaps even remediating (to a certain level) must represent the direction of travel for the SOC of the near future. Organisations can use automation and a managed detection and response (MDR) capability to handle the volume of events. Organisations can use a cross-platform discovery and response tool (XDR) to aggregate and consolidate events dramatically, reducing the demand on people and improving the accuracy and timeliness of protection from threats.

We are not going to solve the skills shortage within a decade, arguably we are not going to solve it at all, particularly if we continue to focus on filling the gap with human brains. The problem is not in the potential recruitment pipeline, it is in the actual data pipeline and that is where technology must play the lead role. An AI driven Tier I SOC platform able to scale with the continually increasing volume of data, automating and accelerating initial analysis, the creation of incident context, chasing down patient zero through an automated root cause analysis. Such a system would present the human Escalation Analysts with aggregated data in a logical attack-centric progression automating the *Monitor, Prevent, Detect* and *Investigate* roles and providing the SOC analyst with actionable threat intelligence for real *Response* and *Remediation*.

December

2
Facebook ads manager targeted by new info-stealing trojan

4
UK retailer Sweaty Betty hacked to steal customer payment info

Classification of assets in an ecosystem

Frank Jansen, KPN

Big companies nowadays use a combination of ICT assets such as networks, mainframes, applications, databases, software and office automation equipment to conduct their business and operations. After many years the ICT landscape has grown into an ecosystem of assets (new, legacy). Legacy assets stay alive to keep earlier versions of services working and to support a variety of hard- and software at customer premises. In addition, all these assets are prone to confidentiality, integrity and availability risks, and thus constitute a serious concern about resilience. Implementing measures for all these possible risks requires a lot more money than available. Budgets to accomplish these measures are limited in most companies. From a financial point of view, it is essential to know which assets are the most important for the company in order to stay in business, and to prioritize the most effective measures to be taken to mitigate the risks related to these assets.

Classification of all assets in terms of Maximum Tolerable Period of Disruption (MTPD) or Recovery Time Objective (RTO) represent the longest time that the asset may be unavailable before putting the company in jeopardy. This classification also provides the ranking of priority which will dictate the application of available budgets for increasing resilience of the most important assets.

How to create an inventory of the assets?

A starting point is the list of services the company delivers to its customers, and the list of internal services needed to run the company.
It is important to classify each of these external and internal services using a Business Impact Analysis (BIA) method. Several institutions offer a BIA method applicable for a wide range of organisations. It is also possible to create a tailormade BIA specific for the

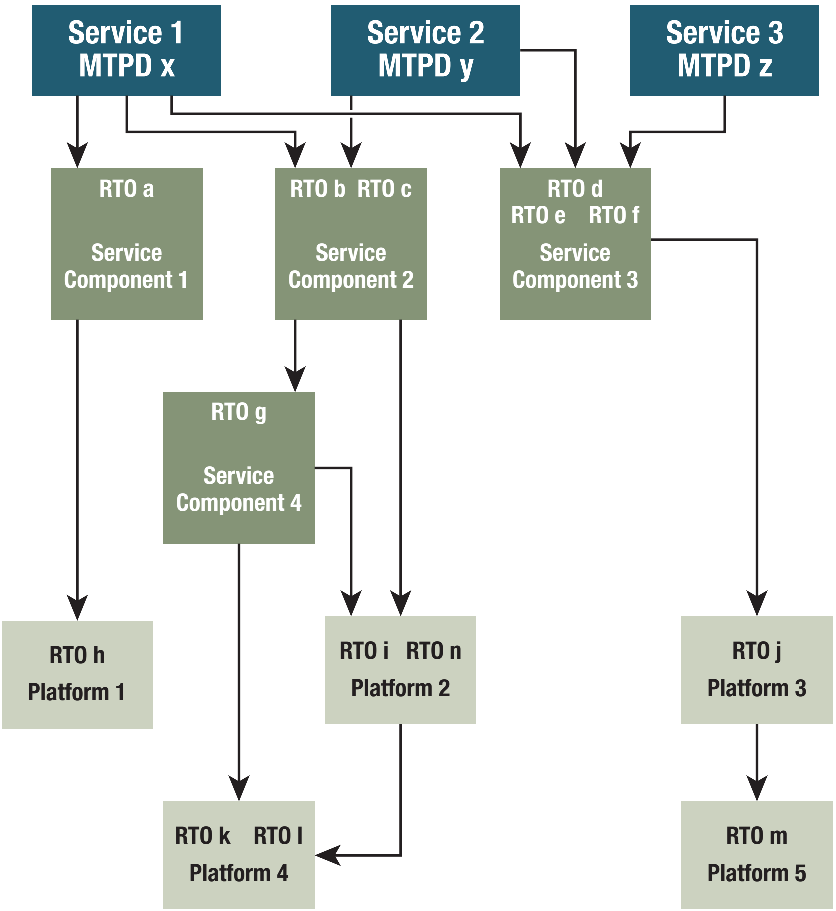


Figure 1: Example of hierarchy of dependency of company services on service components and platforms

company, consisting of questions about the impact of outage for the relevant domains. Our company constructed a BIA based on four questions with four predefined impact levels each:

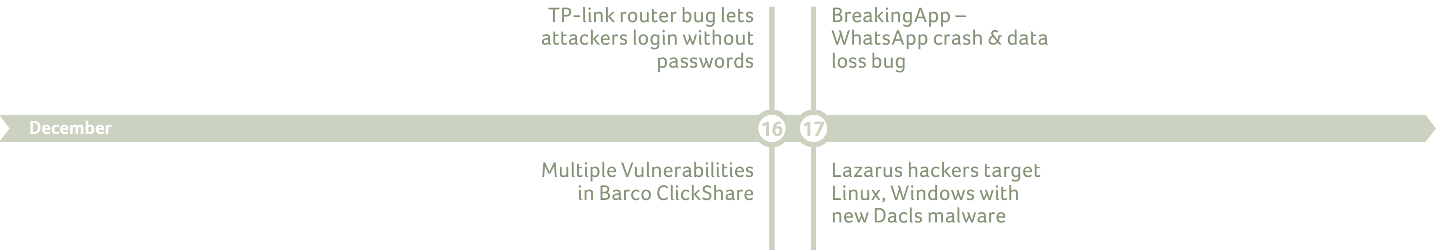
- Quantified level of loss of turnover after 24 hours of service outage, from zero to risk appetite
- Quantified level of fines, courtesy and restoration costs after 24 hours outage of the service, from zero to risk appetite
- Percentage level of (potential) customers after 24 hours outage of the service
- Level of societal impact from none to very large for the customer base after 24 hours of service outage

Each question is answered by a choice out of the four levels. The highest impact chosen in these four questions displays the Business Impact Level and corresponds with an MTPD (KPN uses the following MTPD boundaries: more than a week, one week, one day and four hours). These MTPD's must be aligned with the risk appetite the company accepts for its services.

The MTPDs defined for the external and internal services are the starting point of classifications for all assets in the company that are necessary for one or more of these services.

The next step is to list per service which assets are required to make the service work. This can be a combination of ICT components: networks, platforms, applications etc. The chain of dependencies might be complex. It may help to distinguish Service Components consisting of several ICT components that act together as a complete unit, necessary for more than one service. An example of a Service Component can be the Internal Office Network, that is used by several internal and maybe external services. A Service Component can be dependent on one or more other Service Components: the Service Component Internal Office Network may depend on a Service Component Office workplace and a Service Component Internet Access.

A service may also be dependent on one or more platforms consisting of a host with specific software and databases, delivering the specific functionality


TP-link router bug lets attackers login without passwords
BreakingApp – WhatsApp crash & data loss bug
December
16
17
Multiple Vulnerabilities in Barco ClickShare
Lazarus hackers target Linux, Windows with new Dacls malware

needed for the service to function. Other services may be dependent on the same platform as well.
In general, the availability of a service in terms of its classification derived MTPD sets a requirement on the availability of the Service Components and the platforms it depends on. This requirement is the RTO that is needed for the service to be restored within its MTPD after a failure. In most cases the RTO of a Service Component or platform is, for this reason, shorter than the MTPD of the service. This MTPD can only be met when its underlaying parts can be restored faster after a disaster.

In addition, we also determine an MTPD for each Service Component and platform based on turnover and dependency of network management for the asset. In the same manner the MTPD of a Service Component defines the RTO of its underlaying service components and platforms, this in turn defines the RTO of their dependencies also. See figure 1 for a scheme of this hierarchy defining RTO's.

It is extremely important that all assets on which a service, service component and a platform depend are known and registered. Otherwise some continuity risks to the services might be overlooked. A valuable check can be done by verifying if all assets managed by the company are present in the hierarchy. Assets that are not present in the hierarchy may constitute a continuity risk. To do this verification, a complete inventory of all assets is essential.

When a new asset is being conceived, its RTO can be defined by the requirements of existing assets that will depend on the new asset.

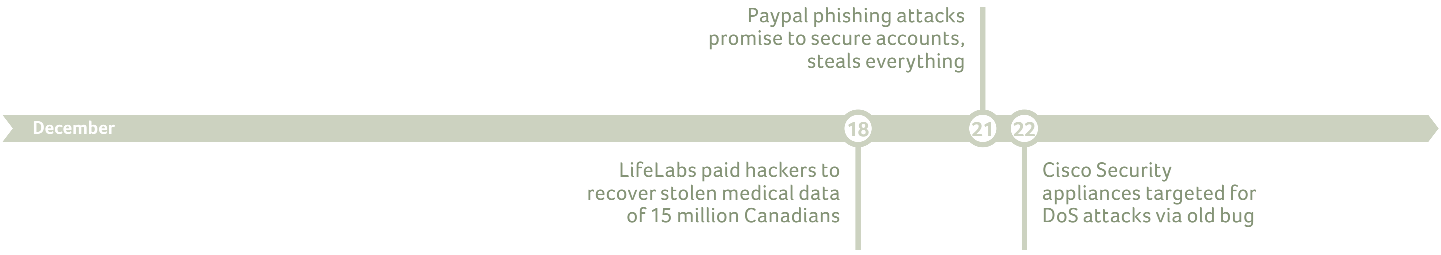
Assess the classification of the assets

Each asset in the hierarchy has RTOs from other assets depending on it. The lowest RTO specified for this asset is leading. The lowest RTO defines the classification level. For this purpose we have build a dedicated application for supporting the classification and registration process, in which all assets are defined with a scope description and all its dependencies. This application supports the classification of each asset by means of a BIA and requests the specification of an RTO for each underlying asset it depends on. The application automatically determines the lowest RTO specified from other assets depending on it together with the intrinsic MTPD of the asset itself (in the case of service components), and the corresponding classification.

Go top down securing your assets!

If you know the RTOs of all assets needed for the external and internal services, a ranking list of assets based on RTO from low to high can be compiled. Depending of the prioritisation and therefore the criticality of the assets, resilience measures can be taken for availability (such as geographic redundancy), confidentiality (such as hardening) and integrity (such as checksums and back-ups). In many cases a restore on new hardware will be accomplished within one week, even when no spares are present, as long as a regular back-up scheme is in place. If budget allows, measures can also be taken for assets with an RTO of one week or more.

In this way you can create an appropriate business resilience at minimal cost.



Paypal phishing attacks promise to secure accounts, steals everything

LifeLabs paid hackers to recover stolen medical data of 15 million Canadians

Cisco Security appliances targeted for DoS attacks via old bug

Overview contributing partners

kpn

KPN is the largest telecom and IT service provider in the Netherlands. We make life more free, easy and more fun by connecting people. We are passionate about offering secure, reliable and future-proof networks and services, enabling people to be connected anytime, anywhere, whilst at the same time creating a more prosperous and cleaner world. We've been doing this on the basis of a strong vision. Every day, for more than 130 years. We bring people closer to their loved ones, connect everything and everyone, we make working and doing business easier and we ensure that people can connect and stay connected anywhere.

National Cyber Security Centre
Ministry of Justice and Security

The National Cyber Security Centre (NCSC) is the central information hub and centre of expertise for cyber security in the Netherlands. NCSC's mission is to contribute to the enhancement of the resilience of Dutch society in the digital domain, and thus to create a secure, open and stable information society. On an international level the NCSC is the Dutch point of contact in the field of ICT threats and cyber security incidents. The NCSC is also a key figure in the operational coordination during a major ICT crisis and the Computer Emergency Response Team (CERT) for the Dutch central government and the critical infrastructures. The coming years we will foster and strengthen the existing cooperation and information exchange with the Dutch central government and the providers of the critical infrastructures and services. While at the same time expand the range by creating a nationwide network of cybersecurity partnerships. The aim of this nationwide network is to strengthen the capabilities of both public and private parties.

Deloitte.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people. At PwC in the Netherlands over 5,000 people work together. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.nl.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

IDQ

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organisations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries - such as security, encryption and online gaming - where trust is paramount. IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. As a privately held Swiss company focused on sustainable growth, IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners. For more information, please visit http://www.idquantique.com/.

accenture

Accenture Security helps organisations build resilience from the inside out, so they can confidently drive innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organisations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defence, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown.
Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

ANALYZEDATA

AnalyzeData provides a broad spectrum of services to help you bring added value to your products/services based on data. No modern company can afford to not do data. If you are not leveraging your data to gain benefits, your competitors are! Unfortunately, data analysis can be hard requiring large upfront investments in time, staff, and money. AnalyzeData wants to change that by providing you in house expertise and services to bring your data awareness to the next level."

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Eindhoven University of Technology (TU/e) is a research university specializing in engineering science & technology. The TU/e profiles itself as a leading, international, in engineering science & technology specialized university. We offer excellent teaching and research and thereby contribute to the advancement of technical sciences and research to the developing of technological innovations and the growth of wealth and prosperity both in its own region (technology & innovation hotspot Eindhoven) and beyond.

Cyber attack against the University Maastricht

Entercom radio network hit by second cyber attack this year

December

23 24

Unauthenticated remote code execution vulnerability in Citrix ADCs and gateways

TNO, The Netherlands Organisation for Applied Scientific Research, is one of Europe's leading independent R&D organisations. TNO is a non-profit and operates independently and objectively. Its unique position is attributable to its versatility and the capacity to integrate knowledge across specialist disciplines. TNO innovates for a secure cyberspace and provides cyber security research, development, engineering and consultancy services to government and industry. Its partners include Dutch government agencies and private sector companies across Europe, including many providers of national critical infrastructure (a.o. in telecoms, finance and energy).

The Faculty of Governance and Global Affairs is an internationally acclaimed academic knowledge hub that studies world-wide issues from the varied perspectives of governance, politics, law, sociology and economics.

We contribute to far-reaching socio-cultural debate through our acquired knowledge. We aim to do this not only through education and research, but also by organising lectures and debates to learn from.

Our faculty has an entrepreneurial mind set, expressed through a continuous quest for links with other academic disciplines and innovative educational methods.

Radboud University is a comprehensive, internationally-oriented university that aspires to be one of the best in Europe. Together with Radboudumc, we have created an intellectual environment that inspires and challenges our students and staff so that they can extend the scope of academic disciplines and benefit society.

Radboud University challenges its students to actively participate in the academic community and trains them to be critical and committed academics, with their own views regarding scholarship and society, who will take up responsible positions in a society which is becoming increasingly internationalised.

The university's academic staff come from all over the world, and a large proportion of our student population has spent at least some months studying at a university abroad.

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organisations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices.
Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

We're a group of highly ambitious craftsmen. From strategy to technology implementation, Xebia is a one-stop shop for full stack digital transformation.

We provide innovative solutions and services to help your organisation become a digital winner.

We're organized in specialized centers of excellence all over the world. We are like-minded individuals who aim for authority in our respective fields.

NLnet Labs is a not-for-profit foundation with a long heritage in research and development, Internet architecture and governance, as well as stability and security in the area of DNS and inter-domain routing. For many years we have been responsible for several widely used and well respected DNS implementations: the authoritative nameserver NSD and the validating recursive resolver Unbound. In the area of inter-domain routing, we develop a full featured RPKI toolset, named Krill and Routinator, to help prevent BGP hijacking. NLnet Labs promotes open source software development and open standards. We actively contribute to the Internet Engineering Task Force, with several published RFCs carrying our name. We also play an active role in Internet governance, offering independent advice to governments and regulatory bodies to sustain a safe and stable DNS and inter-domain routing infrastructure.

Ever since it was founded in 1880, VU Amsterdam has been known for its distinctive approach to knowledge. VU is an open organisation, strongly linked to people and society. What matters is not just the acquisition of a greater depth of knowledge, but also a wider one. We ask and expect our students, researchers, PhD candidates and employees to look further – to look further than their own interests and their own field, and further than what is familiar and further than the here and now.

December

25 Researchers demonstrate chip-to-chip Quantum teleportation

26 Dutch teenage hacker prosecuted for DDoS attacks

@KPNCISO
@_SectorC

Github
https://github.com/kpn-ciso

CISO apps
https://itunes.apple.com/nl/app/kpn-ciso/id1122223795?mt=8

https://play.google.com/store/apps/details?id=com.kpn.ksp&hl=en_US

KPN
@KPN
https://overons.kpn/nl