Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341,
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61, Web: www.cyber-risk-gmbh.com

Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

November 2017, cyber risk and compliance in Switzerland

We have the 25th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI). This is an excellent paper.

It is not a technical paper. The board of directors, the CEO and senior managers must also understand the threats *and* the modus operandi of the attackers.

Published on 2 November 2017, the paper addresses the most important cyber incidents of the first half of 2017, both in Switzerland and abroad. The encryption Trojans Wanna Cry and NotPetya, which made the headlines worldwide in spring 2017, are the focal point of the report.

According to the MELANI report, in the first half of 2017 there was a significant increase in emails used to distribute malicious software which allegedly were sent by federal offices and well-known companies.

This included an email which apparently came from the Federal Tax Administration (FTA) which held out the prospect of tax refunds.

In another case, court summonses were sent which appeared to be from the cantonal police.

Companies such as DHL, Swiss Post and Swisscom are regularly misused for emails which fake a high level of integrity.

Years before, in its semi-annual report 2012/2, MELANI warned of the risks brought by the increasing inclusion of third-party content in websites.

Media portals are often the number one target, as they have linked videos, advertising, and posts leading to social networks.

At this point, MELANI reported visitor infections from such media portals *on numerous occasions.*

In spring 2017, Swiss news portals were attacked once again. In March, 20min.ch reported that unauthorised parties had managed to access their online portal in order to place malicious scripts. A similar incident occurred again at pctipp.ch in April. A smuggled script was used to try to redirect online readers to sites containing malware.

Media portals are of interest to attackers, because their high number of visitors means they reach a large range of potential targets.

An example of this, was the massive malvertising campaign ran by the group known as AdGholas. With the help of so-called exploit kits, tailor-made malware is distributed to the victim.

In the report there are some interesting tricks, that have been used by hackers, criminals, spies, but also advertisers:

MacOS operating system users should be prepared for malware attacks via Microsoft Office documents: security researchers have discovered Word documents in circulation which contain macros specifically designed for MacOS.

If a user opens a manipulated document and allows the macro function to be activated despite the warning notice, the malware it contains will verify whether the Little Snitch safety tool is active.

If this is not the case, malicious code is downloaded and a backdoor is installed on the Mac.

Other attacks on MacOS contained a ZIP file attachment which allegedly contained the detailed invoice for a supposed order. The aim was to install the Retefe banking Trojan on these computers.

Retefe is a malicious program well-known in Switzerland, which attackers, until now, had only used on Windows operating systems.

In order to determine a particular victim's operating system and install the correct version of the malicious software, the criminals first attempt to send an unsuspicious email which automatically provides the attacker with the required information.

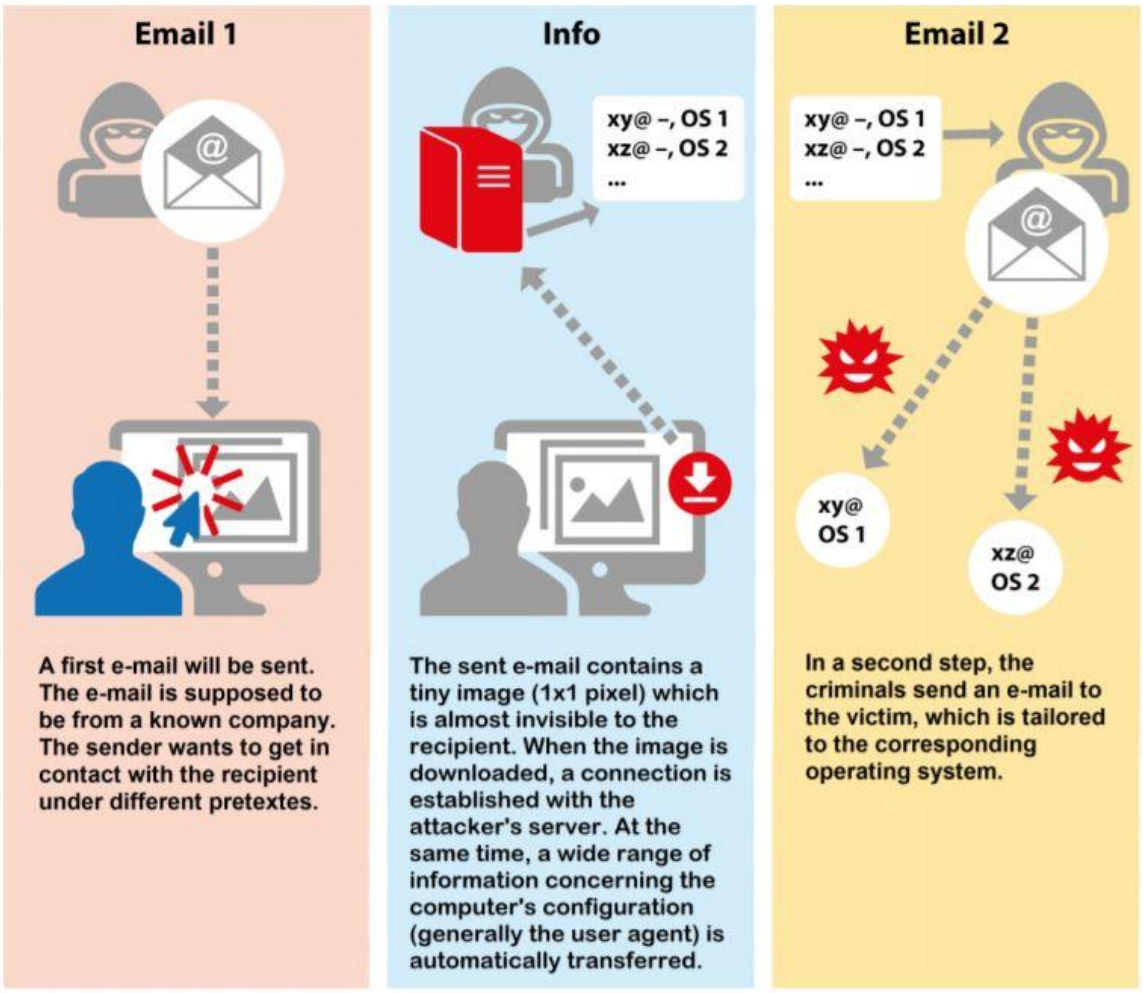


Figure 7 Schematic process: how fraudsters determine which operating system a particular victim has

The email contains a tiny image (1x1 pixel) which is almost invisible to the recipient of the email. When the image is downloaded (which can happen automatically depending on the email configuration), a connection is established with the attacker's server where the image is stored.

At the same time, a wide range of information concerning the computer's configuration, including information on the operating system being used, is automatically transferred.

This allows the criminals to link the email address with the computer's

configuration. In a second stage, they then send an email which is designed for the relevant operating system.

You must read the report:
www.newsd.admin.ch/newsd/message/attachments/50180.pdf

Welcome to our monthly newsletter.

Best Regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our catalog, *in-house* instructor-led training in Switzerland:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

Our events and *open* instructor-led classes:
www.cyber-risk-gmbh.com/Events.html

Number 1 (Page 9)

An overview of the Wi-Fi WPA2 vulnerability

A security researcher discovered and disclosed a serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol, which is used by all modern, protected Wi-Fi enabled devices.

The vulnerability enables an attacker to modify the protocol's handshake, which can essentially lead to intercepting the internet traffic of a Wi-Fi network -and depending on the network configuration, it is also possible to inject and/or manipulate data, without owning or breaking its password security.

The vulnerability is serious, has a very big attack surface but it also has its limitations: it cannot be performed remotely.

Number 2 (Page 15)

Bad Rabbit ransomware

'Bad Rabbit' ransomware infections have been reported in countries including Russia, Ukraine, Bulgaria, Turkey, Germany and Japan.

The NCSC has not received any reports that the UK has been affected by this latest malware attack. The majority of infections have been in Russia, where media organisations were worst affected. Russia's Interfax News Agency suffered outages to several of its services, including its news portal. Ukrainian victims included the Ministry of Infrastructure, Odessa airport and Kiev metro.

Bad Rabbit asks victims to pay 0.05 Bitcoin (currently worth approximately £210) to restore their files.

Number 3 (Page 17)

Fifth BCBS-FSI-BSCEE high-level meeting on supervisory priorities in Europe, Basel, Switzerland.

Fifty-two senior representatives from 30 European jurisdictions discussed topical banking regulatory and supervisory issues such as proportionality in banking regulation; identification, measurement and resolution of non-performing loans (NPLs); implementation of the post-crisis banking resolution framework; and regulation and supervision of cybersecurity.

Number 4 (Page 20)

Li-Fi technology offers benefits in mobility, speed, cost, security

Light fidelity, or Li-Fi, is a ground-breaking light-based communication technology which makes use of light waves instead of radio technology to deliver data.

Li-Fi is a bidirectional, high-speed, and fully networked wireless communication technology similar to Wi-Fi, but capable of 10 times faster transmission rates from point to point.

“Li-Fi technology has the potential of being faster than any radio based technology existing at present,” said Dr. Bill Butler, project lead for the DISA Li-Fi University Affiliated Research Center (UARC) Project.

Number 5 (Page 23)

The Internet of Things: when your washing machine and blood pressure monitor become a target for cyberattacks

Europol-ENISA conference tackles security challenges of IoT

With at least 20 billion devices expected to be connected to the internet by 2020, the Internet of Things (IoT) is here to stay. While it has many undeniable positive effects, the threats and risks related to the IoT are manifold and they evolve rapidly.

For this reason, ENISA and Europol joined forces to tackle these security challenges by organising a dedicated two-day conference on 18 and 19 October 2017, which was attended by more than 250 participants from the private sector, security community, law enforcement, the European Computer Security Incident Response Teams (CSIRT) community and academia.

Number 6 (Page 25)

Clear Talk for First Responders

NIST modeling tool to help advance cellular emergency communications

For first responders, such as firefighters, police officers and emergency medical technicians, a successful outcome to a mission—and perhaps the difference between life and death for them and those they are helping—depends on their communications system.

Recognizing this critical need, first responders and emergency management officials have been calling for high-speed, LTE (Long-Term Evolution) cellular devices with three public safety "mission-critical voice" capabilities: "push-to-talk" for an immediate connection, "one-to-many" allowing an individual to broadcast to a large group, and "direct mode" that maintains a walkie-talkie connection when a wireless network is down, blocked or otherwise unavailable.

Number 7 (Page 28)

Code-signing certificates worth more than guns on the Dark Web

National Cyber Security Centre
a part of GCHQ

An investigation by a company specialising in identity protection solutions, into the sale of code-signing certificates on the Dark Web suggests they are selling for up to $1,200, making them more expensive than fake driver's licences, stolen credit cards, commissioning a targeted cyber attack, or even buying a handgun.

This relatively high price presumably reflects customer demand.

Number 1

An overview of the Wi-Fi WPA2 vulnerability

What happened?

A security researcher discovered and disclosed a serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol, which is used by all modern, protected Wi-Fi enabled devices.

The vulnerability enables an attacker to modify the protocol's handshake, which can essentially lead to intercepting the internet traffic of a Wi-Fi network -and depending on the network configuration, it is also possible to inject and/or manipulate data, without owning or breaking its password security.

The vulnerability is serious, has a very big attack surface but it also has its limitations: it cannot be performed remotely.

It can be performed only when the attacker has physical proximity to the victim. There are already ways that people can protect themselves from the attack while waiting for security patches to be released for their devices.

The severity of the issue should not be underestimated, albeit people should not panic as well.

The biggest issue raised by this vulnerability -given its scale - is the fact that a vast majority of affected devices, e.g. smart devices, IoT, routers etc., might never receive a patch addressing the issue.

This note provides an overview of the vulnerability, and some basic recommendations that can be followed whilst patches are rolled out by the various manufacturers/vendors.

Overview of the vulnerability and attack

The identified weakness is in the Wi-Fi standard itself, and not in individual products or implementations.

Hence, according to the researcher, any correct implementation of WPA2 is likely affected (list of affected vendors).

The attack against the vulnerability is dubbed KRACK (Key Reinstallation Attack) and enables an attacker to attack the 4-way handshake of the WPA2 protocol, i.e. the initiation of the WPA2 connection.

This handshake takes place every time a client wants to join a WPA2 Wi-Fi protected network in order to confirm that the client and access point hold the correct credentials, i.e. Wi-Fi password, before the client joins the network.

During the same 4-way handshake a fresh encryption key, which is used for encrypting subsequent traffic is established.

By manipulating this 4-way handshake an attacker can trick a victim into reinstalling an already-in-use encryption key, while a key should only be installed and used once.

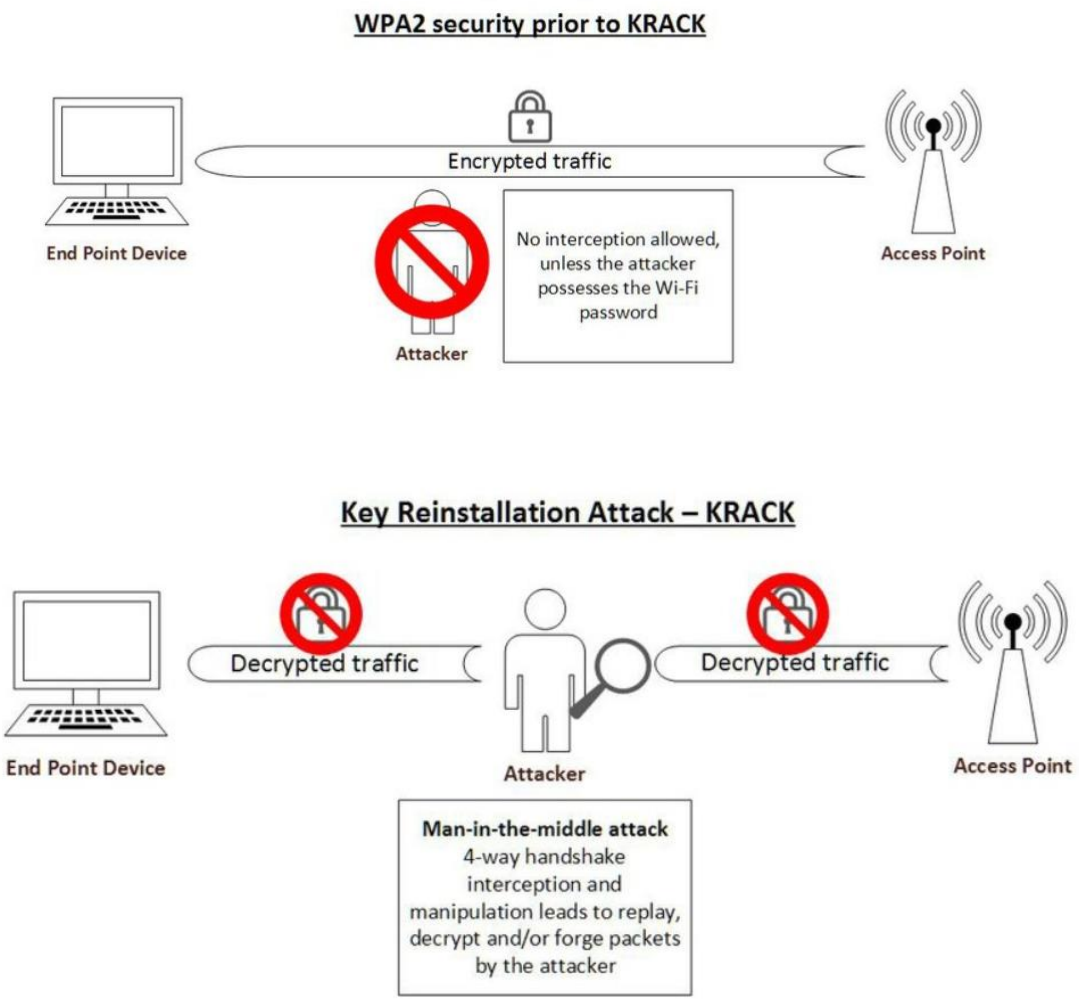
Reinstalling an encryption key, forces two counters (known as “nonces”) used by the encryption protocol to reset and this enables an attack against the protocol e.g. replay, decrypt and/or forge packets.

A potential attacker who is in the physical proximity of a protected Wi-Fi network and carries out this attack, performs a man-in-the-middle attack.

The attacker can essentially intercept/decrypt internet traffic without owning the credentials of the protected Wi-Fi network (therefore changing the Wi-Fi password won’t help).

This attack can further be combined with downgrade attacks against SSL/TLS websites (that have not applied security measures against downgrade attacks) in order to turn an HTTPS connection to HTTP and steal more sensitive information.

The Key Reinstallation Attack is illustrated in the simplified figure below:



The attack works against personal and enterprise Wi-Fi networks, against the original WPA, WPA2, and even against networks that only use AES, i.e. pretty much most Wi-Fi network setups.

For the technical interested audience, the researcher who discovered the vulnerability noted that the same key reinstallation technique can also be used to attack the group key, PeerKey, TDLS, and fast BSS transition handshakes as well.

The researcher describes the vulnerability in the paper called “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, which is a highly technical paper for those interested in the details of the attack.

To read it: https://papers.mathyvanhoef.com/ccs2017.pdf

Additionally, the researcher provided a video with a proof-of-concept attack against an Android smartphone.

Lines to take

- Despite the fact that vulnerability is present in the Wi-Fi standard and thus affects a very large number of devices, do not panic!

- The WPA2 vulnerability is severe and provides a big attack surface but it can only be exploited within the physical proximity of the target Wi-Fi network and not remotely through the Internet, which reduces its impact.

- WPA2 is only one of the available layers of security impacted. Keep in mind that properly configured websites, e.g. usually banks, e-mail providers, social media etc. that use TLS (HTTPS) are still protected from such an attack.

- There is no evidence that the vulnerability has been exploited in the wild and it is uncertain of how easily this vulnerability can be exploited.

- WPA2 is still a more secure solution compared to WEP -the previous Wi-Fi protocol. Hence, switching to an older -trivially exploitable- protocol, is highly discouraged. It is better to continue using WPA2 when using Wi-Fi.

- Avoiding WPA2 protected Wi-Fi networks all together is highly unrealistic. Thus, in such cases people should be pragmatic, apply available security measures or use 4G mobile internet connections, while waiting for manufacturers to prepare and push patches for their devices.

- The issue can be resolved with software/firmware updates. Check with the manufacturer/vendor for each of your Wi-Fi enabled devices and apply patches as soon as they become available. Manufacturer readiness on such issues should be a weighting factor for purchasing technological devices. Home users who obtain their routers from their broadband providers should contact their provider and check whether there is a patch available for their equipment and ask for installation instructions.

- Whenever possible use a 4G mobile internet connection instead of a Wi-Fi connection.

- While waiting for patches, you may treat all Wi-Fi networks like public, open and insecure networks. Therefore, apply security measures on different layers. This is an essential rule in security and quite effective in this case as well.

  Namely:

  a. Use only HTTPS websites. Refrain from using simple HTTP websites and sharing personal information through them. Consider using a browser extension like HTTPS Everywhere, which forces any site that supports HTTPS connections to encrypt your communications with that website by default

  b. Use a trusted Virtual Private Network – VPN provider. VPNs establish an encrypted tunnel between an endpoint and the trusted provider, protecting internet traffic routed through untrusted networks. This means that by using a VPN, an attacker that carries out KRACK cannot intercept the user's traffic. Keep in mind that choosing a trusted VPN provider is crucial when using a commercial VPN solution.

- Organisations should separate their wireless networks from their enterprise, wired networks.

Relevant ENISA actions

In the last years ENISA has invested a lot of resources in the Telecom area. Since 2011 a considerable number of guidelines/studies have been produced and more than 700 incidents have been collected and analysed. All those were made possible through the support of the Art. 13a Expert Group, a dedicated security group made of national authorities across EU.

In the case of the WPA2 vulnerability, an ad-hoc cooperation initiative started within the group, and the results can be summarised at this point as follows:

- All Member States regulatory authorities are aware of the seriousness of the situation; they have issued warnings, alerts or other relevant information that include also recommendations for end users;

- A dialog has been established between authorities and telecommunication providers (ISP) at national level in order to identify specific risks within each context (e.g. main types of routers used in

each country, if patches have been released etc.) and actions taken by providers.

Closing Remarks

Every time a vulnerability affects the security of a network or a cryptographic protocol a wide range of devices or services are potentially put at risk. In such cases it is useful not to panic and carefully assess the theoretical and practical risk of the vulnerability.

Having said that, it is advised to also take into account the available security measures, in order to determine the vulnerability's potential impact.

One of the main issues and challenges raised by this vulnerability is the state of readiness of manufacturers to respond to such incidents, prepare, push patches to their products in a timely manner, and not leave their products vulnerable.

As internet connected devices are becoming ubiquitous, it is essential to work on keeping this ecosystem protected since we have already experienced security incidents that aim to undermine the state of cyber security.

Number 2

Bad Rabbit ransomware

National Cyber Security Centre
a part of GCHQ

'Bad Rabbit' ransomware infections have been reported in countries including Russia, Ukraine, Bulgaria, Turkey, Germany and Japan.

The NCSC has not received any reports that the UK has been affected by this latest malware attack. The majority of infections have been in Russia, where media organisations were worst affected. Russia's Interfax News Agency suffered outages to several of its services, including its news portal. Ukrainian victims included the Ministry of Infrastructure, Odessa airport and Kiev metro.

Bad Rabbit asks victims to pay 0.05 Bitcoin (currently worth approximately £210) to restore their files.

A small number of transactions are reported to have been made, although these are unconfirmed, and it is currently unknown whether paying the ransom leads to decryption of files.

The infection vector is believed to be via certain compromised media websites in the affected regions, which asks the user to execute a fake Adobe Flash Player update.

Researchers including FireEye and Crowdstrike have identified several links between Bad Rabbit and the NotPetya ransomware, including the use of similar Javascript code to redirect victims.

While claims have been made that Bad Rabbit made use of the EternalBlue exploit leveraged by WannaCry and NotPetya, these have been widely refuted; subsequent claims have been made that the EternalRomance exploit was leveraged.

It is currently unclear who is responsible for this ransomware. NCSC technical analysis is ongoing to provide more clarity on technical indicators. There are no reported UK victims to date.

Nevertheless, it should be noted that UK organisations would be vulnerable were they to visit any of the infected websites. In the case of NotPetya for instance, a number of UK organisations were infected.

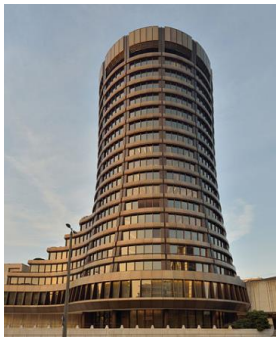
The NCSC has provided some mitigation advice in its public statement, highlighting the importance of patching, using proper antivirus services and having effective backup procedures. To read the advice: https://www.ncsc.gov.uk/news/statement-bad-rabbit-malware-incident

In addition to this, Bad Rabbit makes use of a set of hard-coded username/password combinations in order to attempt to spread to SMB shares on the local network.

Organisations should ensure that these username/password combinations do not exist anywhere on their network, and in general that they follow good password practices (as per NCSC password guidance at https://www.ncsc.gov.uk/guidance/password-collection).

Number 3

Fifth BCBS-FSI-BSCEE high-level meeting on supervisory priorities in Europe, Basel, Switzerland.



The Basel Committee on Banking Supervision (BCBS), the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS) and the Group of Banking Supervisors from Central and Eastern Europe (BSCEE) jointly organised the fifth high-level meeting on supervisory priorities in Europe at the BIS in Basel on 18-19 October 2017.

The event was co-chaired by Mr Fernando Restoy, FSI Chair, and Mr William Coen, BCBS Secretary General, and attended by Ms Helen Mashnina in representation of the Chair of the BSCEE group.

Fifty-two senior representatives from 30 European jurisdictions discussed topical banking regulatory and supervisory issues such as proportionality in banking regulation; identification, measurement and resolution of non-performing loans (NPLs); implementation of the post-crisis banking resolution framework; and regulation and supervision of cybersecurity.

In his opening address, Mr Claudio Borio, Head of the Monetary and Economic Department at the BIS, shared his views on prospects for financial stability in Europe and worldwide.

He elaborated on the implications of three long-term trends, termed the "risky trinity": declining labour productivity growth, rising global debt and narrowing policy room for manoeuvre.

He noted the types of risk faced in a number of countries less affected by the Great Financial Crisis, in the form of a build-up of traditional financial imbalances, and those in some countries most affected by it, in the form of incomplete balance sheet and bank repair. He highlighted the possible risk of a debt trap.

In her keynote address, Ms Danièle Nouy, Chair of the Supervisory Board of the European Central Bank, argued that Europe chose the right regulatory and supervisory response to the financial crisis.

The revamped European rulebook for banks as well as the European banking supervisory and resolution frameworks have made banks safer and sounder, and reduced the likelihood of future crises.

At the same time, they have helped to level the playing field for banks and set the ground for a truly European banking sector.

However, Ms Nouy also pointed out that more needs to be done: a European deposit insurance scheme needs to be set up and the rulebook for banks needs to be harmonised further.

Mr Andrea Enria, Chairperson of the European Banking Authority, highlighted the importance of accurate valuation for both going- and gone-concern supervision.

He noted that there have been improvements in addressing the "too little too late" concern of the G20, thanks to more forward-looking valuations and enhanced transparency to foster market discipline.

However, he also underlined that accounting valuation is a necessary but not sufficient step to address all supervisory concerns, especially those related to NPLs.

Therefore, Mr Enria indicated that supervisors, through their own mandates, can and should actively encourage banks not only to make realistic valuations, but also to take proactive steps to address potential weaknesses.

In his concluding remarks, Mr Restoy stressed that with the post-crisis regulatory reforms nearing completion, the international regulatory community is now shifting emphasis from regulation to effective implementation.

In this context, he emphasised the importance of facilitating the exchange of experiences and approaches among supervisors, to ensure that sound practices are disseminated throughout the global supervisory community.

Note

The FSI was jointly created in 1998 by the BIS and the BCBS to assist supervisors around the world in improving and strengthening their financial systems.

The FSI achieves its mandate through its policy implementation work, in particular the FSI Insights publications; outreach events to senior officials such as high-level meetings, policy implementation meetings and conferences; and FSI Connect, the BIS's web-based learning tool for financial sector supervisors.

For further information on the FSI, visit www.bis.org/fsi

Number 4

Li-Fi technology offers benefits in mobility, speed, cost, security

Light fidelity, or Li-Fi, is a ground-breaking light-based communication technology which makes use of light waves instead of radio technology to deliver data.

Li-Fi is a bidirectional, high-speed, and fully networked wireless communication technology similar to Wi-Fi, but capable of 10 times faster transmission rates from point to point.

"Li-Fi technology has the potential of being faster than any radio based technology existing at present," said Dr. Bill Butler, project lead for the DISA Li-Fi University Affiliated Research Center (UARC) Project. "With Wi-Fi, all devices are fighting for the same 800 megabits per second (Mbps) of bandwidth. With Li-Fi, the entire visible and non-visible light spectrum is available for use - laying the groundwork for 10 gigabits per second (Gbps) transmission rates within the next calendar year."

Li-Fi can provide the military with high speed, non-detectable communications that cannot be identified through current direction-finding technology. The high-speed, multi-frequency communication capability inherent in Li-Fi can free up bandwidths used in critical legacy applications that haven't converted to newer technology.

With Li-Fi, inter-soldier, inter-vehicle, and inter-ship line-of-sight communications can render mobile units ubiquitous relays of information and orders without any verbal communication, while remaining totally invisible in the battlespace.

Li-Fi will be especially valuable in commercial applications, such as communication between cars and other vehicles requiring integrated high-speed motion detection; in hospitals, where radio waves interfere with delicate instrumentation; in airplane environments, where radio frequencies (RF) can interfere with navigation equipment; and in

construction, where heavy explosives are currently detonated through radio signals.

How it works

According to Dr. Butler, "light is already used for data transmission in fiber-optic cables and for point-to-point links, but Li-Fi is a special and novel combination of technologies that allow it to be universally adopted for mobile ultra-high speed internet communications using normal light frequencies across the 440 to 770 terahertz (THz) spectrum. However, Li-Fi can also be used in the non-visible frequencies, such as infrared, X-ray, and ultra-violet frequencies between 300 gigahertz (GHz) to 400 THz - presenting endless possibilities for manufacturing new and complex communication equipment."

Li-Fi uses a photo-detector to receive light signals and a signal processing element to convert the data into 'streaming binary digital' content.

An LED lightbulb is a semi-conductor light source, meaning that the constant current of electricity supplied to an LED lightbulb can be dipped and dimmed, up and down at extremely high speeds, without being visible to the human eye.

For example, data is fed into an LED light bulb (with signal processing technology), it then sends data (embedded in its beam) at rapid speeds to the photo-detector (photodiode). The tiny changes in the rapid dimming of LED bulbs is then converted by the 'receiver' into electrical signal.

The signal is then converted back into a binary data stream that we would recognize as web, video, and audio applications running on internet enabled devices.

Benefits

"Li-Fi offers benefits in mobility, speed, cost, and, most importantly, security," said Dr. Butler.

Currently available Li-Fi commercial products run on visible light, and because light cannot penetrate through solid walls, signals can't be intercepted while being transmitted - unlike traditional radio frequencies. This is a critical advantage when it comes to protecting classified and sensitive DOD missions.

"In battlefields, Li-Fi can be used for vehicle-to-vehicle communications through the use of headlights and taillights without system interference, and the data is secure because information is only transmitted to those in the line of direct sight. It can also replace the complex cabling required in forward-deployed command centers by combining the network access points in the overhead lighting. This reduces power consumption and simplifies command center setups," said Dr. Butler. "Additionally, there is greater bandwidth availability in light waves than radio waves, and the transmission of data using LEDs is highly energy efficient."

On the Horizon

DISA is in the early stages of exploring Li-Fi technology and the applicable uses for DOD. The technology was demonstrated in a classified work environment and initial pilots confirmed Li-Fi provided secure networked communication within an enclosed space.

"Right now, we are working to procure equipment and configure a demonstration of Li-Fi within a secure, multipoint networked environment," said Dr. Butler. "We will continue to work with our academia partnerships to explore and prototype the next-generation DODIN and move the DOD towards a wireless non-RF complimentary environment."

In the future, Li-Fi may be offered as an enterprise service for secure environments, and may also serve as a solution for other communication requirements.

Data for laptops, smart phones, and tablets is transmitted through the light in a room using diodes pulsing at extremely high speeds undetectable to the human eye. Security is established through direct light transmission, therefore if you are not in the amplified light network you can't access the data or other networked appliances.

Note

DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations.

Number 5

The Internet of Things: when your washing machine and blood pressure monitor become a target for cyberattacks

Europol-ENISA conference tackles security challenges of IoT

With at least 20 billion devices expected to be connected to the internet by 2020, the Internet of Things (IoT) is here to stay.

While it has many undeniable positive effects, the threats and risks related to the IoT are manifold and they evolve rapidly.

For this reason, ENISA and Europol joined forces to tackle these security challenges by organising a dedicated two-day conference on 18 and 19 October 2017, which was attended by more than 250 participants from the private sector, security community, law enforcement, the European Computer Security Incident Response Teams (CSIRT) community and academia.

The Internet of Things is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context.

In simpler words, it makes our cameras, televisions, washing machines and heating systems 'smart' and creates new opportunities for the way we work, interact and communicate, and how devices react and adapt to us.

It is important to understand how these connected devices need to be secured and to develop and implement adequate security measures to protect the Internet of Things from cyber threats.

Beyond technical measures, the adoption of IoT has raised many new legal, policy and regulatory challenges, broad and complex in scope. In order to address these challenges, cooperation across different sectors and among different stakeholders is essential.

The risk of criminals 'weaponising' insecure IoT devices was already identified in the 2014 and 2015 editions of Europol's Internet Organised

Crime Threat Assessments and in ENISA's 2016 Threat Landscape Report. It became a reality at the end of 2016 with several DDoS attacks of unprecedented scale originating from the Mirai botnet.

It must be assumed that cybercriminals will develop new variants and enlarge the variety of IoT devices affected by this type of malware.

This joint Europol-ENISA conference, the first one on the topic, provided the opportunity for all the relevant stakeholders to come together, discuss the challenges faced and identify possible solutions, building on existing initiatives and frameworks. A specific focus was on the role of law enforcement in responding to the criminal abuse of the IoT.

The two-day meeting was testimony to the willingness of all the relevant international actors to ensure that the many benefits of the IoT can be fully realised by jointly addressing the security challenges and combating the criminal abuse of such devices, ultimately making cyberspace a safer place for all.

To read more:
https://www.enisa.europa.eu/news/enisa-news/the-internet-of-things-when-your-washing-machine-and-blood-pressure-monitor-become-a-target-for-cyberattacks

Number 6

Clear Talk for First Responders

NIST modeling tool to help advance cellular emergency communications

For first responders, such as firefighters, police officers and emergency medical technicians, a successful outcome to a mission—and perhaps the difference between life and death for them and those they are helping—depends on their communications system.

Recognizing this critical need, first responders and emergency management officials have been calling for high-speed, LTE (Long-Term Evolution) cellular devices with three public safety "mission-critical voice" capabilities: "push-to-talk" for an immediate connection, "one-to-many" allowing an individual to broadcast to a large group, and "direct mode" that maintains a walkie-talkie connection when a wireless network is down, blocked or otherwise unavailable.

To make this technology work effectively and ensure consistent product quality, the experts have already started developing standards.

There's just one catch: a device that employs all of these desired features doesn't yet exist. And without a working device to scientifically evaluate in different emergency situations, it hasn't been easy to design the standards that will optimize its performance.

So, to keep mission-critical voice communications development and standardization moving forward, the National Institute of Standards and Technology (NIST) is putting a new computer modeling tool on the job.

The NIST tool uses ns-3 (https://www.nsnam.org/https://www.nsnam.org/), an open-source network simulation software, giving researchers the ability to virtually recreate any emergency scenario and draw upon a variety of environmental, structural, technological and human behavioral factors that could impact the performance of future LTE cellular devices.

Models produced by the NIST tool address performance issues such as voice traffic: who's talking, blocked or waiting in line to speak at any

moment, and how well is the overall conversation flowing; location: how do first responder movements—such as into and out of buildings, behind trees or next to metal walls—affect transmissions; networking: how easily can additional first responder units join the communications network established by the team initially on the scene; and the use of protocol emergency buttons: how effective are these functions that give first responders the ability to break through ongoing communications to request immediate assistance for victims or themselves.

A graphical user interface (GUI) can be used with the NIST tool so that results from the models can be viewed as animations.

Videos with demonstration scenarios showing first responders and the LTE communications protocol in operation during different types of emergencies are available from NIST.

"We hope that the new modeling tool will be widely used by researchers who want to experiment with different ways to optimize the three key mission-critical voice capabilities, by manufacturers who want to 'field test' device designs without having to build multiple versions, and by emergency management officials who want to educate first responders under their command about the advantages of LTE communications in hazardous situations," said Richard Rouil (link sends e-mail), a computer engineer in NIST's Communications Technology Laboratory (CTL) who helped create the tool.

"Most importantly, the tool makes it possible to develop, test and refine standards for the next generation of emergency response communications devices concurrently with, rather than after their development."

According to Rouil, a collaborative effort with the University of Washington will work toward integrating the NIST module directly into the ns-3 software to enable expansion of the tool's modeling capabilities.

Funding for this project comes from a NIST grant awarded in June 2017 to the University of Washington as part of the Public Safety Innovation Accelerator Program, a technology advancement effort for public safety communications that also is funding the development of the LTE modeling tool.

The Innovation Accelerator Program, managed by NIST CTL's Public Safety Communications Research (PSCR) Division, provides research,

development, testing and evaluation of broadband communications technologies to foster nationwide interoperability among first responders. The NIST LTE Device-to-Device Communication Model for ns-3 is available for downloading (link is external) as is the free ns-3 software (link is external).

A recent NIST paper provides information on the implementation and validation of the model – you may visit: https://www.nist.gov/publications/implementation-and-validation-lte-d2d-model-ns-3

Number 7

Code-signing certificates worth more than guns on the Dark Web

National Cyber Security Centre
a part of GCHQ

An investigation by a company specialising in identity protection solutions, into the sale of code-signing certificates on the Dark Web suggests they are selling for up to $1,200, making them more expensive than fake driver's licences, stolen credit cards, commissioning a targeted cyber attack, or even buying a handgun.

This relatively high price presumably reflects customer demand.

This is not the first time that security researchers have highlighted the issue of stolen or fraudulently obtained code-signing certificates. Since at least 2011, they have noted a trend for both cyber criminals and APT cyber actors to sign their malware using stolen or fraudulently obtained certificates to bypass security measures.

Signed code tends to be treated as trusted and some operating systems will flag up, or refuse to run, code that is not signed.

Over the years, attackers have managed to sign their malicious executables with certificates obtained by a variety of methods – reportedly stealing them from technology companies (including some well-known names), penetrating the networks of companies and using their signing facilities, or applying for certificates in the names of fake companies or real companies who have no need for them.

As far back as 2010, the destructive worm Stuxnet included components that were signed with stolen certificates. More recently, the cyber actors who corrupted an update of clean-up tool CCleaner managed to get the update signed.

Amongst other things, this highlights the fact that, when attackers do manage to penetrate a network, they will often seek out things that facilitate further intrusions – like passwords (not only password caches, but sometimes also emails containing passwords or access codes), cookies, digital certificates and keys. System administrators should make sure they know where these are located.

The NCSC has published guidance to help organisations protect their End User Devices which, when deployed correctly, can help mitigate the risks of malware attacks.

Disclaimer

Cyber Risk GmbH enhances public access to information about cyber risk and compliance in Switzerland.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which Cyber Risk GmbH has no control and for which Cyber Risk GmbH assumes no responsibility;

- is not professional or legal advice);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.