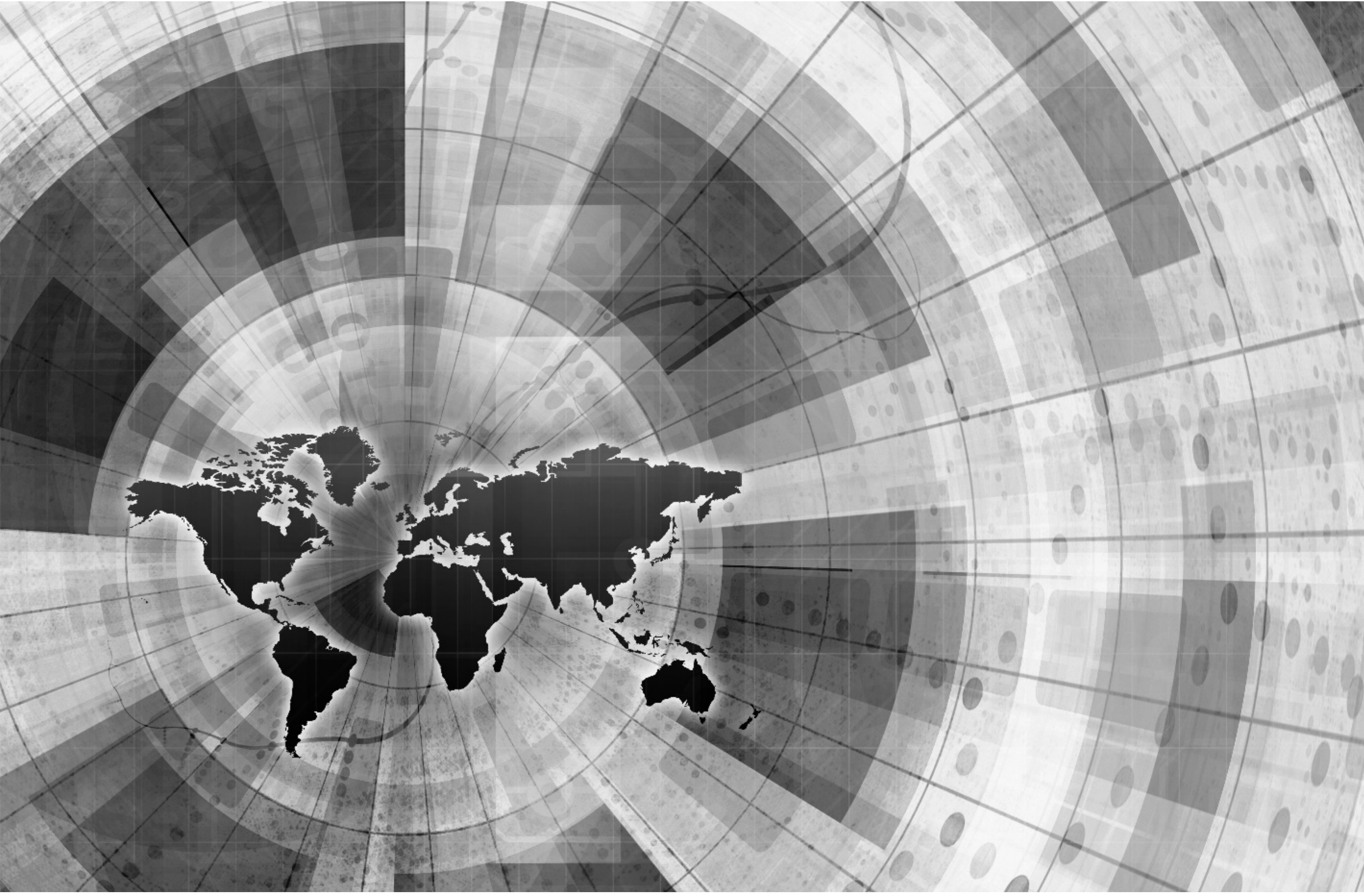


Supply Chain Security

Analysis and measures to secure the digital supply chain

The Supply Chain Security working group of the
Cybersecurity Commission of ICTswitzerland

September 2019

ICTSWITZERLAND

Publication details

ICTswitzerland
Aarbergergasse 30
CH-3011 Berne

Authors:
Dr Stefan Frei, Christof Jungo[1], Daniel Busch[2], Dr Raphael Reischuk

Note:
This report primarily represents the opinion of the advisory group. The report does not necessarily reflect the positions of the members' organisations.

Advisory team:
The Supply Chain Security working group of the Cybersecurity Commission of ICTswitzerland

Dr Stefan Frei	Cyber Security Principal, Accenture Head of the Supply Chain Security working group of ICTswitzerland
Umberto Annino	Head Security Governance, SIX Group
Markus Bischof	Director Europe Security & Trust Organization, Cisco Systems GmbH
Tobias Ellenberger	Board Member, Swiss Cyber Experts Chief Operating Officer, Oneconsult AG
Dr Jon Albert Fanzun	Special Envoy for Cyber-Foreign and Security Policy, Federal Department of Foreign Affairs (FDFA)
Christophe Gerber	Head of Business Line, ELCA Informatique SA
Christian Grasser	Managing Director, asut
Thomas Holderegger	Head of Security IT, UBS AG
Andreas Kaelin	CEO of ICTswitzerland
Uwe Kissmann	Managing Director Cyber Security Services EALA, Accenture Chairman, Cybersecurity Commission of ICTswitzerland
Arié Malz	ICT and Digitalisation Officer, General Secretariat of the Department of Finance
Dr Raphael Reischuk	Head of Cyber Security Services, Zühlke Engineering AG Vice-Chairman, Cybersecurity Commission of ICTswitzerland
Gérald Vernez	Delegate Cyberdefence, Federal Department of Defence, Civil Protection and Sport (DDPS)
Nicole Wettstein	Director of Priority Program Cybersecurity, Swiss Academy of Engineering Sciences (SATW)

[1] SecIntel GmbH
[2] Symantec (Deutschland) GmbH

Executive summary

The Internet is connecting people and machines more and more and has already made a lasting difference to our lives. While the integrity and safety of products from traditional sectors are inspected for certain issues prior to market approval (e.g. in the areas of mobility, food, medicines, etc.), the quality and safety of many digital products is not assured. There are various reasons for this. Today's supply chain security for digital products is often inadequate and undermines the existing security measures. Also, decision-makers are often unable to make sustainable decisions due to a lack of well-founded and transparent information.

As digitalisation progresses, ignorance concerning the level of security of the products used can lead to critical threats. If incompletely tested products are used in critical infrastructures, threats may be widespread and endanger the provision to society in the areas of electricity, medicine, mobility and physical protection. These risks are abstract, have developed slowly and, consequently, were ignored for a long time and continually accumulated until now.

The Supply Chain Security working group analyses how technological risks are dealt with in other sectors (e.g. electricity supply) and, based on this, identifies and documents the measures that are needed for secure digitalisation. The following topics are addressed, among others:

- What are the biggest risks of the digital society and where do they lie?
- What do critical attack scenarios look like and who are the attackers?
- What can and must we – as an industry or as society in general – consider or undertake right away?
- What measures are necessary and helpful to secure the digital supply chain?

As a society, we have a duty to prevent known and avoidable mistakes so that now and in the future the opportunities offered by digitalisation outweigh the risks.

Contents

Initial situation: the digital society

Development and cyber risks

With the growing number of novel interactions between people, machines, services and various feedback processes, the complexity of the networked society is increasing rapidly and continually. In particular, dependencies on hardware and software as well as the purchase of services (direct or delegated) create new risks for critical infrastructures[3]. Security incidents can be triggered by malfunctions or manipulation of hardware or software components, by chance occurrences due to insufficient quality of the development and design of components, or by targeted attacks.

If digital products with security defects find their way into the market, these vulnerabilities may have effects that last for decades. This applies, for example, to permanently installed equipment in industrial and building control systems, and even extends to critical infrastructures.

The properties of a complex, networked system can no longer be inferred from an isolated analysis of the behaviour of individual components. New, often surprising system properties appear, such as self-organisation and "emergence"[4]. A small local disturbance – triggered by a chance occurrence or malfunction – can have unpredictable and distant effects.

Examples:

- Mass influencing of entire societies by social media[5].
- Fitness tracker apps lead to the detection of secret military bases[6].

Cybercriminals and state actors

Digitalisation is actively tracked and exploited by attackers of all kinds. Recently, there has been an increase in attacks aimed at enforcing a political agenda by exploiting the vulnerabilities of the digital society. It is known from history that both intelligence agencies and criminals acquire new technologies very quickly. Throughout history, governments and

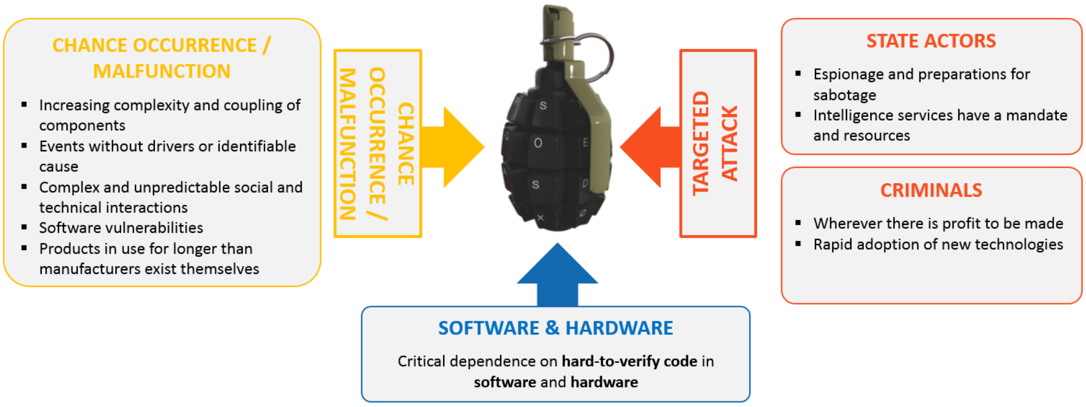
[3] "Critical infrastructures are processes, systems and facilities that are essential for the functioning of the economy and the well-being of the population." (for example: electricity and water supply)
Definition by the Federal Office for Civil Protection (FOCP): https://www.babs.admin.ch/en/aufgabenbabs/ski.html

[4] Complex adaptive systems:
https://en.wikipedia.org/wiki/Complex_adaptive_system

[5] How social networks permeate society (article in German):
https://www.nzz.ch/feuilleton/medien/wie-die-sozialen-netzwerke-die-gesellschaft-praegen-ld.1380183

[6] Fitness tracking app Strava gives away location of secret US army bases:
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

secret services have been involved in espionage and sabotage, and these tactics are increasingly being planned as a part of military defence and attack strategies[7].



CHANCE OCCURRENCE / MALFUNCTION

- Increasing complexity and coupling of components
- Events without drivers or identifiable cause
- Complex and unpredictable social and technical interactions
- Software vulnerabilities
- Products in use for longer than manufacturers exist themselves

STATE ACTORS

- Espionage and preparations for sabotage
- Intelligence services have a mandate and resources

CRIMINALS

- Wherever there is profit to be made
- Rapid adoption of new technologies

SOFTWARE & HARDWARE

Critical dependence on **hard-to-verify code** in **software** and **hardware**

Illustration 1: Threats within the complex system of the digital society – triggered by chance occurrences or targeted attacks.

To assess critical vulnerabilities, the digitalisation of society must be viewed from the attacker's point of view. The following questions help us to assume the right point of view:

- How could an experienced attacker gain the maximum impact and persistence with the least chance of detection?
- How does an attacker proceed if his primary target is very well secured?

Criminal and military history both show that successful attackers would often find the weakest point. The attack is launched just where the defenders least expect it. The compromising of digital products before they are delivered, i.e. during their design, manufacture or at some point in the supply chain, fulfils precisely this criterion for an attack.

Numerous nations are currently expanding their offensive and defensive cyber capabilities. Unlike cybercriminals and other attackers, state governments can . . .

- . . . gain direct access to critical parts of the Internet infrastructure ("the Internet backbone").
- . . . compel service providers or manufacturers by law to cooperate or carry out monitoring.
- . . . systematically and extensively monitor Internet traffic.

[7] Luiijf, E., Besseling, K. and de Graaf, P. (2013) "Nineteen national cyber security strategies", Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, pp. 3–31.

Government-based attackers have above-average resources and the stamina to persistently reach a target via multiple attack channels and for extended periods while remaining undetected. Persistence and accessibility in case of need are the highest goals. The attackers' activities include the hidden introduction of malware and backdoors into the hardware and software of the target systems of other countries (or competitors).

Cybersecurity should not be limited to software and network security, but should include the integrity and security of the hardware and its components, as well as the human factor. Ultimately, most components are installed, configured and operated by people.

Examples:

- Israelis and Americans are said to have jointly developed the computer worm Stuxnet, which paralysed large parts of Iran's nuclear facilities[8].
- After compromising the system of the computer manufacturer ASUS, malware is distributed to the systems of ASUS customers via the automatic update function[9].
- List of significant cyber attacks on government agencies, defence and high tech companies[10].

Digitally "flying blind"

In principle, attacks in the supply chain can neither be excluded nor completely prevented. At present, effective protection against such threats of digitalisation is practically non-existent. The barrier to entry for any type of attack is unnecessarily low as long as the following factors continue to apply:

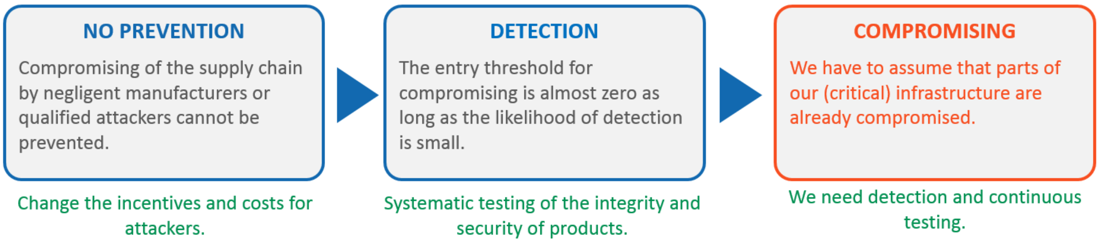
- The compromise of a product cannot be detected.
- It is difficult to demand minimum quality requirements from the manufacturer (and its suppliers).
- Maintenance of the infrastructure is not guaranteed because security updates are not reliably installed.

[8] Israel and the USA said to be behind computer attack (article in German): https://www.nzz.ch/iran_israel_usa_stuxnet-1.9110811

[9] Hundreds of thousands of Asus computers infected with virus (article in German): https://www.tagesanzeiger.ch/digital/computer/hunderttausende-von-asuscomputern-mit-virus-infiziert/story/19690172

[10] Significant Cyber Incidents Since 2006: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

This situation is no longer acceptable in view of the increasing dependence on digital products. Due to inadequate detection capabilities, it has to be assumed that parts of Switzerland's critical infrastructure have already been compromised.



NO PREVENTION

Compromising of the supply chain by negligent manufacturers or qualified attackers cannot be prevented.

Change the incentives and costs for attackers.

DETECTION

The entry threshold for compromising is almost zero as long as the likelihood of detection is small.

Systematic testing of the integrity and security of products.

COMPROMISING

We have to assume that parts of our (critical) infrastructure are already compromised.

We need detection and continuous testing.

Illustration 2: If the quality and security of digital products is neither required nor verified, we have to assume that a large number of products, even those for critical functions, have been compromised.

The following examples show the consequence of insufficient detection of products being compromised in the supply chain:

- **IBM typewriters | Soviet Union 1970**
  The Soviet Union compromises IBM typewriters before delivery to the US embassy in Moscow. For about 8 years, the Soviets were able to read the typewritten texts of the US embassy[11].

- **Payment terminal (POS) | Cybercriminals 2008**
  Compromised payment terminals (chip and pin machines) in Europe exfiltrate credit card information and passwords via an implanted GSM device and send them directly to cybercriminals abroad[12].

- **NSA toolbox | USA 2013**
  Malware and hardware implants for computers from Cisco, Dell, Juniper, Hewlett-Packard (HP) and Huawei are installed by the US intelligence agency NSA[13].

- **BlackIOT, high wattage botnet | 2018**
  A botnet with compromised IoT air conditioners and heaters can threaten a region's power supply[14].

[11] Operation GUNMAN: https://www.cryptomuseum.com/covert/bugs/selectric/

[12] Chip and pin scam "has netted millions from British shoppers": https://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html

[13] The NSA's secret toolbox (article in German): https://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html

[14] BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

Even if there is no such thing as absolute security (neither in the digital nor in the real world), appropriate measures must be taken to. . .

- . . . increase the entry barrier, complexity, and cost for the attackers.
- . . . reduce the attacks' chance of success.
- . . . enable the detection of attacks and identification of the attackers.
- . . . make the manufacturers and operators of the products responsible for quality and security.

This means that, firstly, an attacker should no longer be able to jeopardise the security of digitalised systems without facing considerable personal risk. And secondly, manufacturers must take responsibility for the security of their digital products.

The supply chain of digital products

As mentioned above, supply chain security is of particular importance here, and so this aspect is examined in detail below.

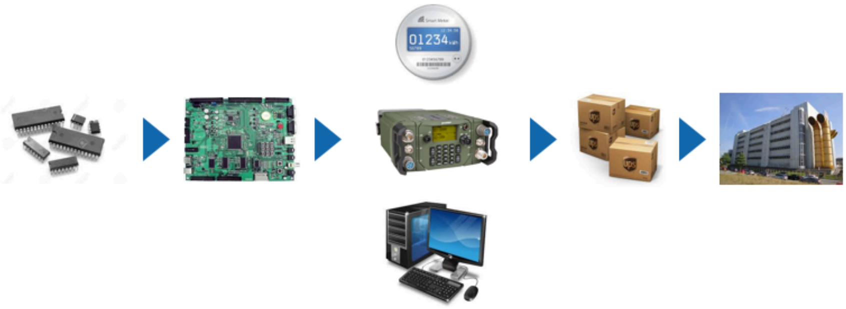


Illustration 3: The supply chain of digital products and components, from design of the hardware, to integration and shipping, and on to end-user deployment.

Origin and manufacturer

Most digital infrastructures come from a variety of suppliers of different origins. Components and sub-components are usually manufactured in a complex supply chain, which because of this complexity is hard to understand and uncontrollable. As digital products become more widespread, the growing complexity of the supply chain poses a significant threat to the digital society.

Traditional versus digital supply chain

The traditional approach to securing the supply chain works on the assumption that the threat is greatest at the manufacturing stage. For digital products, this approach needs to be extended.

- With the increasing complexity of processors and chips, the threat is shifting towards the design of chips and components. This includes the development environments including the software and tools for chip design.

- Traditional non-networked products hardly change after delivery. By contrast, malfunctions integrated within networked products can also be activated after delivery. A malfunction or backdoor can just as well be triggered by an update.

- Unlike with non-networked products, security updates by the manufacturer are a necessity. This applies throughout the whole service life of the digital product.

- Conventional products can usually be inspected visually. Often, the integrity of digital products can only be assessed with complex test procedures.

- It is hardly possible to manipulate conventional products individually, due to the lack of networkability. All the products in a series are the same. Networked products, by contrast, can be manipulated individually from a distance. The test procedures are correspondingly more complex.

- A small number of manufacturers dominate the market for certain types of digital products or sub-components (e.g. processors, WLAN chips, adapters). The result is a concentration of incentives for attackers. An attack on one of the dominant manufacturers will have far-reaching consequences.

Integrity of the supply chain

In a supply chain attack, components are already compromised or manipulated before delivery to the end user. This can already be done during the design and development of the chips, the manufacture or integration of components or during transport to the end user. Manipulation during operation, e.g. by supplying compromised firmware, also needs to be taken into account. The integrity of supplied digital items is particularly endangered by undocumented access and backdoors or implanted malfunctions.

As an initial approach, we distinguish the following types of threats:

(A) Targeted attack	(B) Opportunistic attack
A single compromised product has critical effects on the targeted organisation.	**The situation only becomes critical when there is a widespread distribution of the compromised products.**
Targeted compromising of specific products of an organisation or industry allows the attacker to gain access and influence in a precisely specified environment.	The compromising of digital consumer goods that are generally accessible to private individuals and/or to industry allows influence to be exerted on a large population of product users.
• Special network equipment (ISP, GSM, etc.) • Industrial control systems (ICS) • Industrial Internet of Things (IIoT) • Industry-specific products (military, energy, medical)	• Computer / computer peripherals • Smart metre, toaster, TV, washing machine • Home control systems • IoT, sensors • e.g. Mirai Botnet DDoS attack

The boundaries between these types of threats are fluid.

Sabotage and espionage

Intelligence agencies are increasingly implementing measures such as “kill switches” (emergency stop switches) to prepare for sabotaging foreign systems in case of need. Such functions can be found, for example, in software vulnerabilities or permanently installed access accounts for supposed maintenance purposes. It is very difficult for the attacked party to clearly trace such defects back to a targeted action by an opponent. Thus, it is almost impossible to obtain clear evidence of the sabotage.

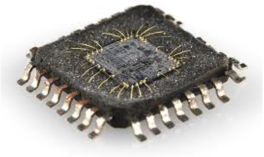
Compromised hardware

Hardware can also be fitted with hidden functions before it is delivered, which can then be remotely activated when required. Many digital products without input devices (no mouse, screen, etc.) do not look like networked computers (e.g. IoT devices such as smart toasters). But it is precisely these digital products that are often used with inadequately secured hardware and software in a largely unprotected network. Attacks on both firmware and hardware of digital products are possible and very attractive for attackers.

Every year, over 5,000 new chips are developed in countless companies around the world with hundreds of thousands of engineers. In statistical terms, therefore, there are clearly enough employees with the necessary skills and access to compromise chips at the design stage. They might do this at their own initiative or they could be blackmailed into taking such action[15].

Among other things, compromised hardware allows:

- Exfiltration of sensitive data, e.g. via covert channels
- Remote access to and control of systems
- Manipulation of functioning, e.g. generation of incorrect results
- Import of compromised software and forced use of insecure algorithms
- Physical destruction on command (kill switch)



In many cases, a software update is not sufficient, and defending against and removing insecure hardware can require a great deal of effort and expense – e.g. the replacement of all smart metres in a city or even an entire region.

In the absence of a reliable quality inspection of digital products, we have to assume that compromised components are already in use today. Further compromised components will be added continuously, sometimes in critical functions.

General Michael Hayden, former Director of the CIA and the NSA, described the issue like this: *"Frankly, it's not a problem that can be solved, this is a condition that you have to manage."*[15]

[15] Compromised By Design? https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf

Technology and history of innovation

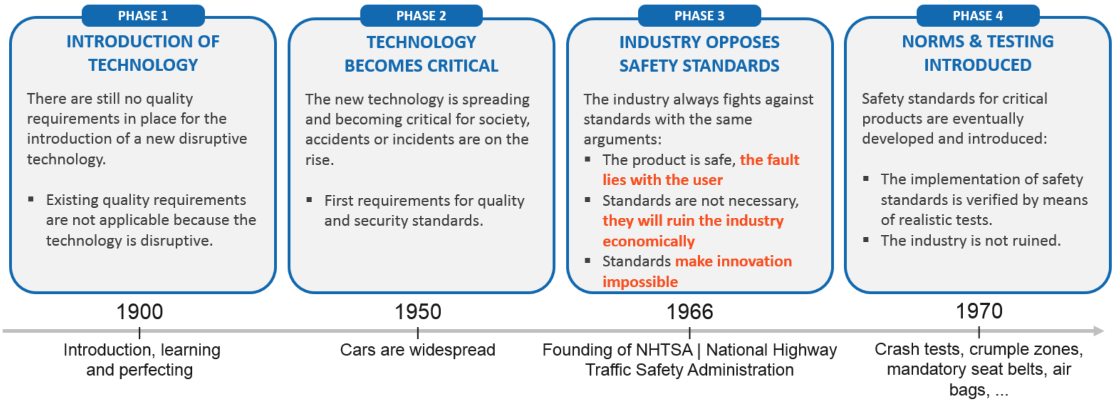
Are there lessons to be learned from history that could help us to better understand or even drive forward the development of cybersecurity in the digital society?

The launch of disruptive innovation

When introducing an innovation (e.g. in the automotive or aviation industries), safety is secondary, and there is still a lack of experience and safety standards. As use becomes more widespread, the incidents multiply in number, and society begins to question the lack of safety. Demands for binding safety standards are often fiercely opposed by the industries concerned with the following arguments:

- The product is considered safe and accidents are attributed to the user.
- Safety standards are not considered essential and would mean economic ruin for the industry.
- Safety standards would make innovation impossible.

Ralph Nader's book "Unsafe at any Speed" from 1965 illustrates this conflict. The publication of the book – following disputes with the automotive industry – led to the introduction of safety belts, crash tests and the recall of entire product series[16]. In the early days, the aircraft industry fought against aircraft engine tests. When these were finally introduced, more than half of the engines failed to pass the first tests[17].



PHASE 1
INTRODUCTION OF TECHNOLOGY

There are still no quality requirements in place for the introduction of a new disruptive technology.

- Existing quality requirements are not applicable because the technology is disruptive.

PHASE 2
TECHNOLOGY BECOMES CRITICAL

The new technology is spreading and becoming critical for society, accidents or incidents are on the rise.

- First requirements for quality and security standards.

PHASE 3
INDUSTRY OPPOSES SAFETY STANDARDS

The industry always fights against standards with the same arguments:

- The product is safe, **the fault lies with the user**
- Standards are not necessary, **they will ruin the industry economically**
- Standards **make innovation impossible**

PHASE 4
NORMS & TESTING INTRODUCED

Safety standards for critical products are eventually developed and introduced:

- The implementation of safety standards is verified by means of realistic tests.
- The industry is not ruined.

1900 – Introduction, learning and perfecting

1950 – Cars are widespread

1966 – Founding of NHTSA | National Highway Traffic Safety Administration

1970 – Crash tests, crumple zones, mandatory seat belts, air bags, ...

Illustration 4: The introduction of quality standards was initially opposed by the automotive and aviation industries. Today, a lack of such standards and tests is no longer conceivable.

[16] Unsafe at Any Speed: The Designed-In Dangers of The American Automobile: https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed

[17] A History of Aviation Safety: Featuring the U.S. Airline System: https://www.amazon.com/History-Aviation-Safety-Featuring-Airline/dp/144900797X

It would be inconceivable today to do without safety standards and tests in these industries. Both the automotive and aviation industries are still thriving and are regarded as key innovators.

In all critical industrial sectors, such as the automotive, aviation, medical technology, energy and food industries, quality controls by independent bodies are part of the product approval process. It is only the ICT sector that still has hardly any binding standards to guarantee the security or integrity of its products. There is no product liability for software, and security updates can be regarded as recalls of faulty software at the expense of the customer.

Lessons to be learned for the digital society

As stated above, in the case of critical technologies or where there is a high potential for damage (such as in the food, pharmaceuticals, transport, energy and construction industries), society has introduced appropriate standards to ensure quality and safety. These are supported and monitored by realistic tests. The lack of standards and tests for digital products is to be seen as critical in view of the increasing importance of these products.

The history of technology suggests that society will also develop and introduce binding quality standards for digital products. This includes testing through realistic test and analysis procedures. As experience has shown, the introduction of binding quality standards will not lead to the demise of the affected industry. It is imperative that society, industry and politicians jointly discuss the following topics and work on the corresponding issues:

- What are the minimum requirements for the integrity and security of digital products and services?
- What are the minimum requirements for the specific types of digital products, services, applications and industrial sectors?
- How do we check compliance with the minimum requirements, not only during approval, but also throughout the whole life cycle?

These binding quality standards correspond to the active and passive safety precautions familiar to us from the automotive industry, such as safety glass, multi-circuit brake systems, air bags, crash tests and periodic motor vehicle inspections.

Outlook and measures required

To secure the supply chain, measures must be introduced at various levels.

Responsibility of the manufacturer and the supplier

Manufacturers and suppliers must be held responsible for the security and quality of digital products and services and their production. Sector-specific contract templates (Security Appendix) must be developed to document the relevant security criteria. In this way, security concerns will be given more weight than individual agreements between customer and manufacturer.

Important minimum requirements for a Security Appendix are for example:

- The manufacturer commits to Coordinated Disclosure (ISO 29147) for the handling of reported vulnerabilities. It documents the implementation of the process, the contact persons and the processing time[18].

- The manufacturer undertakes to provide complete and exhaustive documentation of all default accounts, passwords, certificates and keys built into the product.

- The manufacturer grants the customer the right to check the hardware and software of the product for integrity and security (reverse engineering) without violating intellectual property rights (IPR).

In the event of any later discoveries (e.g. weak points or backdoors), the manufacturer can be held liable as the originator (no “plausible deniability”), and the customer has the possibility to investigate the cause of any security incidents (forensics, reverse engineering).

Confidence and transparency are increased and the manufacturer bears its share of the responsibility. Misconduct can have consequences and, in the worst case, lead to exclusion from the market.

Product requirements

Security updates from the manufacturer are required throughout the lifetime of a digital product. Many digital products have a service life of decades (e.g. Electricity metres, control systems) and replacement would be hardly possible or too expensive (e.g. after the bankruptcy of the manufacturer).

At least one of the following precautions must be taken before critical products are used:

[18] ISO/IEC 29147:2014 Vulnerability Disclosure: https://www.iso.org/standard/45170.html

- The source code is freely available (open source).
- Before procurement, the source code of the latest version is deposited with an independent authority. In the event of the manufacturer’s bankruptcy, the source code passes to the customer.

In any case, relevant network-enabled products must have a robust and secure mechanism to deploy security updates in a timely and scalable manner. This ensures the ability to protect critical products throughout their service life, even after the manufacturer has closed down.

Independent cyber-testing lab

The networked society must be able to analyse and assess the integrity and security of digital products by means of independent and credible tests.

Such tests should include at least the following features:

- Review of source code (if available), configuration and settings
- Analysis of software and hardware by reverse engineering, if necessary
- Risk assessment of results, coordination of communication with client and manufacturer (coordinated disclosure)
- Publication of results

The development of the appropriate skills takes time and requires a testing lab with the necessary high-tech equipment, trained specialists and close contacts to industry, academia and the security community. In the long term, an international exchange of ideas is necessary.

Vision of digital Switzerland

The ability to independently and effectively test digital products – including the reverse engineering of chips and firmware – will become increasingly important in the near future. The growing digitalisation of routine and critical functions will increase the need for this capability in industry as well as among government authorities, the police and the army. It is foreseeable that cyber testing will soon develop into a central, national task.

The ability to perform effective software and hardware tests must be regarded as a core competency of the digital society.

To avoid being exclusively dependent on external partners for this core competency in the future, Switzerland should quickly set up a cyber-testing lab in partnership with industry, academia and government authorities, along the lines of the Spiez[19] chemical laboratory model. The purpose of the cyber-testing lab is to execute and coordinate tests on behalf of industry, the country or international organisations.

As a neutral nation with a stable jurisdiction and a long tradition of being a centre for international services, Switzerland is predestined to be a competence centre and operator of an independent cyber-testing lab.

[19] Spiez Laboratory: https://www.labor-spiez.ch/en/lab/ubu/index.htm

Conclusion

The digital society currently runs the risk of creating security problems through the premature use and, in some cases, uncontrolled procurement and distribution of digital products – security issues that will only become manifest in the long term and can then only be corrected at huge expense and effort.

- The lack of quality and safety standards and appropriate testing procedures for digital products is to be seen as critical in view of their increasing importance.
- In the absence of a credible quality inspection of digital products, it has to be assumed that compromised components are already in use today. The security of digital products must be verified by credible and independent tests.
- To avoid being exclusively dependent on external partners for cyber-testing, Switzerland should quickly set up a cyber-testing lab in partnership with industry, academia and government authorities, along the lines of the Spiez chemical laboratory model.
- A set of binding minimum requirements for the security of digital products must be worked out in collaboration with the various partners (industry, academia, government authorities).
- For this purpose, cybersecurity must not be limited to software, network security and the human factor. It must also include the integrity and security of the hardware.

The ability to perform effective software and hardware tests must be regarded as a core competency of the digital society. The digital society is called upon to address the issue of supply chain security and to create the appropriate conditions (resources, legal framework, training, etc.) to prevent known and avoidable errors. Only in this way will the opportunities of digitalisation continue to outweigh its risks in the future.