Network Security Course | ETH Zurich - Autumn 2020

Supply Chain Security

Dr. Stefan Frei

Security Officer @ SIX Digital Exchange www.sdx.com
frei@techzoom.net | Twitter @stefan_frei

Head of the working group "Supply Chain Security" @ ICT Switzerland

Main Challenge in Cyber Security?

WE INCREASINGLY DEPEND ON DIGITAL SYSTEMS AS INDIVIDUALS, SOCIETY & INDUSTRY.

INDUSTRY & SOCIETY





EMERGENCY & DEFENSE




ENERGY, FOOD & WATER





TRANSPORT & LOGISTICS



75 BILLION CONNECTED DEVICES BY 2025

HOW DO WE ASSURE THE SECURITY AND INTEGRITY OF CRITICAL DEVICES & INFRASTRUCTURE?

WHAT COULD POSSIBLY GO WRONG?

Exposures in a complex and ever changing environment

COMPLEXITY

COMPLEX ENVIRONMENT

- Increased **complexity** and coupling
- Emerging properties & bad things happen **for no reason**
- **Unpredictability** of user and social behavior
- Continued discovery of new **vulnerabilities**

ACCIDENT

TARGETED ATTACK

ATTACKERS

NATION STATES

- Have always engaged in **espionage** and **sabotage**
- Have the resources and **a mandate** to do so

ORGANIZED CRIME

- Go where the money is
- Fast **adopters of new technologies**
- Sometimes blurry line between nation state activities

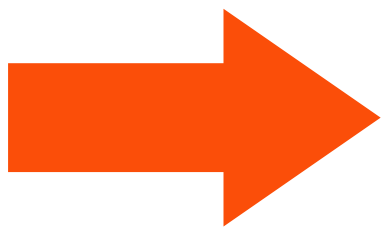
SOFTWARE & HARDWARE

Critical reliance on compiled **code** in **software** and **hardware**, which is **difficult to inspect**.

Attackers Perspective

WHAT WOULD YOU TARGET?

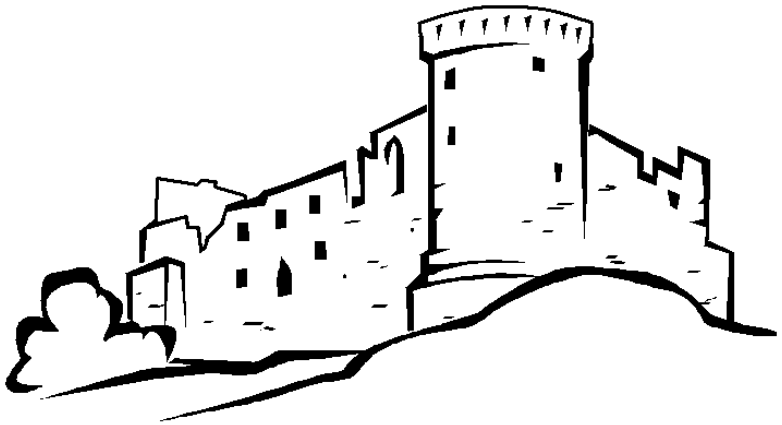
to get the BIGGEST IMPACT
with the LEAST EFFORT
to stay PERSISTENT
and AVOID DETECTION



WHAT WOULD YOU TARGET?

To get the biggest impact with the least effort, stay persistent, and avoid detection?

LESSON FROM HISTORY ..



The majority of mediaeval castles where not taken by direct attack against the enforced walls.

But through ..

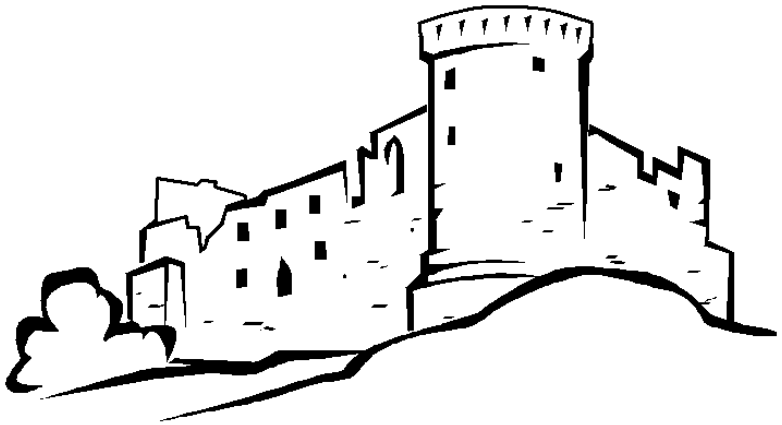
.. FOR TODAYS WORLD

?

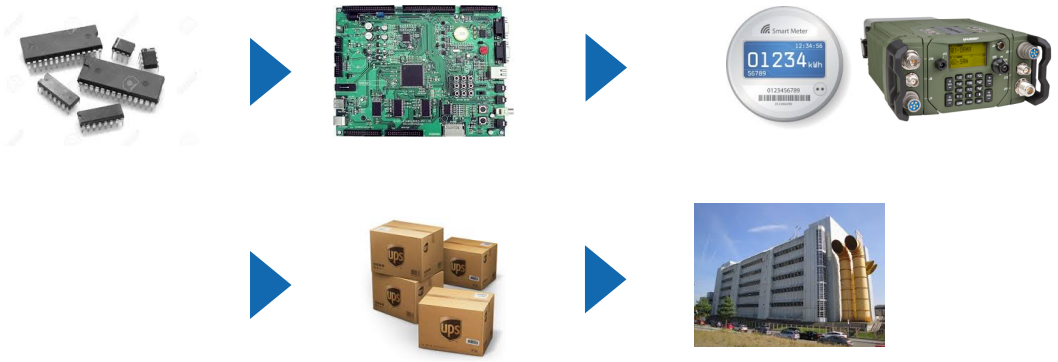
WHAT WOULD YOU TARGET?

Find the weakest link & attack where they expect it the least!

LESSON FROM HISTORY ..



.. FOR TODAYS WORLD



The majority of mediaeval castles where not taken by direct attack against the enforced walls.

But through treason or marry-in

We depend on a **complex supply chain** of numerous sub-systems and various suppliers

.. over which we have limited control at best

We have limited or no control over the supply chain

A globalized production system supplies the components

DESIGN	BUILD	INTEGRATE	DELIVERY	OPERATION
Code & logic design development	Production Foundry	Board System integration	Transport Delivery	Operations Updates

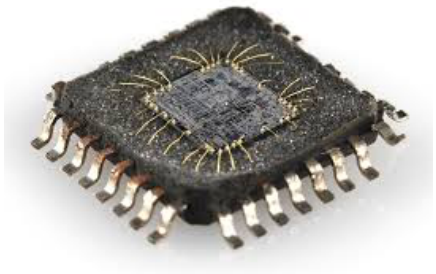
- Many tiers limit visibility
- Impossible to track the origins of all individual components
- Deployed components undergo permanent changes (software/cloud updates)

Expect more attacks on
sub-systems or suppliers
with the objective
to compromise
the primary target.

SUPPLY CHAIN ATTACK

Scenarios and exposed sectors

- Critical systems and devices are **compromised upon delivery**.
- Functionality of critical systems **changes over time**.
- Operation of critical systems **depend on external services** (cloud, vendor).
- Lack of **update-functionality** results in **loss of control**.



TARGETED ATTACK

INDUSTRY SPECIFIC

Targeting non consumer grade products for specific industries.

A single component has critical implications for a targeted sector.

- Special network equipment (ISP router, GSM)
- Industry Control Systems (ICS)
- Industrial Internet of Things (IIOT)
- Industry specific systems (military, energy, transport, medical, ..)

OPPORTUNISTIC ATTACK

OFF THE SHELF COMMODITY

Targeting off the shelve commodity products for consumers and industry.

Only **a large number of compromised components** become critical.

- Computer, logic boards, processors
- Smart meter, toaster, TV, ..
- Home control systems
- IOT, sensors

History & Examples

LONG HISTORY OF SUPPLY CHAIN ATTACKS

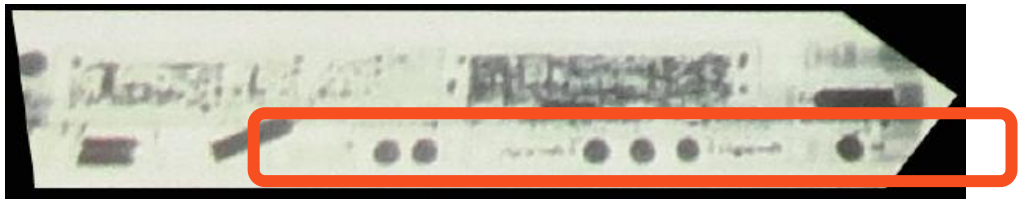
Actor: Nation State | USSR

1970-1978 Soviets replaced the comp support bar in IBM typewrites deployed in U.S. embassy in Moscow.

TRANSMIT IN PLAIN TEXT WHATEVER WAS WRITTEN IN THE EMBASSY

- The Selectric Bug was a sophisticated digital eavesdropping device, developed in the mid-1970's by the Soviet Union (USSR).
- It was built inside IBM typewriters and was virtually invisible and undetectable.
- 16 devices found that were in use at least 8 years.

- *Operation GUNMAN - how the Soviets bugged IBM typewriters*
  https://www.cryptomuseum.com/covert/bugs/selectric



Six black dots in x-ray
Magnetometers that picked up the movements of the six modified latch interposers of the keyboard

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Nation State / Unknown

2007

Hard drives with “report-back mechanisms” embedded in them by a foreign intelligence service sold to U.S. DOD

BACKDOORED HARD DRIVES PRODUCED IN THAILAND BY AN AMERICAN FIRM

- These hard drives were sent to DOD and copied all of the classified files stored on them
- Transmitted the files via the Internet back to the foreign intelligence service
- The hard drive maker is blaming an unnamed subcontractor, located in China, for the problem
- It's easy for this kind of thing to happen, if one PC in the testing, manufacturing and quality assurance chain is infected

Seagate Ships Virus-Laden Hard Drives

- *https://www.pcworld.com/article/139576/article.html*
- *https://www.sciencedirect.com/science/article/pii/S0166497214000194?via%3Dihub*

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Organized Crime | Global

2008 — Hundreds of card terminals in supermarkets exfiltrate information using mobile network.

THE DEVICES WERE OPENED, TAMPERED WITH AND PERFECTLY RESEALED

- An organized crime syndicate is suspected of having tampered with the chip and pin machines
- Tampering either during the manufacturing process at a factory in China, or shortly after they came off the production line.

- *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

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Nation State | USA

2012

Hardware and software components can be compromised with or without the consent or knowledge of the supplier

NSA techs perform an unauthorized field upgrade to Cisco hardware in these 2010 photos from an NSA document.

NSA'S BACKDOOR CATALOG EXPOSED

- Speculation that electronics can be accessed by NSA back door
- In 2012 Snowden reveals that such methods exist for numerous end-user devices. Targets include:
  - *Cisco 500 and ASA series PIX firewalls*
  - *Juniper Networks firewalls, routers, and netscreen appliances*
  - *Huawei Eudemon series firewalls and routers*
  - *Dell PowerEdge 1850, 2850, 1950, 2950 RAID servers*

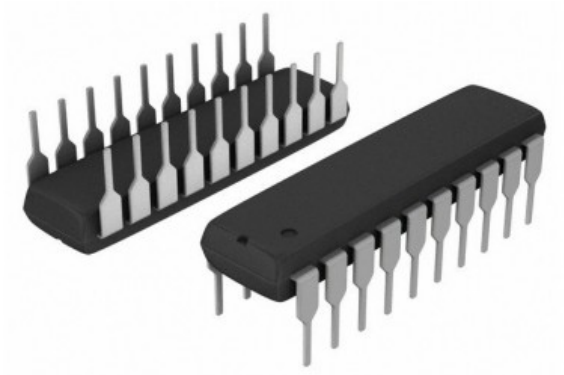
- *NSA ANT Product Catalog*
  https://nsa.gov1.info/dni/nsa-ant-catalog/index.html
- *NSA's backdoor catalog: Targets incl. Juniper, Cisco, Samsung, Huawei*
- *https://gigaom.com/2013/12/29/nsas-backdoor-catalog-exposed-targets-include-juniper-cisco-samsung-and-huawei/*
- *http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html*

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Military-components distributor | USA / China

2013

U.S. Naval Submarine Base used three counterfeit products sold by a U.S. military-components distributor



"I HAVE TO BUY FROM CHINA AND RISK FAKE PARTS TO COMPETE… IT'S MY WHOLE BIZ" THE INDICTMENT QUOTES

- Counterfeit products sold by a Massachusetts man who was indicted on conspiracy, fraud, and trafficking charges
- At least two of the circuits were intended for active-duty nuclear submarines.
- The counterfeit parts bore the trademarks of legitimate companies such as Xilinx Inc., National Semiconductor Inc. and Motorola Inc.

Feds: Counterfeit submarine parts shipped to Groton base

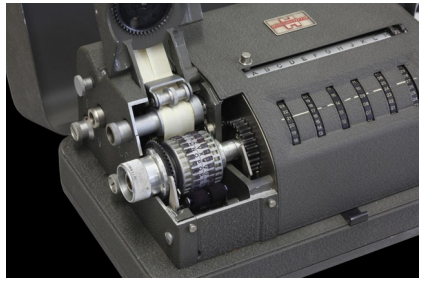
- *https://www.theday.com/article/20130716/NWS09/130719772/1017*

LONG HISTORY OF SUPPLY CHAIN ATTACKS

Actor: Nation State Agencies | USA, Germany (Switzerland)

1970-2018

Swiss Crypto AG at the heart of a huge international spying operation supplying flawed crypto products.



TECHNOLOGY MODIFIED BY DESIGN TO LET THE CIA AND BND BREAK CODES

- *Crypto, a communications encryption, firm sold code-making equipment to more than 120 countries, incl. Iran, India, Pakistan, Latin American, the Vatican and others.*

- *Latest spy scandal 'shatters Swiss neutrality', say papers*
  https://www.swissinfo.ch/eng/politics/press-review_latest-spy-scandal--shatters-swiss-neutrality---say-papers/45553888
- *Swiss cryptography firm helped NSA during Cold War*
  https://www.swissinfo.ch/eng/codebreaker_swiss-cryptography-firm-helped-nsa-during-cold-war/41576576
- *The intelligence coup of the century*
  https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Blind Spot

WEAKEST LINK & BLIND SPOT

Hardware is the least protected layer

PRODUCT
Computer / Device


SOFTWARE
Many layers, lots of security features

Applications
Operating System
Hypervisor

KNOWN TERRAIN
(Software)

HARDWARE
Boards, CPUs, chips, components, designs, ..

Firmware
Hardware

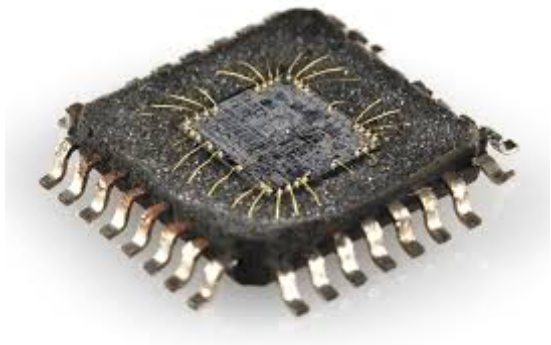

UNKNOWN TERRAIN
(Hardware)

IMPACT OF COMPROMISED HARDWARE OR FIRMWARE

Cybersecurity remains largely SOFTWARE FOCUSED

- in terms of the techniques employed
- the expertise of the people and companies working in the field

Impact of compromised hardware or firmware



- Remotely access & control the system
- Exfiltrate or leak sensitive information
- Disable/cripple functionality, make incorrect results
- Enforce the use of insecure algorithms
- Physically kill the system

HARDWARE ATTACKS

Harder to conduct than software attacks, since far fewer people have the necessary skills and access.

HARDWARE DEFENSE

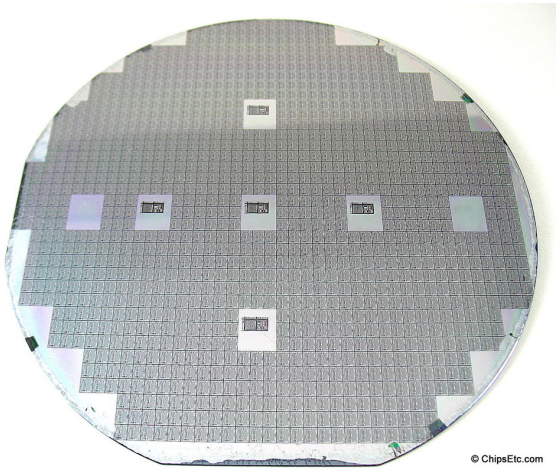
Harder to defend against, since replacing corrupted hardware can be extremely difficult and expensive.

COMPROMISED HARDWARE OR FIRMWARE NULLIFIES ALL OTHER SECURITY MEASURES

CHIP DESIGN CORRUPTION

Over 5,000 new chips designed each year –

involving thousands of companies and hundreds of thousands of chip designers



A skilled attacker could:

- **Compromise a design & minimizing the chance of detection** (chips are so complex that testing is only partial)
- **Introduce a flaw with plausible deniability** (characterizing the back door as a feature to assist in testing prototypes of the chips)

STATISTICALLY, THERE ARE ENOUGH PEOPLE WITH THE SKILLS, ACCESS, AND MOTIVATION TO INTENTIONALLY COMPROMISE A CHIP DESIGN.

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

SUPPLY CHAIN ATTACKS CHIPS

Why Design Corruption Is a Growing Threat

Fabrication facility
("Fab", "Foundry")

- Large number of organizations and people involved in the design of a single large chip.
- Many companies subcontracted to provide designs, and further levels of sub-contracting.
- Pieces of the chip design are stored and exchanged using a myriad of (insecure) computers and networks.

Risk of an insider threat among the dozens or hundreds of engineers with access to the design:

- If only 1 of 1000 chip designers would consider corrupting a chip for profit > corresponds to hundreds of people with exactly the right skills and access.

- IT WOULD DEFY LOGIC TO ASSUME THAT NONE OF THEM WILL EVER TRY.

"Frankly, it's not a problem that can be solved, this is a condition that you have to manage."

General Michael Hayden

retired head of CIA and NSA

CONCLUSIONS SO FAR

The integrity of digital products has to be challenged and questioned to a greater extent.

NO / MINIMAL PREVENTION

We can not prevent adversaries or careless manufacturers from compromising the supply chain

NO / MINIMAL DETECTION

The bar for such compromises is low - as long as the chance of detection is low

ASSUME COMPROMISE

We must assume that parts of our (critical) infrastructure are already compromised

CHANGE INCENTIVE OR COST FOR POTENTIAL COMPROMISE

SYSTEMATIC TESTING OF THE INTEGRITY AND SECURITY

DETECTION, ONGOING TESTING

We have to systematically verify the integrity & security of critical components.

SOCIETIES ALWAYS DEVELOPED NORMS TO ENSURE THE QUALITY OF CRITICAL GOODS - ENFORCED BY HARSH TESTING

AUTOMOTIVE

- Extensive testing of vehicles before admission
- Periodic inspections
- Minimum quality and safety standards

AVIATION

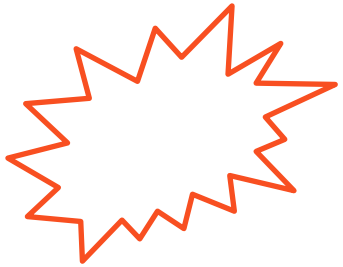
- Extensive testing of aircraft before admission
- Extensive operations requirements
- Periodic inspections & traceability of components

FOOD MEDICINE

- Extensive testing of new drugs before admission
- Extensive requirements for processing and delivery
- Periodic and surprise inspections & traceability of components

CYBER

- No binding norms or minimum requirements
- Security or the integrity of goods at odds, no systematic testing
- No product liability



PHASES OF INTRODUCING QUALITY REQUIREMENTS

Typically fiercely resisted by the industry with the same arguments

PHASE 1

TECHNOLOGY INTRODUCED

New disruptive technology is introduced, there are yet no quality requirements

- Existing norms do not apply as the innovation is disruptive

PHASE 2

TECHNOLOGY BECOMES CRITICAL

The new technology becomes critical for society, increasing number of accidents / incidents

- Calls for quality standards or norms

PHASE 3

INDUSTRY FIGHTS MIN. REQUIREMENTS

Industry fights introduction with always the same arguments:

- Product is safe - **accidents are the users fault**
- Norms are not necessary - they will **ruin the industry**
- Norms will **stifle innovation**

PHASE 4

NORMS & TESTING INTRODUCED

Eventually, society develops and introduces minimum requirements for critical goods

- Minimum safety and security requirements are enforced through harsh testing
- Industry still exists

invented & perfected

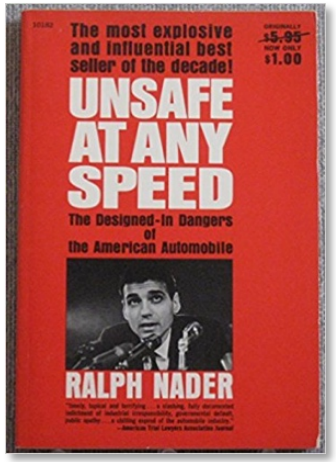
cars become prevalent

creation of predecessor of National Highway Traffic Safety Administration

cars tests, seat belts mandatory, airbags , ..

PHASES OF INTRODUCING QUALITY REQUIREMENTS

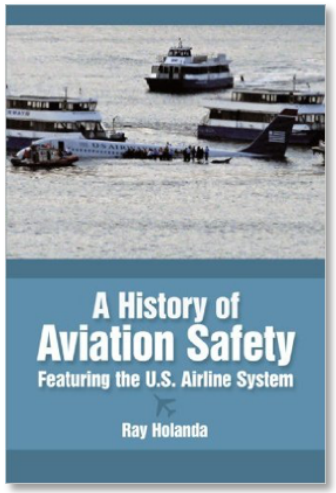
Typically fiercely resisted by the industry with the same arguments



UNSAFE AT ANY SPEED

Book by Ralph Nader accusing car manufacturers of resistance to the introduction of safety features such as seat belts, and their general reluctance to spend money on improving safety.

Ralph's book let to introduction of crash-test dummies and seat belts after disputes. (1965..)



HISTORY OF AVIATION SAFETY

First 50 hour endurance tests for aircraft engines against the protests of the industry: Over half of the engines could not pass the initial test (1920-30).

Early philosophy in aviation: fly it, break it, fix it, blame the pilot

Conclusion & Actions

"Plan for the difficult whilst it is easy. Act on the large while it's minute. The most difficult things in the world begin with things that are easy."

Laozi (Lao Tzu), 600 BC

CONCLUSION | TRUST BUT VERIFY

LESSONS HISTORY

Society has **always developed and introduced:**

- Binding quality norms for **critical goods**.
- Testing **capability to verify required quality**.

FINDINGS CONCLUSION

Effective testing of cyber products (software & hardware)
has to be regarded as a **core competency of the digital society.**

- **An independent and trusted organization** should do that for members.
- Effective cyber testing is a **complex business requiring collaboration** between industry, academia, security community, government)

VISION OPPORTUNITY

Build Joint Cyber Testing Organization (private / public org) today

- Coordinate tests on **behalf of its members** (industry, nation, ..)
- Tests executed by **trusted testing labs** (own labs & industry partner labs)
- **Document and communicate results** (coordinated disclosure)

Switzerland is well positioned to build or host an internationally trusted organization for testing cyber products

- independent, trusted, competent
- long history of hosting similar organizations (Labor Spiez, Red Cross, ..)

SUPPLY CHAIN RISKS

Current state, recommended actions, and vision

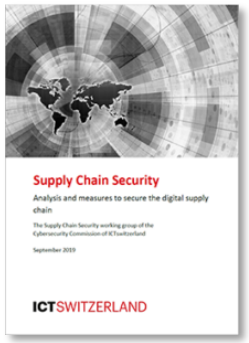
Cyber risks are abstract, have developed slowly and, consequently, were ignored for a long time. Digital products increasingly pervade every area of life, and it is difficult to allocate resources to protect against abstract risks. Such risks are often recognized only once a major event has occurred.

This presentation is about the important but largely overlooked fact that we must assume that critical components of our infrastructure are already compromised, from applications and operating systems down the everyday devices, their firmware, hardware and individual chips. We have come to rely on a complex chain of suppliers for hardware and software, a supply chain which can no longer be fully controlled. On top, the revelations by Snowden have demonstrated that hardware and software can be compromised and backdoored with or without the consent or knowledge of the supplier.

This presentation examines the supply chain risks and remediating measures from the attackers, defenders, technology, and economic perspective. This latest disruptive innovation is not the first to prompt critical questions regarding security and safety, there are effective lessons from history to inform us for the future.

As a society and industry, we are obligated to prevent known and avoidable mistakes.

References / Sources



WHITE PAPER SUPPLY CHAIN SECURITY

Analysis and measures to secure the digital supply chain

https://ictswitzerland.ch/white-paper-supply-chain-security | Sep 2019

https://ictswitzerland.ch/en/topics/cyber-security/supply-chain/

Resources

- https://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html
- https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf
- http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf
- https://www.cryptomuseum.com/covert/bugs/selectric/
- https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf
- https://gigaom.com/2013/12/29/nsas-backdoor-catalog-exposed-targets-include-juniper-cisco-samsung-and-huawei
- Zeljka Zorz, Researchers create undetectable layout-level hardware Trojans - http://www.net-security.org/secworld.php?id=15589.
- Ryan Singel, Industrial Control Systems Killed Once and Will Again - http://www.wired.com/threatlevel/2008/04/industrial-cont