

Supply Chain Security & Integrity

Dr. Stefan Frei
Security Architect

stefan.frei1@swisscom.com

Twitter [@stefan_frei](https://twitter.com/stefan_frei)

Web www.techzoom.net



September 2015

swisscom

Problem Statement

Internet Service Providers (ISP) deploy and operate an array of diverse and fast changing technologies and services to provide cutting edge solutions to their private and business clients. Thereby they rely on a complex chain of suppliers for hardware and software.

Many such components fulfill critical functions at the core of the ISPs business, and often the choice of the third party supplier is limited, for example for high performance networking gear or mobile equipment.

With the reliance on third party components the security and integrity of the supply chain is a concern to the ISP and customers alike.

Recent revelations brought the integrity of such equipment to the attention of the public, as it has been demonstrated that hardware and software components can be compromised and backdoored with or without the consent or knowledge of the supplier.

Such events erode the trust in key deliverables of our business.

Initiative – Call for Participation

Swisscom is examining a program to identify and continuously test critical infrastructure components jointly with other ISPs. With the shared resources of multiple ISPs, the goal is to have critical components frequently reverse engineered (software and hardware) and thoroughly examined for backdoors or hidden functionality.

The results of these tests are shared between the participating organizations, coordinated with the vendor, and ultimately made public.

A joint program credibly demonstrating that critical components are frequently and systematically tested for backdoors sends a strong signal to any adversary.

Adversaries can no more operate under the assumption of undetectability, and the cost (politically, reputation, financially, legally) for any party to participate in a compromise is increased drastically.

Critical Infrastructure

Today, society and businesses alike depend critically on a working Internet infrastructure.

- This infrastructure has become the *primary target* for old and new actors
- We have to *operate* and *protect* this infrastructure

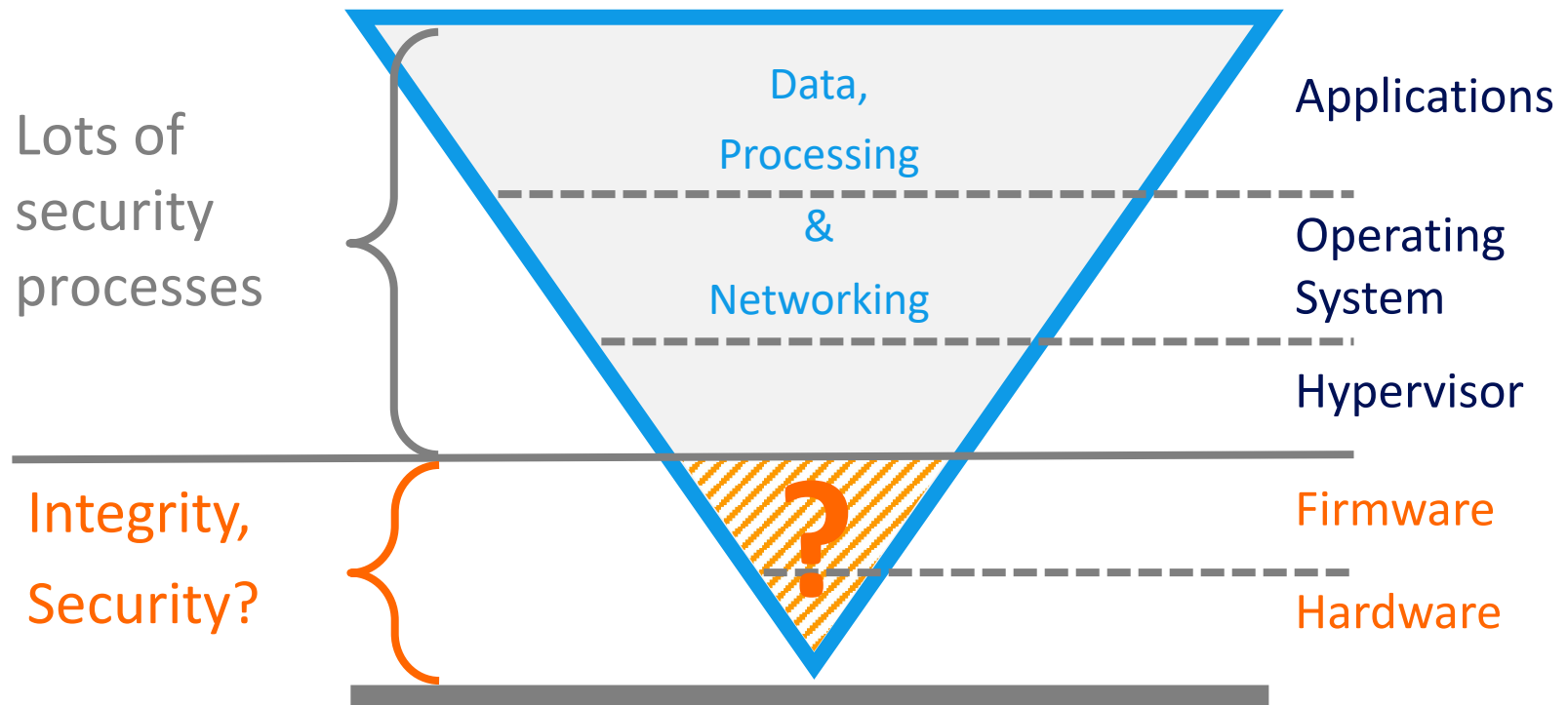
What do you target as an attacker?

- to get the *biggest impact* with the *least effort*?
- to stay *persistent* while *not getting detected*?
- Suttons law: go for the obvious first

The famous criminal Willie Sutton was once asked why he robbed banks.

– Reply: "Because that's where the money is."

Computing Stack



Hardware and Firmware

The hardware and firmware of a device are at the core of all processing and networking

- Compromised hardware or firmware nullifies all other security measures
- Hard to detect and protect against



Attackers Choice





Compromised hardware or firmware allows to:

- remotely access & control the system
- exfiltrate or leak sensitive information
- disable/cripple the functionality, create incorrect results
- enforce the use of insecure algorithms
- physically kill the system



Increasing Exposure

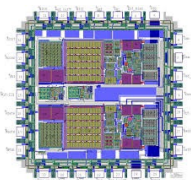
Steadily increasing dependence on all types of devices

Networking	Computing	ICS/SCADA	IOT
<ul style="list-style-type: none">• Backbone• Intranet• GSM, WiFi• Router, Switches, ..	<ul style="list-style-type: none">• Server• Desktop• Mobile Devices	<ul style="list-style-type: none">• Industry• SmartGrid• Traffic, ..	<ul style="list-style-type: none">• SmartHome• Sensor Networks
			

Supply Chain Complexity

We only have limited control over the supply chain

- a globalized production system supplies the components
- many tiers limit visibility
(designers, producers, brokers, subsystem suppliers, major system integrators, etc.)
- it is difficult to track the origins of components



Points of Compromise



Manufacturer	Third Party	Operator
<ul style="list-style-type: none"> • at will or forced by law • compromised sub-suppliers 	<ul style="list-style-type: none"> • intercept in-transit 	<ul style="list-style-type: none"> • software update • insecure operations
<ul style="list-style-type: none"> • "unknown" vulnerabilities • bad features/accounts • kill switch 	<ul style="list-style-type: none"> • hardware implants • modified chips or firmware 	<ul style="list-style-type: none"> • firmware update • compromised mngt system • insecure link



Points of Compromise

- Manufacturers may be forced (by the law) to secretly build/accept backdoors in their products
- Manufacturers rely on components which may be compromised, or be forced to use subcomponents with specific weaknesses
- Equipment for specific destinations may be intercepted and modified upon shipment without the consent or knowledge of neither the vendor nor the customer
- Equipment may be backdoored in general, or selectively for specific customers only
- (Re)deployment of compromised firmware (e.g. through updates or compromised management console)

Who would do that?

Criminals ..

- go where the money is

Nation States ..

- have always engaged in espionage and sabotage
- mandated by law to do so
- may have privileged access to infrastructure (Internet backbone, suppliers, transport, ..)
- Ongoing espionage and preparations for sabotage



In the old days ...

In the 1970s to 80's the Soviets managed to replace the comp support bar in IBM typewrites to transmit in plain text whatever was written

Project GUNMAN: <http://rijmenants.blogspot.ch/2012/11/the-gunman-project.html>



Source:

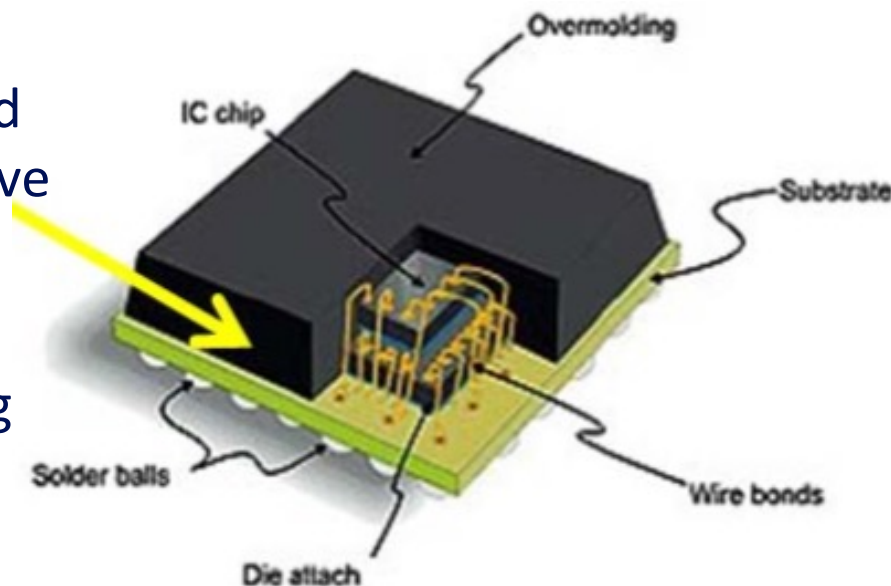
<http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

https://www.nsa.gov/public_info/_files/cryptologic_histories/learning_from_the_enemy.pdf

Modern days

Subvert a chip

- Removal of an integrated circuit from its packaging and replacement with a subversive die into the same package
- no affect on system performance through testing qualification or operation



- This chip could be inserted into a system through or a larger batch of systems during “normal” manufacturing in some foreign nation

Published 2013

16

NSA's backdoor catalog exposed: Targets include Cisco, Juniper, Samsung, Huawei



Cisco 5xx & ASA



Juniper 300/500



Huawei Eudemon



Dell PowerEdge

Source: <https://gigaom.com/2013/12/29/nsas-backdoor-catalog-exposed-targets-include-juniper-cisco-samsung-and-huawei/>

Published 2014

NSA employees intercept servers, routers, and other network gear being shipped to organizations targeted for surveillance

Install covert implant firmware onto them before they're delivered

Other countries do this as well



Absence of evidence is not evidence of absence

Source

<http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/>

Organized Crime

2008

- Hundreds of card terminals in supermarkets exfiltrate information using mobile network
- The devices were opened, tampered with and perfectly resealed



2015

- Cisco router SYNful Knock
- The implant uses techniques that make it very difficult to detect
- A clandestine modification of the router's firmware can be utilized to maintain perpetual presence



Sources

<http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html>

https://www.schneier.com/blog/archives/2015/09/synful_knock_at.html

What can we do?

We cannot prevent that an advanced adversary compromises our supply chain

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

Doing nothing is not an option – we are talking about a critical infrastructure

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

What can we do?

20

You can't manage what you can't measure

1. Trusted Computing
2. Harsh Testing (Reverse Engineering)



Verify the integrity of all components and firmware of a system upon boot

- Swisscom verifies the integrity of all cloud servers with Trusted Platform Modules (TPM)
- Secure boot and remote attestation of server integrity
- Next: TPM in networking gear (with Arista)



Lessons learned with TPM deployment

- Vendors are not used to customers ordering TPMs
(TPM server integration did not work out of the box, lengthy debugging with vendor to fix BIOS)
- Initially internal resistance to TPM ..
- Followed by increased service availability and acceptance
(early detection of changed HW and driver incompatibilities)

Harsh testing: Reverse Engineering

Systematic detection of backdoors through reverse engineering of firmware / hardware

- Systematic testing of critical components identifies backdoors/confirms integrity of device
- Findings used for risk assessment & mitigation
- Demand the manufacturer to fix it
- Publish after a grace period ("coordinated disclosure")



Why reverse engineering? - Changed incentives

Demonstrating that critical components are systematically tested sends a strong signal to any adversary

- Adversaries can no more operate under the assumption of undetectability
- The cost for any party to participate in a compromise is increased drastically
(politically, reputation, financially, legally)



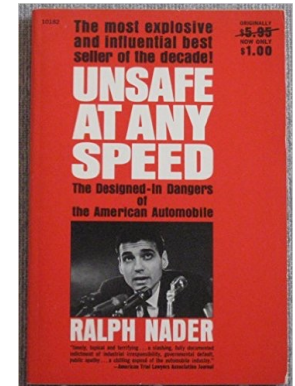
Systematic reverse engineering

- Complexity of handling reverse engineering contractors
- Legal restrictions to reverse engineering
- Handling and publication of critical findings
- Qualification of findings (backdoor vs. feature)
- Coordination with vendor "coordinated disclosure"
- Resources for frequent and systematic testing

History of testing – Car Industry

Unsafe at any speed – 1965

- resistance on road-safety improvements for fear of alienating buyer or car cost
- blame for accidents and fatalities was placed on the driver
- U.S. allocated \$320 million for highway beautification \$500,000 for highway safety



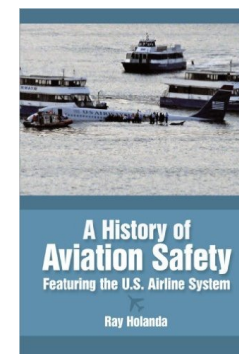
Nowadays, crash test dummies and systematic testing are the norm



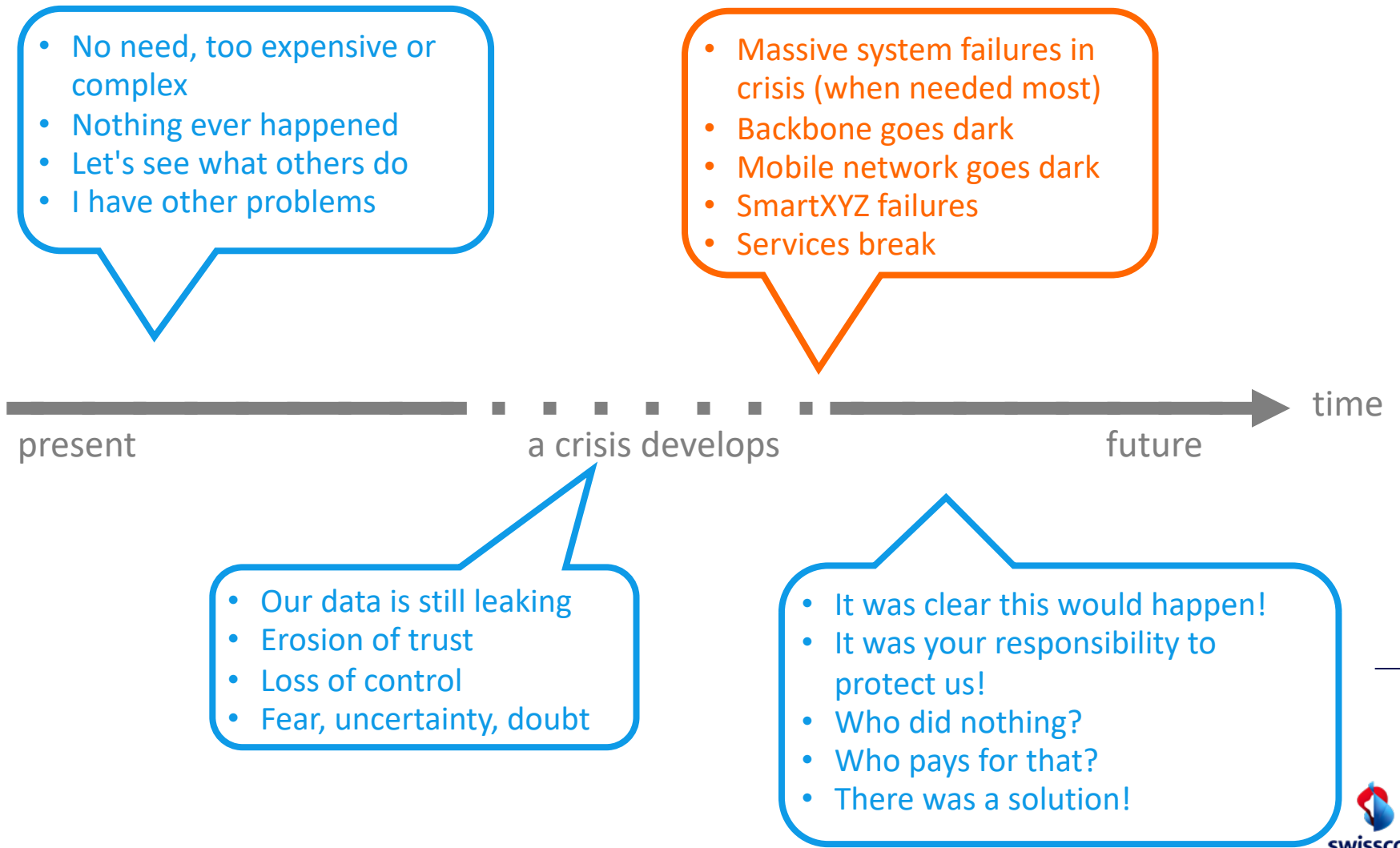
History of testing - Aviation

Aviation 1920-30	Cyber - 2015
It was not fully appreciated that thunderstorm forces could exceed the structural strength of airplanes	It is not appreciated nor accepted that critical ICT systems are already compromised
The first time engines had to pass a 50 hours endurance test caused the rejection of 50% of the engines	Unless tested rigorously, serious defects in cyber systems go undetected and persist

"A common theme throughout the history [..], a technical solution was already available to solve a safety problem before that solution was implemented into the system."



Typical sequence of events



Why Telco's?

We are critical infrastructure providers

- Infrastructure is not attacked for a quick hack

What an infrastructure attacker wants is a solid foothold

- Access to the infrastructure at any time in the future
- Be able to shut down the network at any given time
- Stay undetected

What to test?

Telco's rely on critical devices from few dominant vendors

- We are critical infrastructure providers and face the same challenges
- We pretty much operate the same devices
- The security and integrity and of such devices is neither guaranteed nor systematically verified
- Without testing, we are easily taken hostage by criminals or agencies

Next Step

TALK TO ME

- We want feedback from Telco's & the industry regarding a joint systematic testing program
- Stefan Frei
stefan.frei1@swisscom.com
mobile: +41 79 222 99 22
twitter: [@stefan_frei](https://twitter.com/stefan_frei)
web: www.techzoom.net



Appendix

- Cyber security - the current threat status and its development
- 2015 <http://techzoom.net/Publications/Papers/cyberthreats2015en>
- U.S. Defense Science Board
Cyber Task Force Report – 2013
<http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Worries of the Generals

U.S. Defence Science Board Cyber Task Force Report – 2013

- State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.