


CRYPTO SCHWEIZ AG

CYBER SECURITY SWISS MADE
ENTWICKLUNG UND SUPPLY CHAIN

Today for tomorrow's challenges

- **Post Quantum Cryptographies**
- **Machine Learning** – AI, behaviour based attack detection
- **Blockchain** – hardware based trust concepts
-  **Hardware Trojan** – PCB, chip, firmware.
- **Controller-less SDN** – new attack vectors
- **Big Data** to (social-) engineer attack targets
- **Identity** – biometric ID
- **Secure Update and upgrade**
- ...

Hardware Trojaner Angriffe in der Supply Chain

Es gibt zwei Wege, um Computer Hardware zu verändern.

- 1) Manipulation auf dem Weg vom Hersteller zum Kunden (Interdiction)
- 2) Manipulationen bereits ganz am Anfang der Supply Chain

Entwicklung und Produktionskette:

Kontrolle während Design, Entwicklung, Produktion, Lieferung und Unterhalt wird extrem wichtig.

Schadenspotential

Hardware attack – The Big Hack:

This attack was something graver than the software-based incidents the world has grown accustomed to seeing.

Hardware hacks are more difficult to pull off and potentially more devastating, promising the kind of long-term, stealth access that spy agencies are willing to invest millions of dollars and many years to get.

“Having a well-done, nation-state-level hardware implant surface would be like witnessing a unicorn jumping over a rainbow”

Quelle: Bloomberg Businessweek

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

By Jordan Robertson and Michael Riley - 4. Oktober 2018, 11:00 MESZ

The Big Hack

Real or Fake news?



[Bloomberg Businessweek](#)

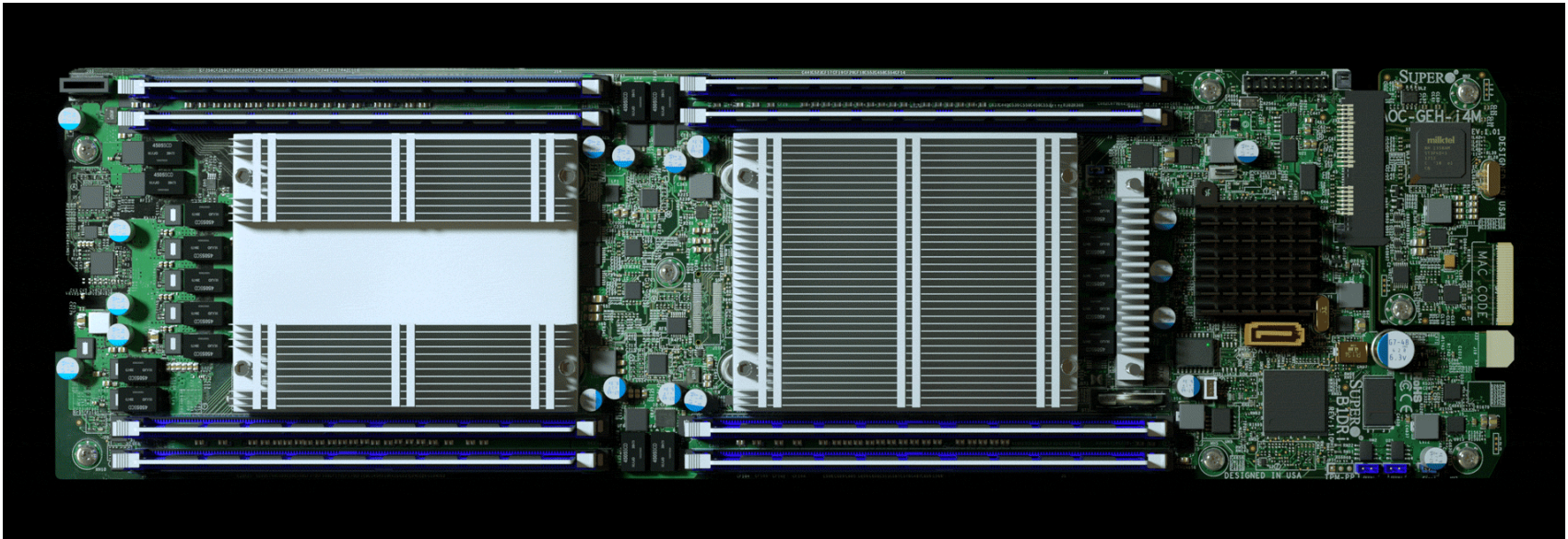
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Featured in
Bloomberg Businessweek
Oct. 8, 2018.
Photographer: Victor Prado
for Bloomberg Businessweek

By Jordan Robertson and Michael Riley
4. Oktober 2018, 11:00 MESZ

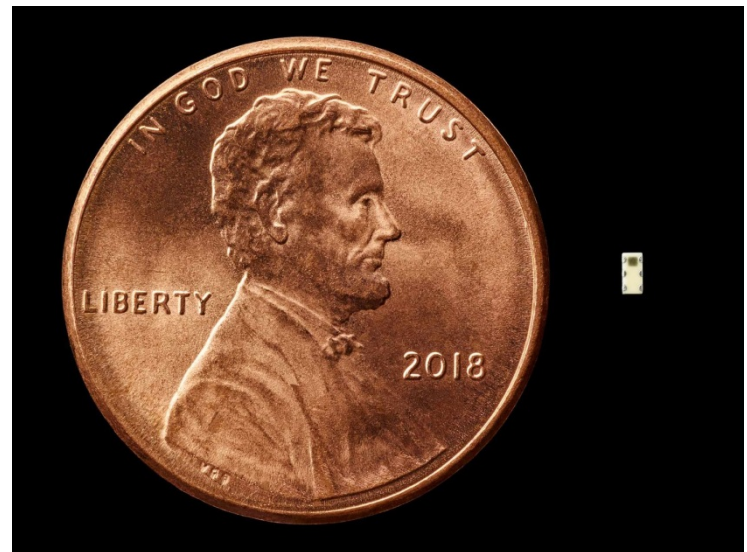
Illustration



Illustrator: Scott Gelber for Bloomberg Businessweek

Ein Kommentar zur Story:

Bloomberg used fake photos presented zero evidence and published a story that Apple, Amazon and Super Micro DENIED BEFORE AND AFTER publishing.



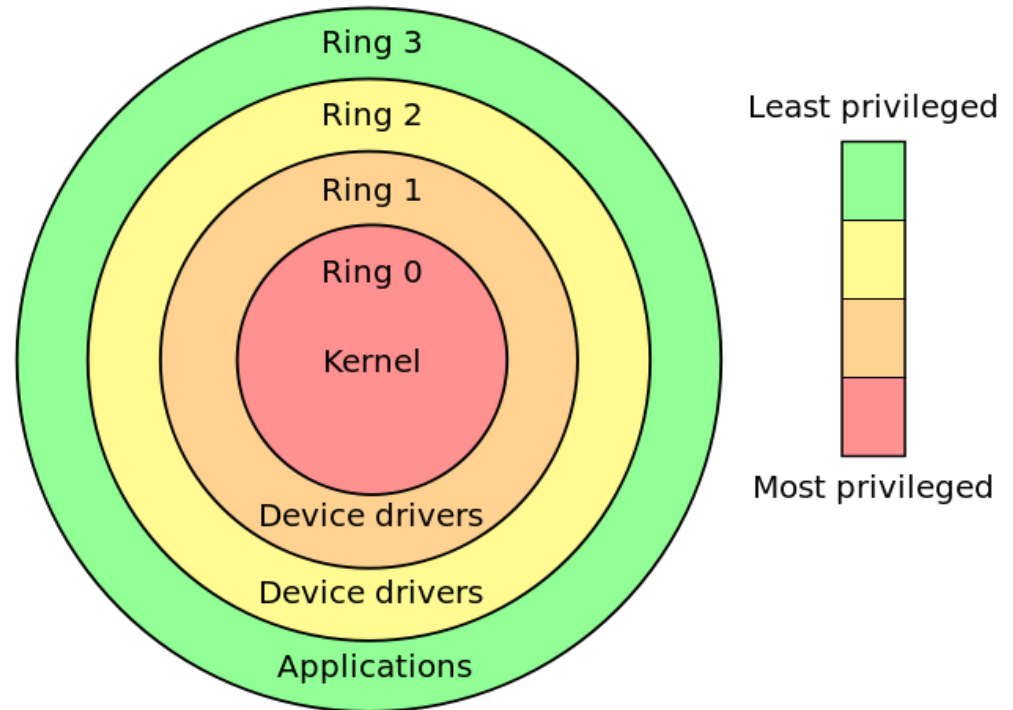
Intel ME (no fake news) Privilege rings for the x86

ME is categorized as ring -3

below System Mgmt Mode
(ring -2) and

the hypervisor (ring -1)

all running at a higher
privilege level than the
kernel (ring 0)



Massnahmen

- 100% Transparenz für Kunden über alle Designs
- 100% in Schweizer Besitz
- Sicherheitsüberprüfte Supply Chain
- Sicherheitsüberprüfte Mitarbeiter
- Dauernde Weiterentwicklung der Schutzmechanismen
- Multiple Lines of Defense



Entwicklung – Schweizer Sicherheitsanforderungen



- Entwicklungsabteilung in der Schweiz (Steinhausen)
- Eigene Hardware und Softwareentwicklung
- Sicherheitszertifizierte Entwicklungsprozesse

Produktion in der Schweiz



- Produktion aller sicherheitsrelevanten Komponenten in der Schweiz
- Sicherheitsauditierte Wertschöpfungskette in der Schweiz
- Spezielle Prozesse für Sicherheitsparameter
- Spezielle Prozesse für Sicherheits- und Chiffriermodule

Unser Beitrag zu Cyber Security

Advanced and proven concepts

Customer specific,
manageable cryptography

Security Architecture

Secure Software Design

Red-Black separation

Secure software logistics

Trust injection concepts

Tamper proof/resistance

Highly skilled staff

Security Hardware
Developer

Microchip Design Expert

Cryptographer

Secure Software
Developer

Cyber Security Experts

Embedded Systems

PC-Applications

resilient technology

Smart Protect (Secure
Hypervisor/ Microkernel)

Secure OS

Quantum resistant
cryptography

Management and
monitoring systems

Scalable secure
hardware

Danke für Ihre Aufmerksamkeit

Giuliano Otth

CEO

Direkt +41 41 749 74 85

giuliano.otth@crypto.ch

Crypto Schweiz AG

Zugerstrasse 42

6312 Steinhausen

Schweiz

T +41 41 749 77 22

F +41 41 741 22 72

crypto@crypto.ch

www.crypto.ch