
SBA
Research

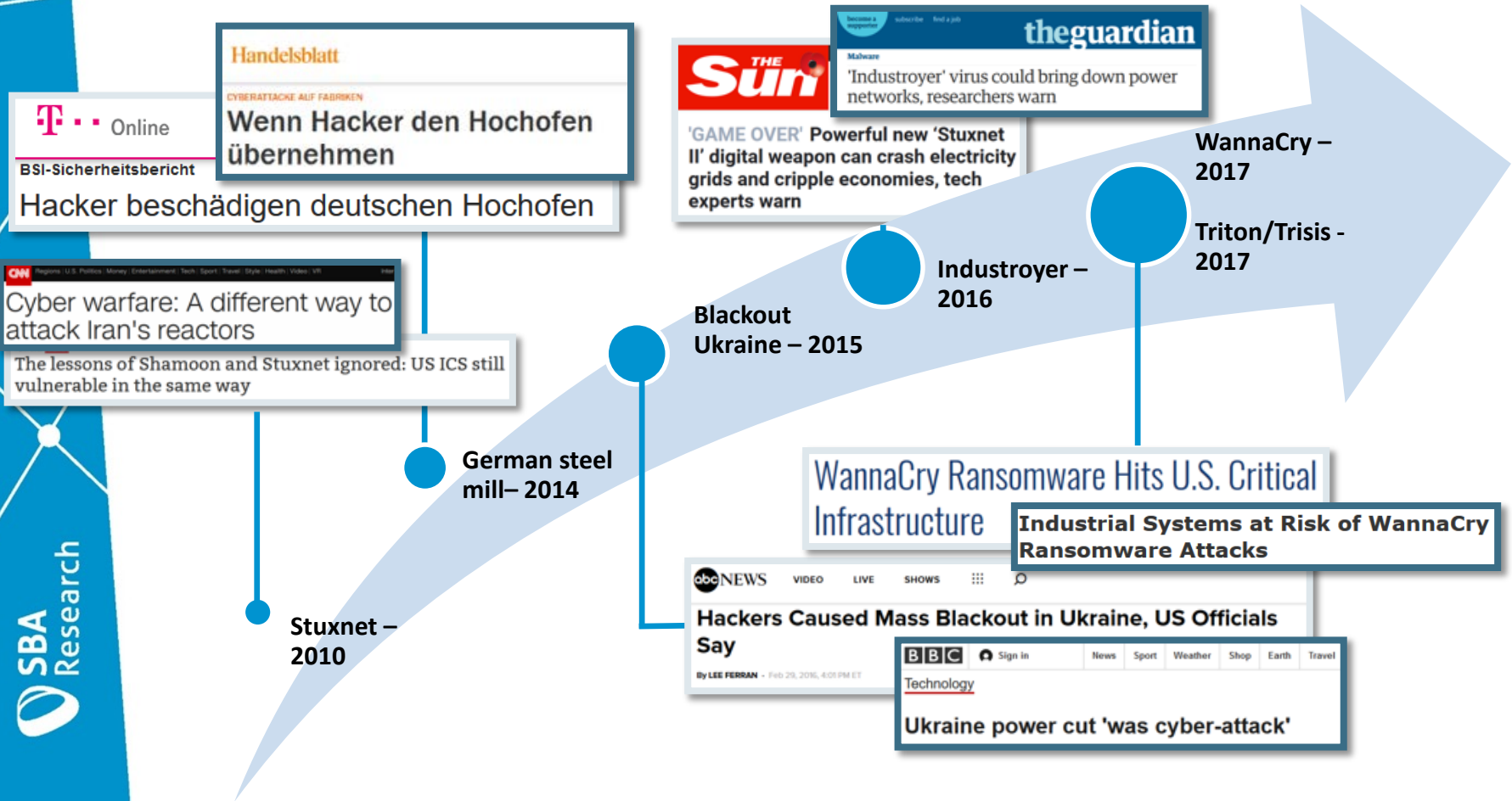
Competence Centers for Excellent Technologies

SECURING THE DEVELOPMENT LIFECYCLE IN PRODUCTIONS SYSTEMS ENGINEERING

Edgar Weippl, SBA Research & CD-Lab SQI.at @TU Wien

SBA Research

Well-known CPS attacks

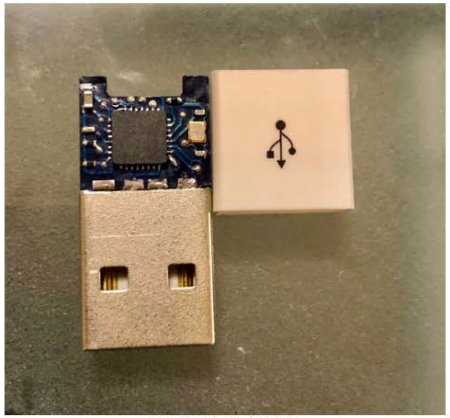


Discarded smart lightbulbs reveal your wifi passwords, stored in the clear

Japanese government plans to hack into citizens' IoT devices

Japanese government wants to secure IoT devices before Tokyo 2020 Olympics and avoid Olympic Destroyer and VPNFilter-like attacks.

By Catalin Cimpanu for Zero Day | January 27, 2019 -- 14:39 GMT (14:39 GMT) | Topic: Security



PCB with Embedded WiFi Chip

In a video demonstration by Grover, you can see how the researcher simply plugs a cable into the PC and is able to connect to it remotely to issue commands through an app on his mobile phone.

https://www.bleepingcomputer.com/news/security/new-offensive-usb-cable-allows-remote-attacks-over-wifi/#.XGMw6lwAr1w.linkedin
https://boingboing.net/2019/01/29/fiat-lux.html
https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/
https://www.zdnet.com/article/japanese-government-plans-to-hack-into-citizens-iot-devices/

SBA Research

Safety vs. Security

- Incentives. Who is hurt?
- Legal aspects

- Fundamental cause:

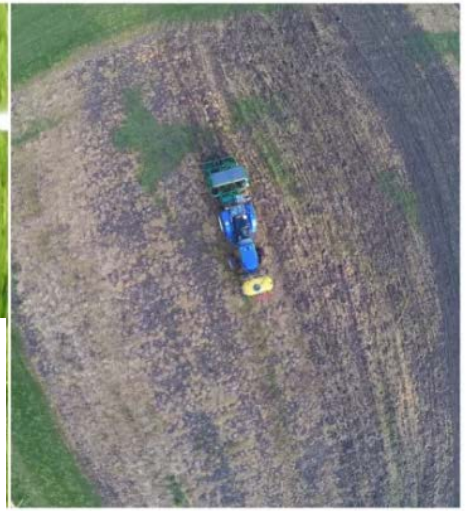
General purpose computer is cheaper than tailor-made machine

ANALYSIS

Drones, tractor hacks and robotic sprayers: the technology of farming

AI machines and digital tools can make farming more efficient and reduce its environmental impact

Ramona Pringle · CBC News · Posted: Sep 17, 2017 5:00 AM ET | Last Updated: October 2, 2017



Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware

A dive into the thriving black market of John Deere tractor hacking.

https://www.cbc.ca/news/technology/farming-technology-advances-1.4290569
https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

SBA Research

Attacks: Replay

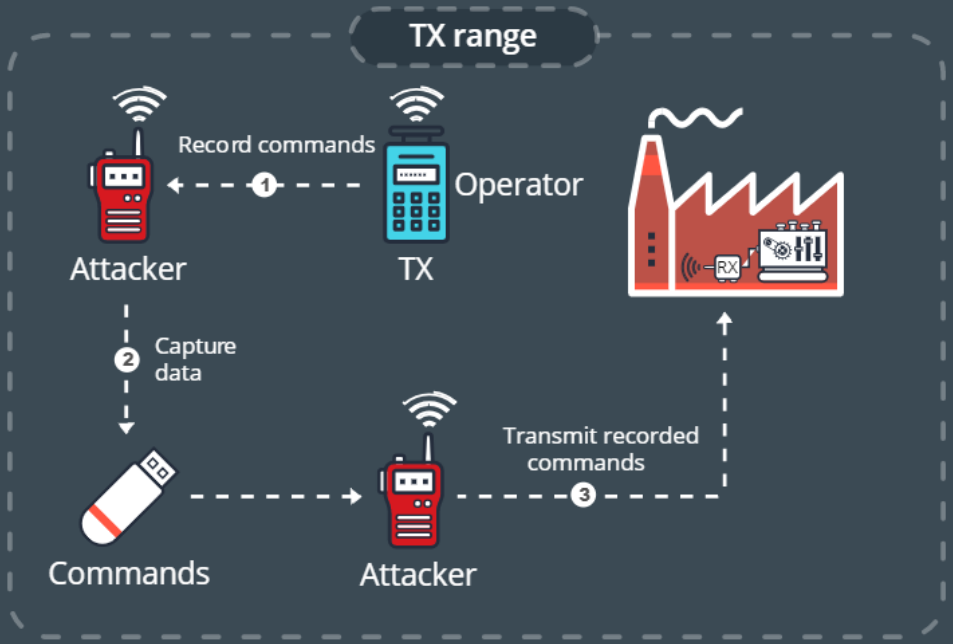
ATTACK 1:

REPLAY ATTACK

DIFFICULTY: EASY

ACCESS: LOCAL OR TEMPORARY LOCAL

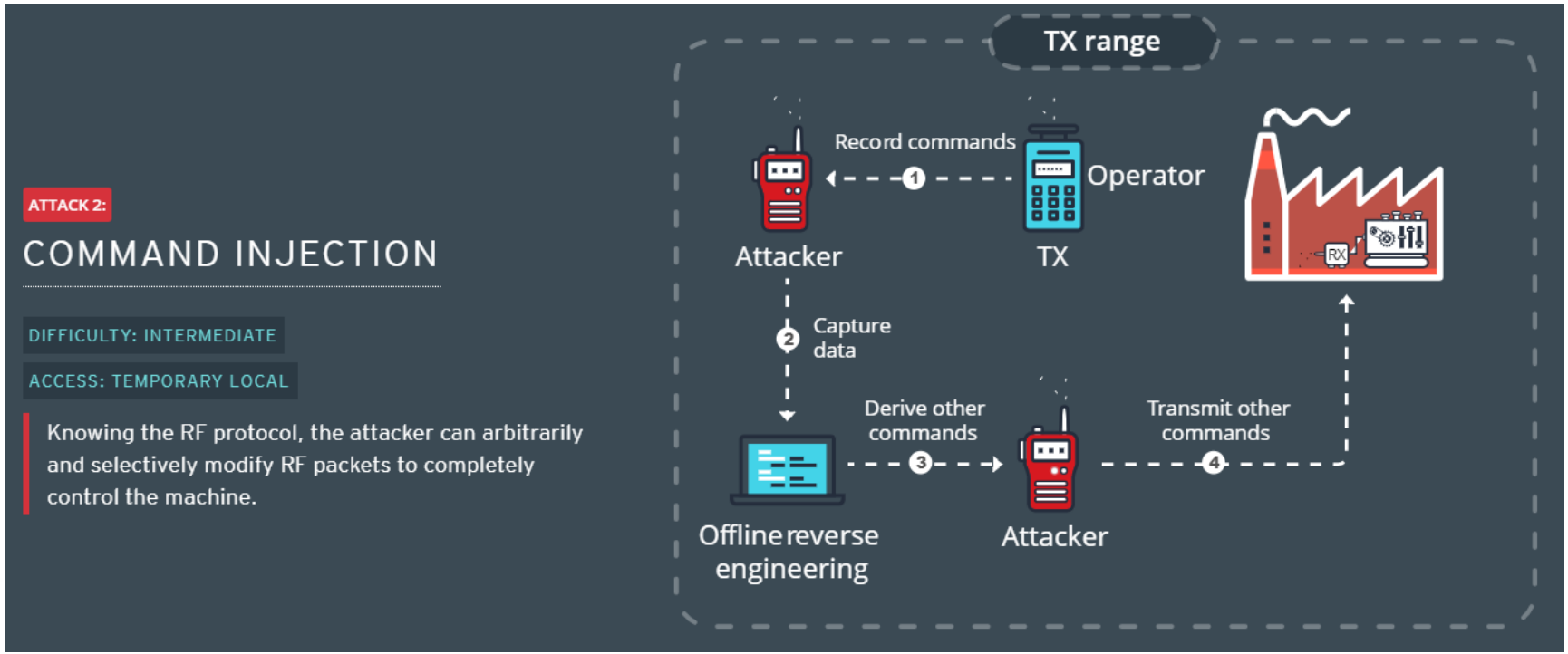
The attacker records RF packets and replays them to obtain basic control of the machine.



https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations
https://youtu.be/XY7MDhE3tfE
https://youtu.be/WXHVA9gGh4o
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

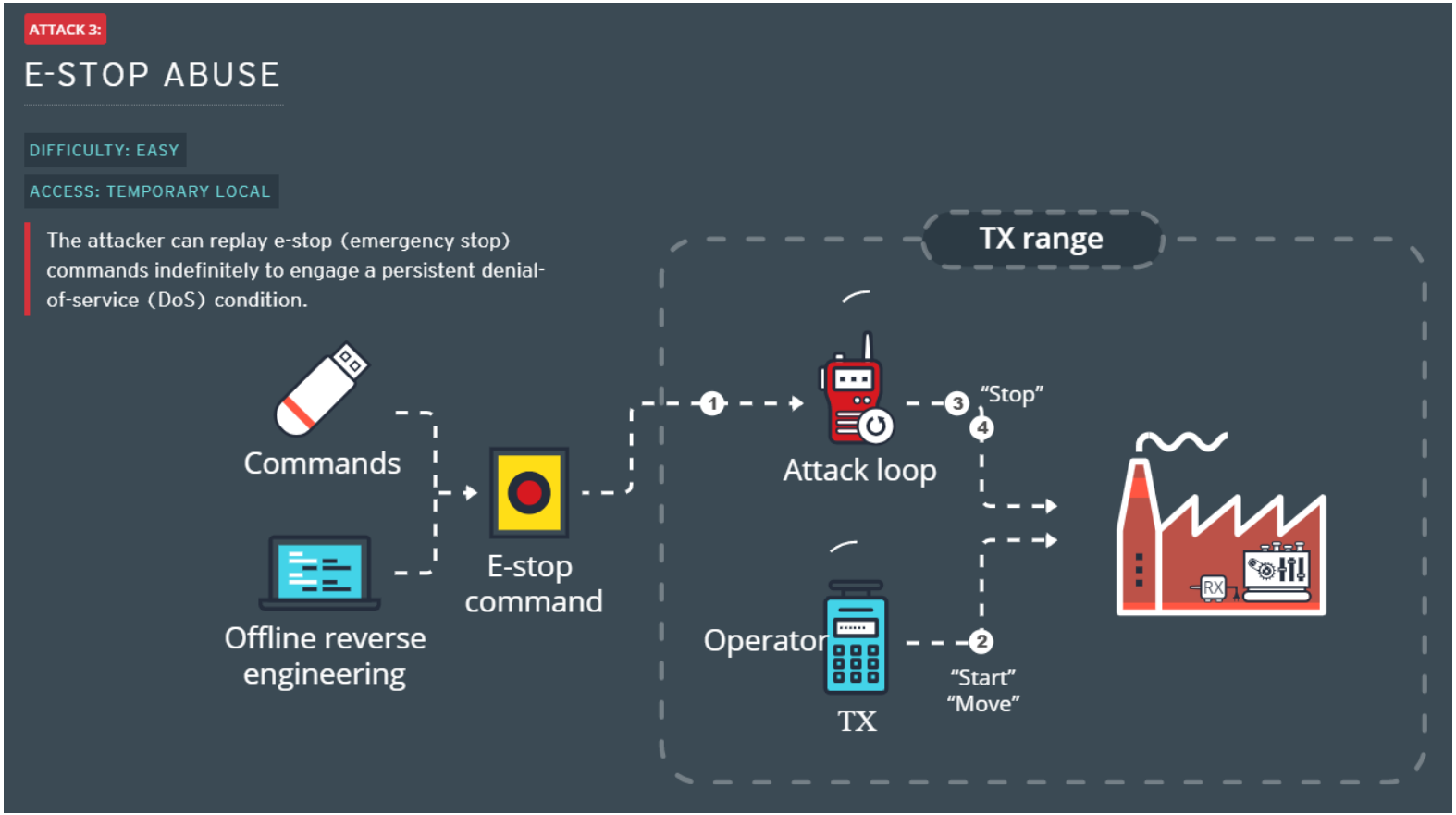
SBA Research

Attacks: Command Injection



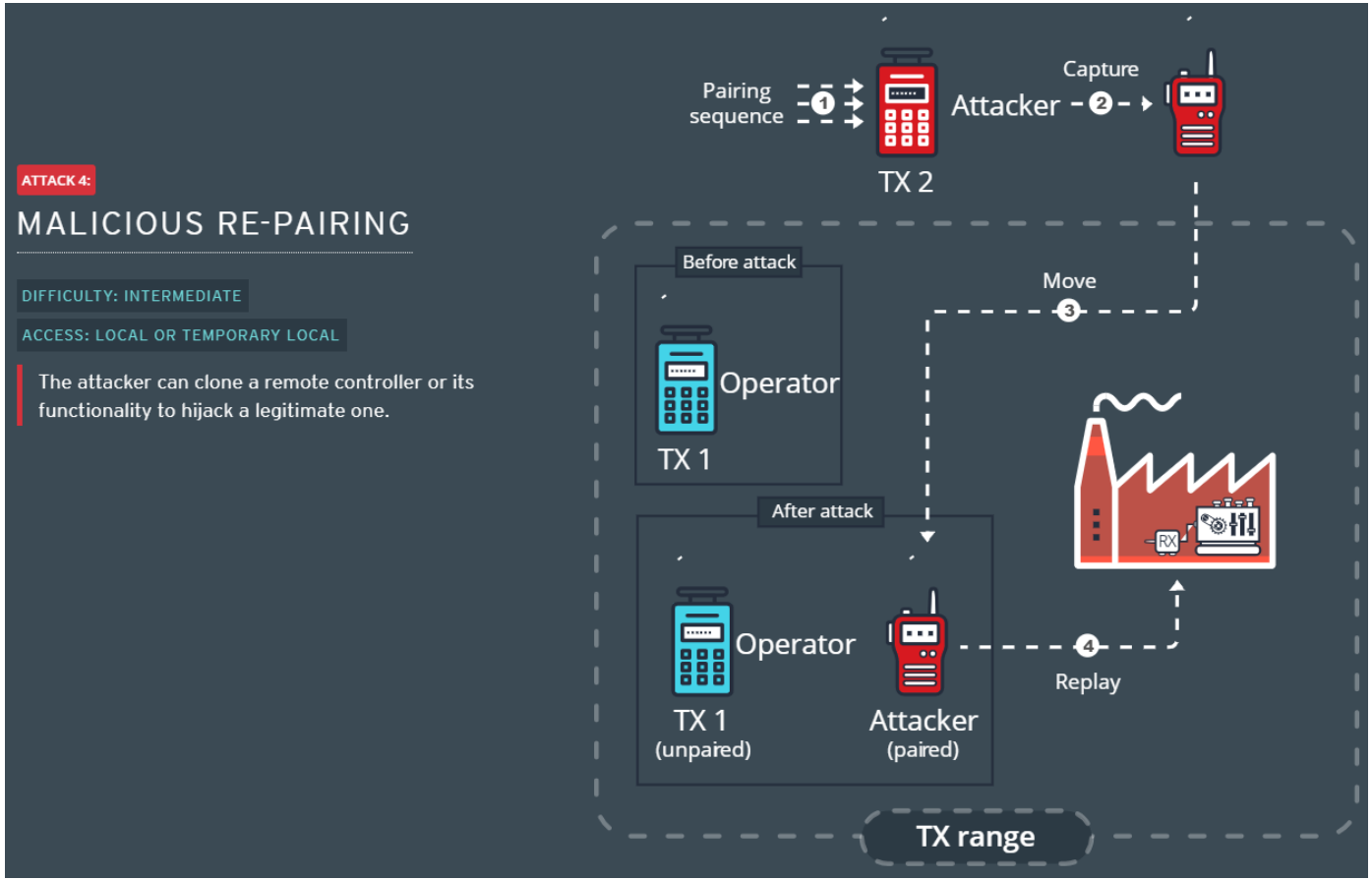
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

Attack: Denial-of-Service



https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

Attack: Impersonation



https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

Attack: Full Control

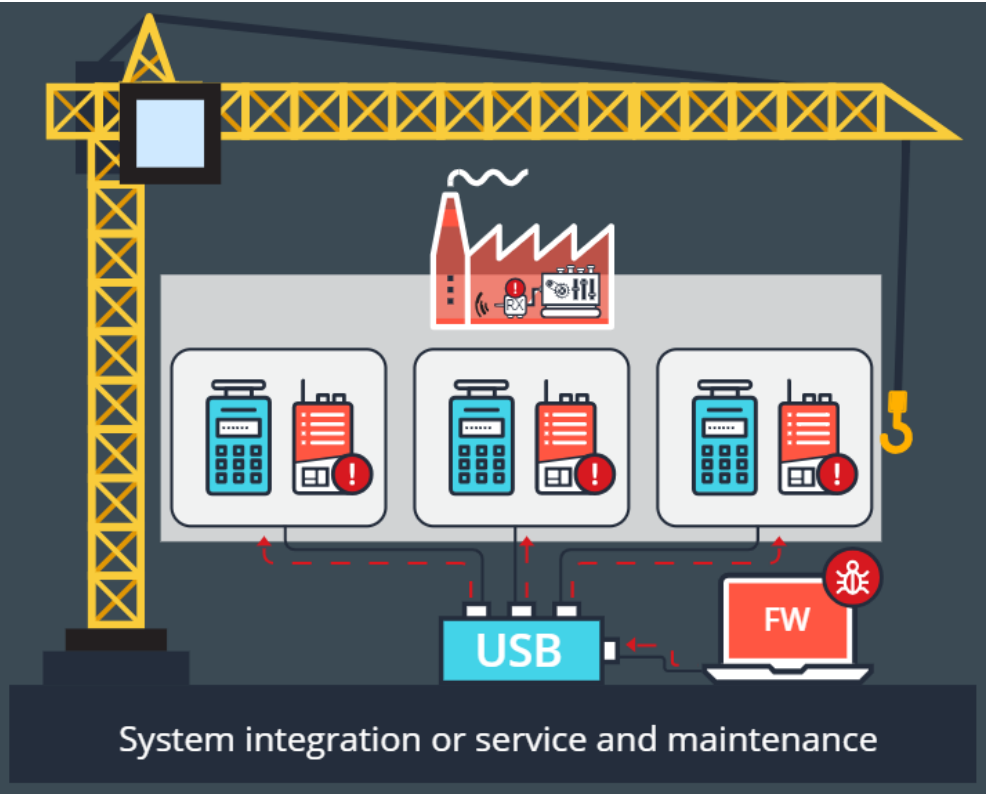
ATTACK 5:

MALICIOUS REPROGRAMMING AND REMOTE ATTACK VECTORS

DIFFICULTY: HARD

ACCESS: REMOTE OR TEMPORARY LOCAL

The attacker “trojanizes” the firmware running on the remote controllers to obtain persistent, full remote control.



https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

SBA Research


https://www.economist.com/node/471614
WIEN

Reflections on Trusting Trust

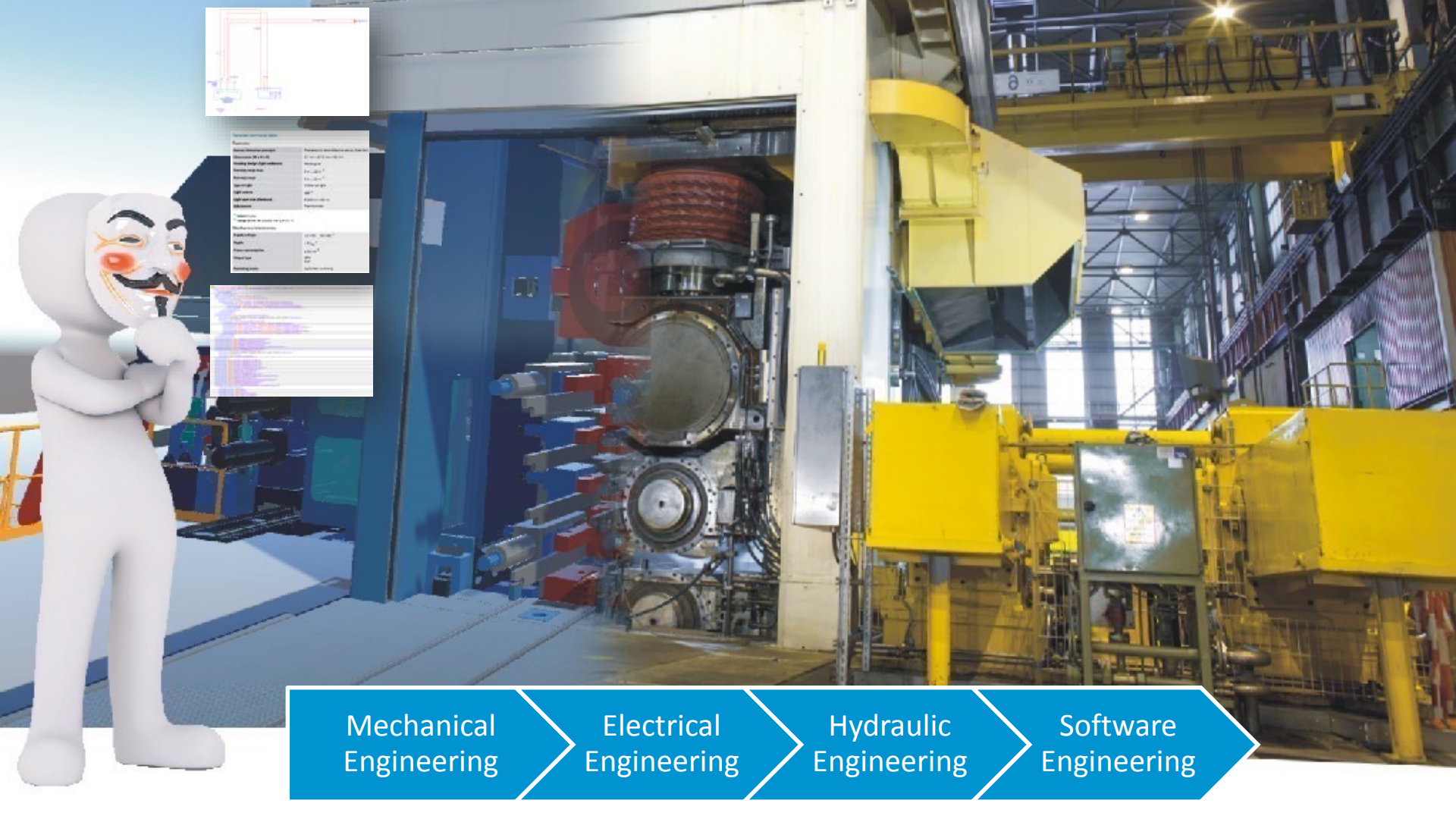
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

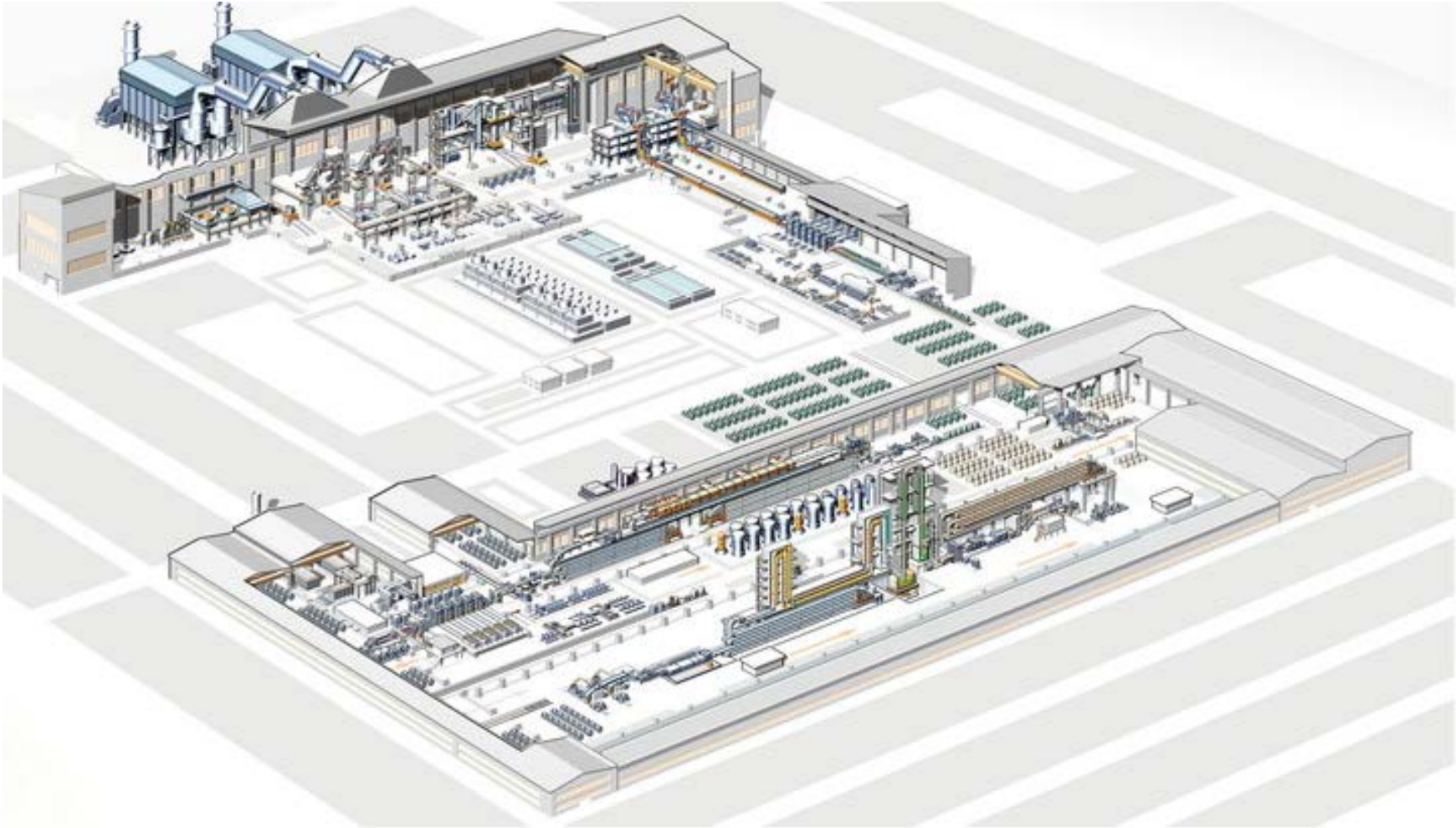
I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.

Peter Hamer - Uploaded by Magnus Manske
https://en.wikipedia.org/wiki/Ken_Thompson#/media/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg

KEN THOMPSON

Ken Thompson. 1984. Reflections on trusting trust. Commun. ACM 27, 8 (August 1984), 761-763. DOI=http://dx.doi.org/10.1145/358198.358210

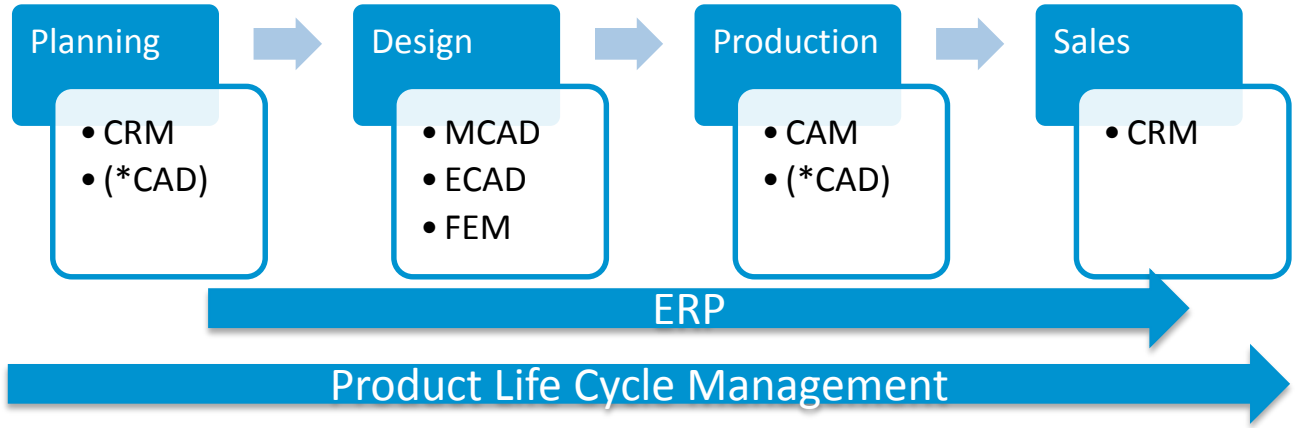

Mechanical Engineering
Electrical Engineering
Hydraulic Engineering
Software Engineering



https://www.sms-group.com/press-media/press-releases/press-detail/big-river-steel-officially-opens-north-americas-latest-steel-complex-725/

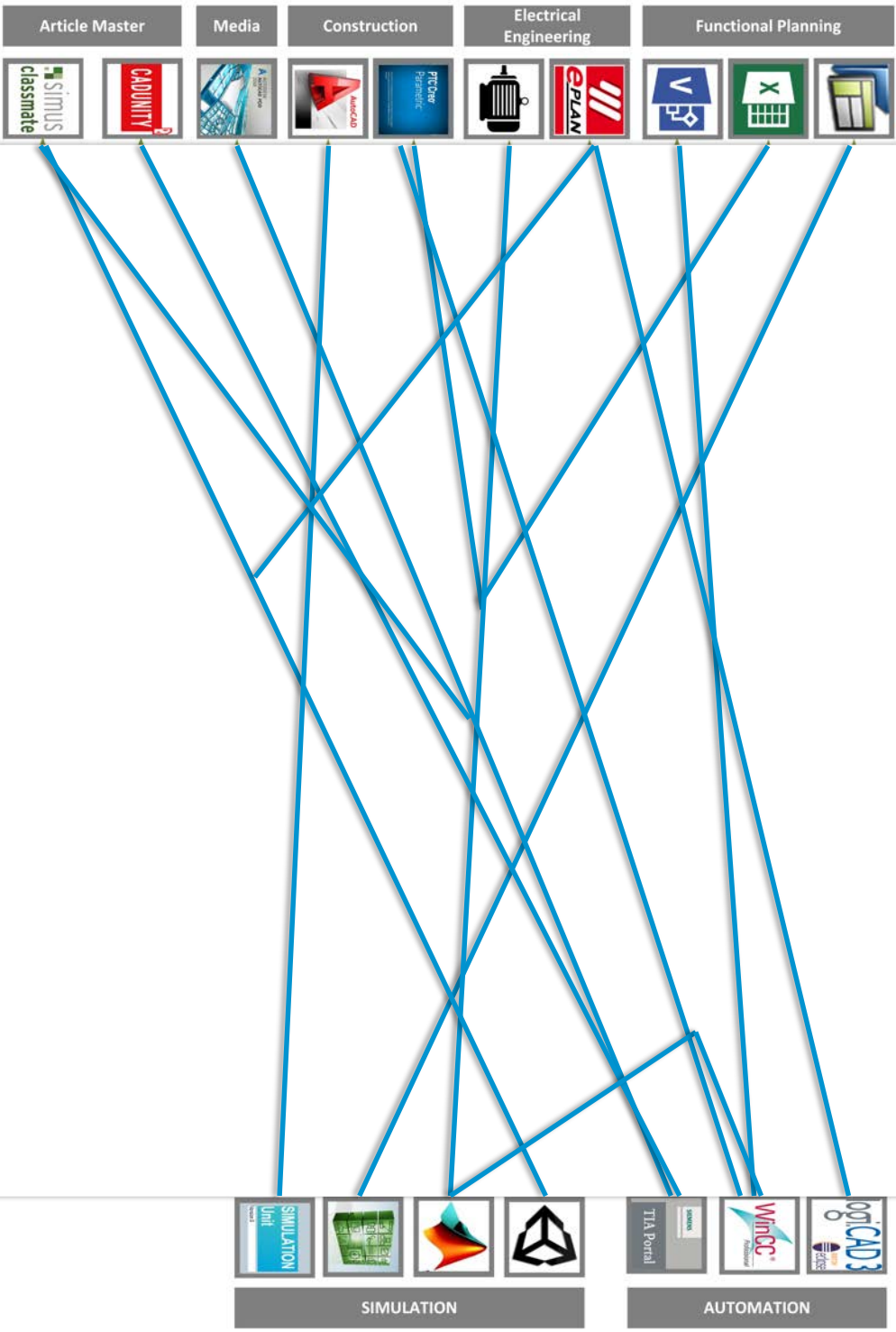
http://www.laweco.de/.cms/Blech_Industrie/183-1

Product Lifecycle



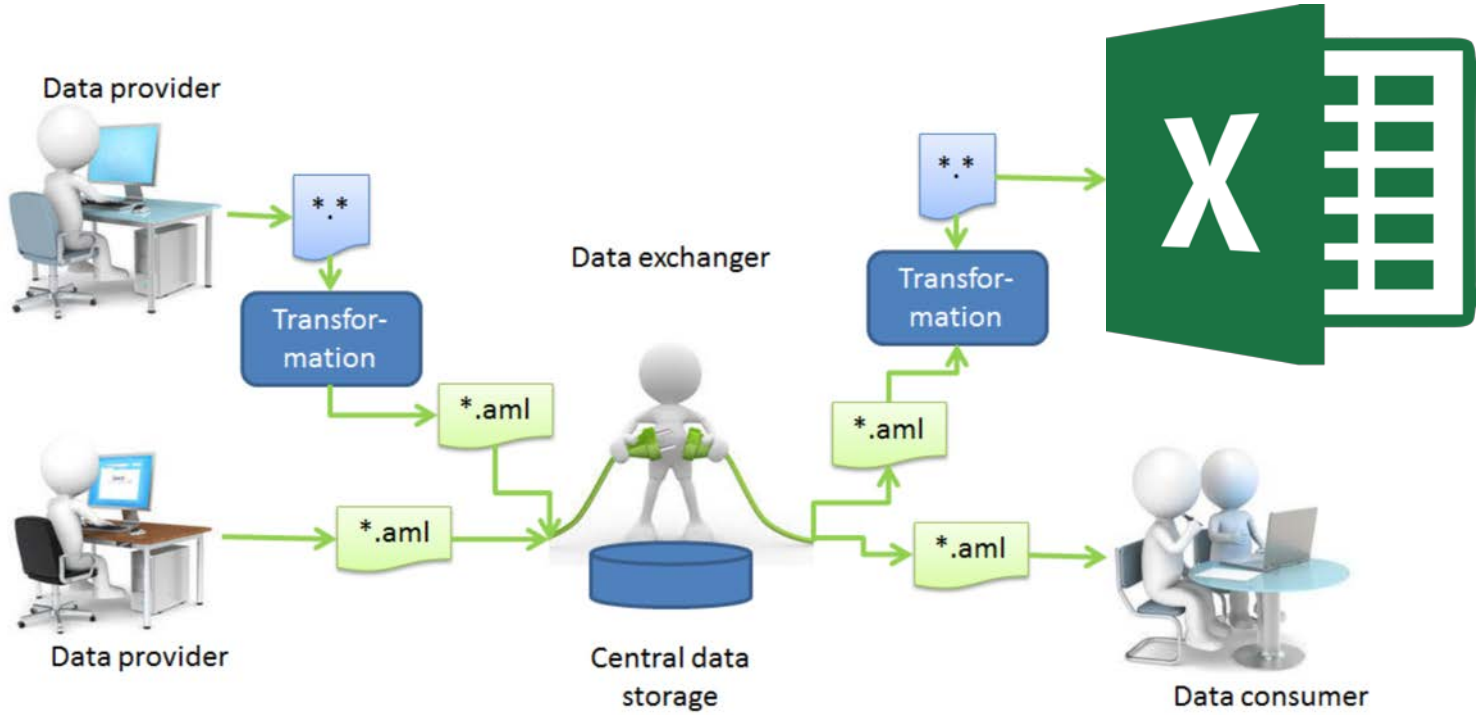
SBA Research

SBA Research



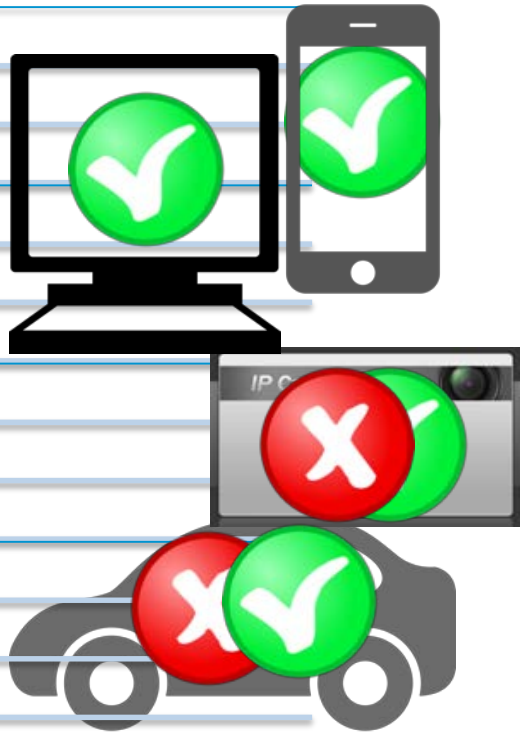
SBA Research

Transformation is good…



Adoption of Software Security is difficult

Governance	Strategy & Metrics (SM)
	Compliance & Policy (CP)
	Training (T)
Intelligence	Attack Models (AM)
	Security Features & Design (SFD)
	Standards & Requirements (SR)
SSDL Touchpoints	Architecture Analysis (AA)
	Code Review (CR)
	Security Testing (ST)
Deployment	Penetration Testing (PT)
	Software Environment (SE)
	Configuration M. & Vulnerability Management (CMVM)



Source: https://www.bsimm.com/

SBA Research

Changes in Production System Engineering

- Centrally accessible data repositories
- Global collaboration with partially trusted and untrusted parties
- Modern information technology in PSE
  - Security Mechanisms in a production system environment
  - Threat Landscape

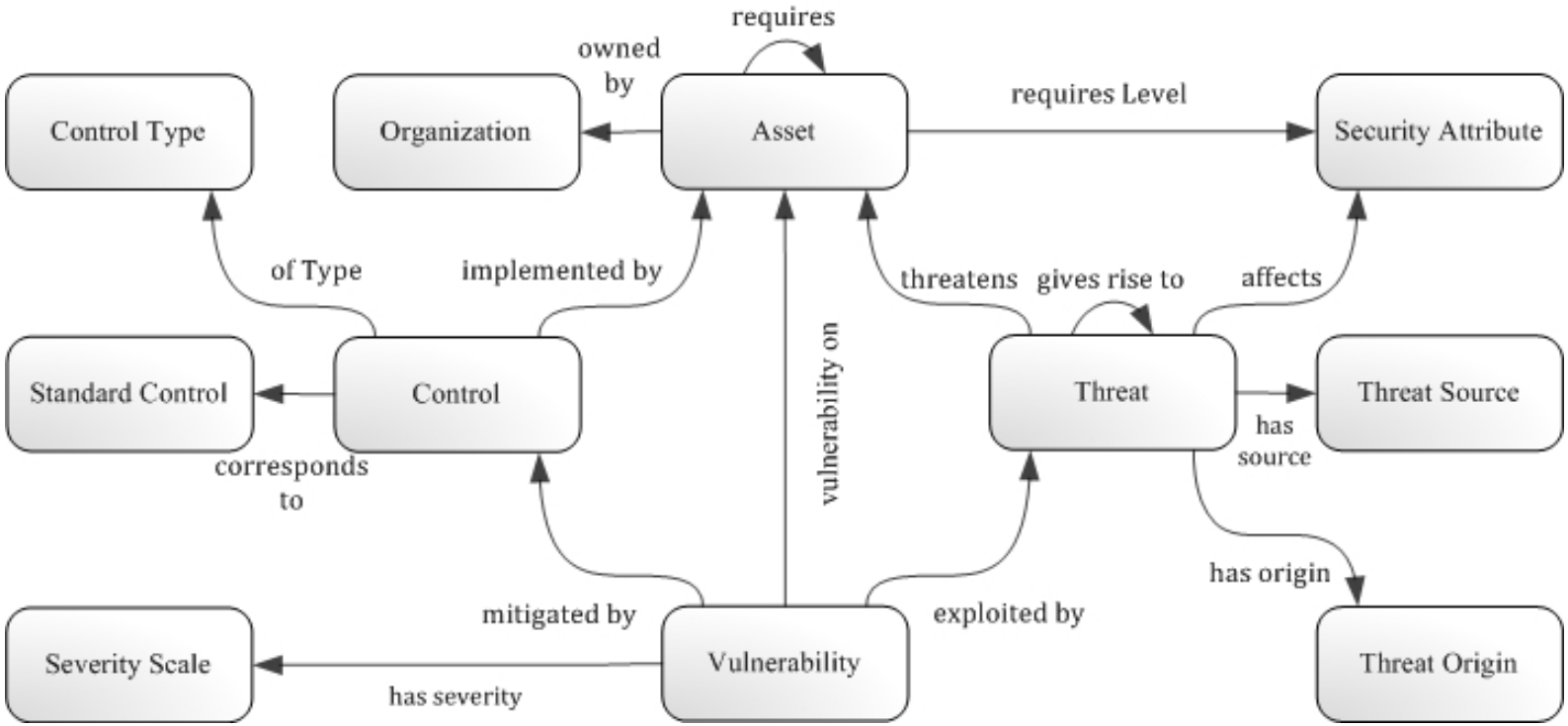
SBA Research

Centrally accessible data repositories

- Data Provenance
  - Tools modify certain properties
  - Software errors
- Remote Attestation
  - Sensors in adversarial environment
- Availability and Confidentiality of Testing Data
  - Modelling “everything”?
  - Verfication vs. real world, e.g. KRACK

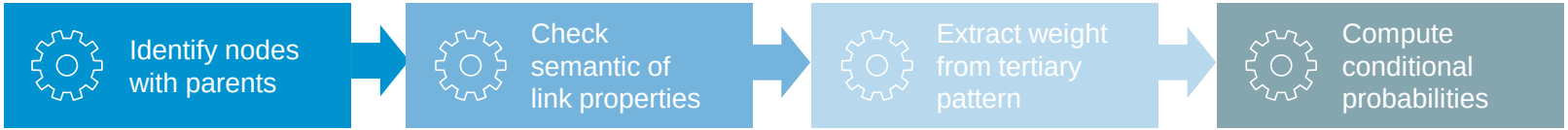
SBA Research

Security Ontology



S. Islam, S. Fenz, E. Weippl, H. Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support", Journal of Risk and Financial Management, 10 (2017), 1 – 24.

Ontology-based Bayesian Network Construction

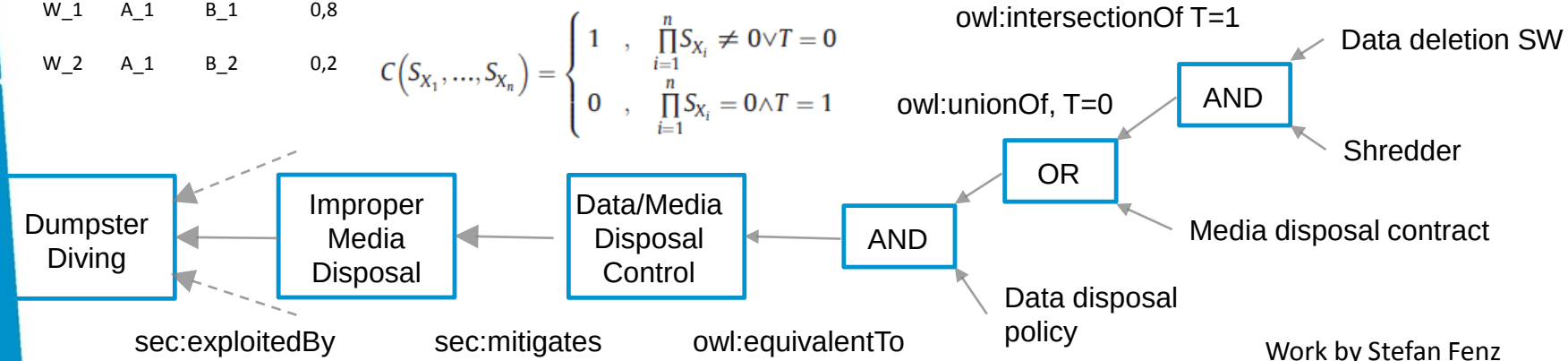


Class W

Ind	Child	Parent	Val
W_1	A_1	B_1	0,8
W_2	A_1	B_2	0,2

$$P(N|X_1,\ldots,X_n)=\left(\left(\frac{S_{X_1}}{h_{X_1}}*w_{X_1}\right)+\ldots+\left(\frac{S_{X_n}}{h_{X_n}}*w_{X_n}\right)\right)*C\left(S_{X_1},\ldots,S_{X_n}\right)$$

$$C\left(S_{X_1},\ldots,S_{X_n}\right)=\begin{cases}1 & , \prod_{i=1}^{n} S_{X_i}\neq 0 \vee T=0\\ 0 & , \prod_{i=1}^{n} S_{X_i}=0 \wedge T=1\end{cases}$$



Work by Stefan Fenz

EWeippl@sba-research.org