Bridging the air-gap

Out of sight, (but not) out of mind

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Agenda

- Motivation
- Attack scenario
- Famous examples
- Academic research
- Future attack vectors

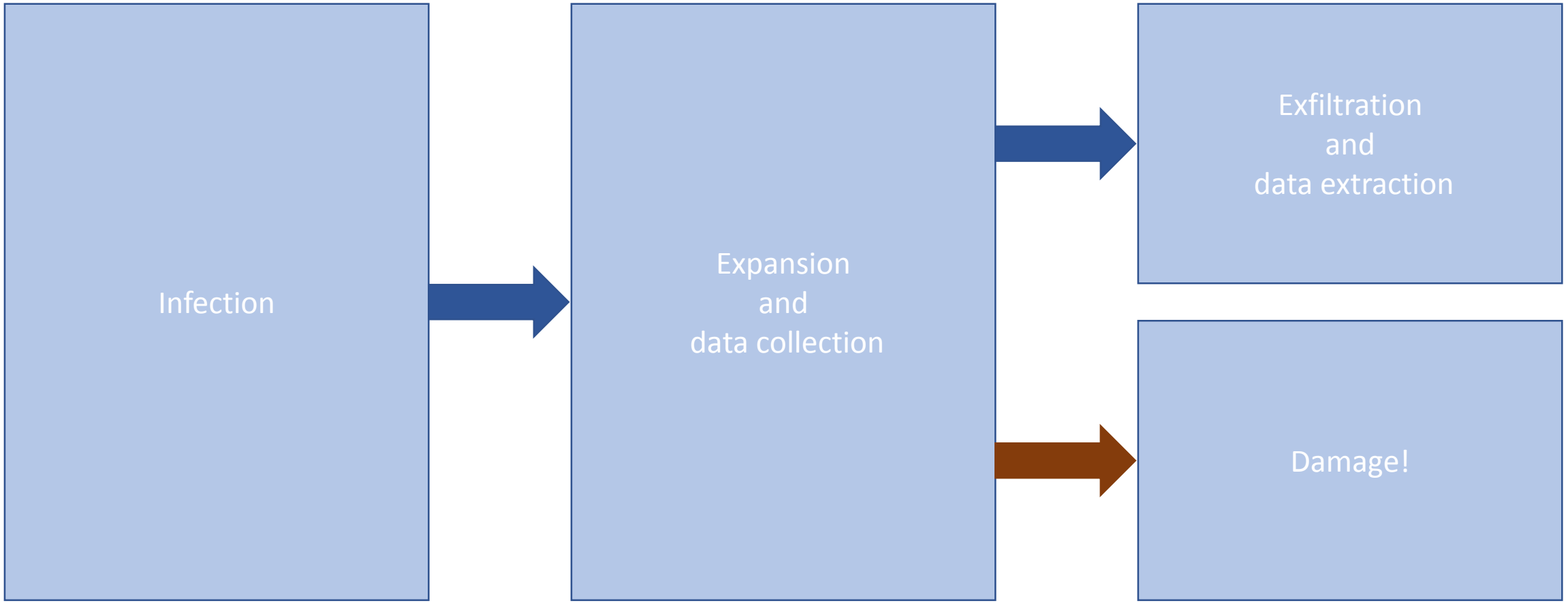
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Agenda

- Motivation
- Attack scenario
- Famous examples
- Academic research
- Future attack vectors

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Attack scenario



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Agenda

- Motivation
- Attack scenario
- Famous examples
- Academic research
- Future attack vectors

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Agent.BTZ

Infection

The Register®
Biting the hand that feeds IT

Security 21

US Army bans USB devices to contain worm

Unfriendly fire

By John Leyden 20 Nov 2008 at 13:41 SHARE ▼

The US Army has reportedly suspended the use of USB and removable media devices after a worm began spreading across its network.

Use of USB drives, floppy discs, CDs, external drives, flash media cards and all other removable media devices has been placed on hold in order

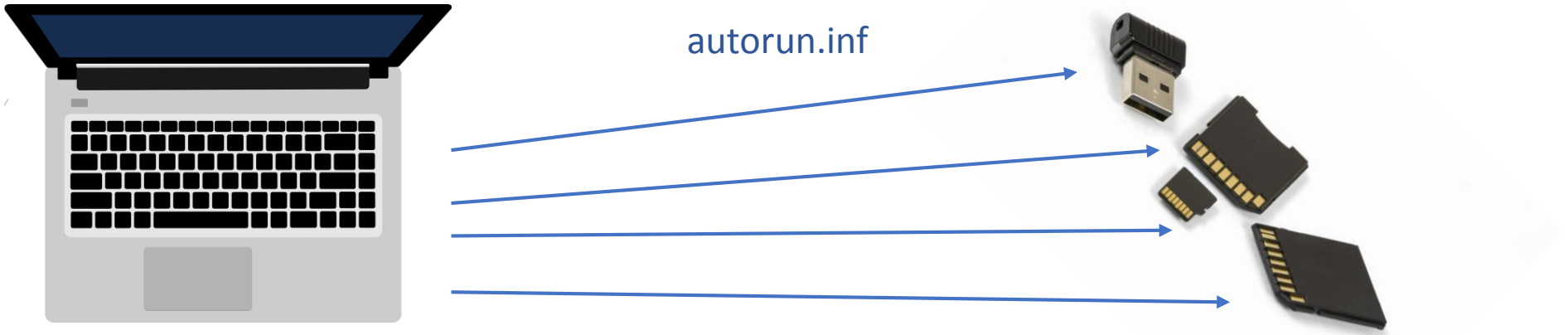
autorun.inf

```
rundll32.exe .\\[random_name].dll,InstallM
```


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Agent.BTZ

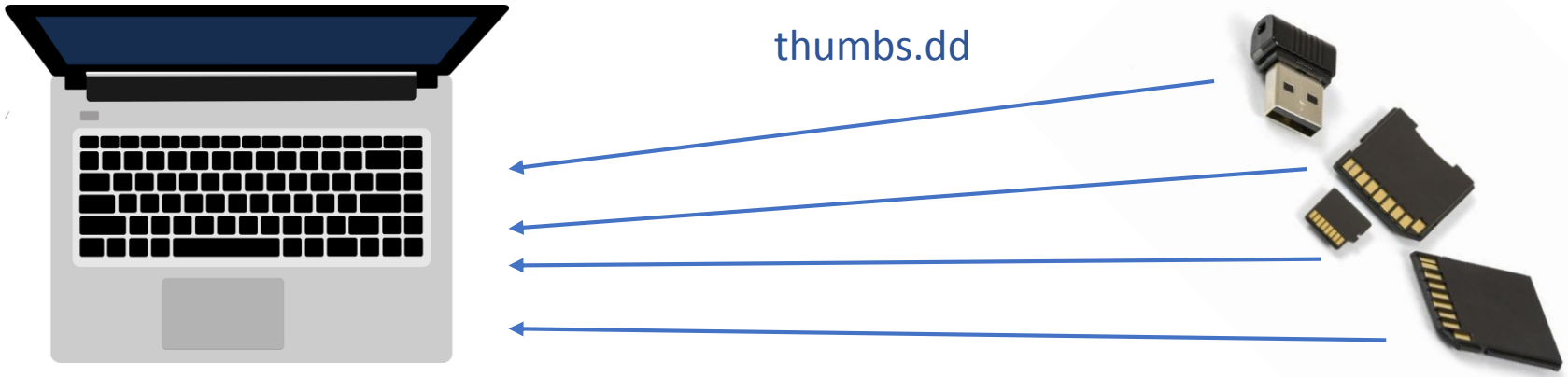
Infection → Expansion



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

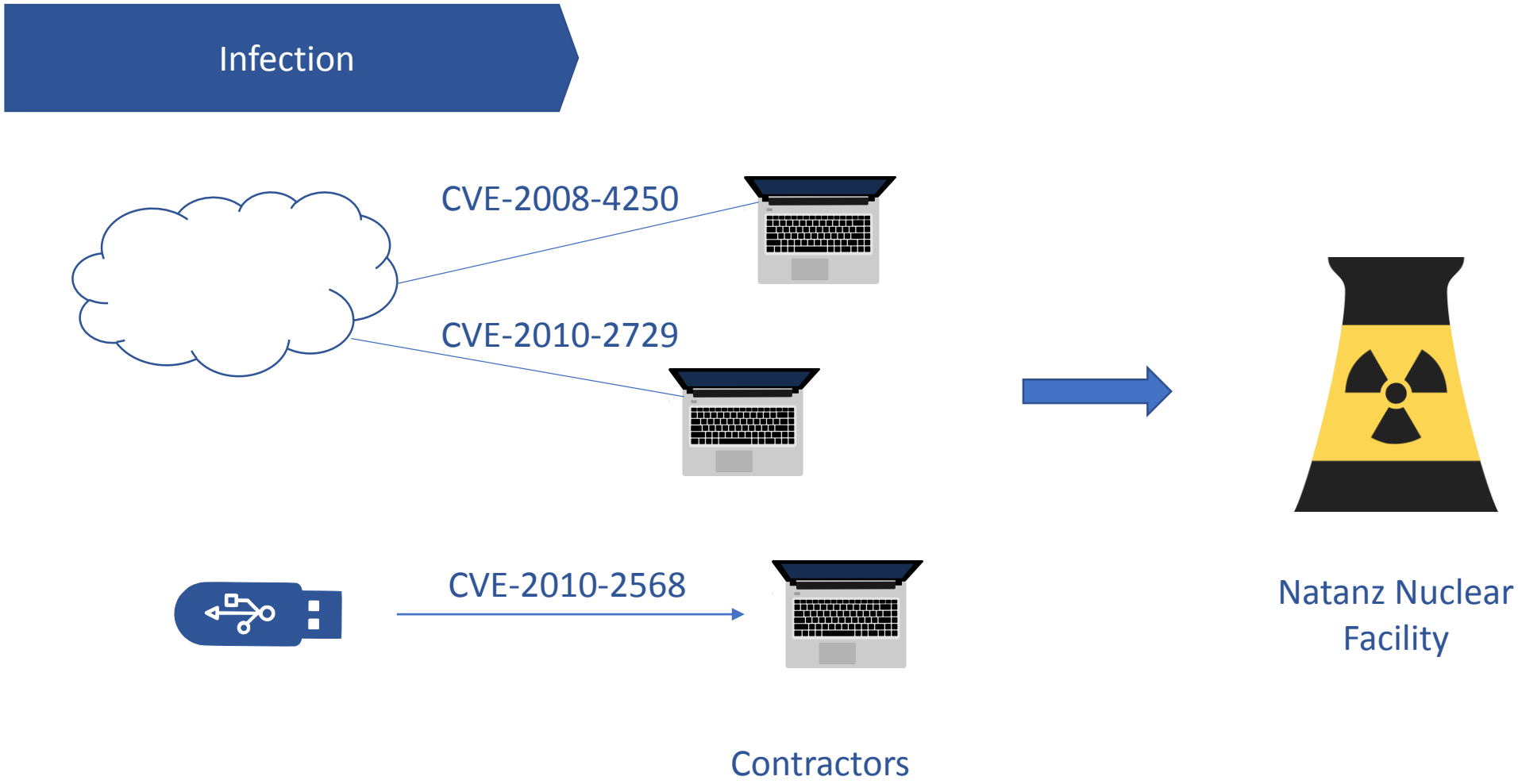
Famous examples: Agent.BTZ

Infection → Expansion → Extraction



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

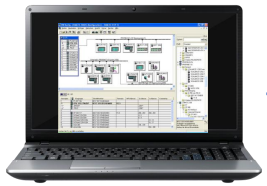
Famous examples: Stuxnet



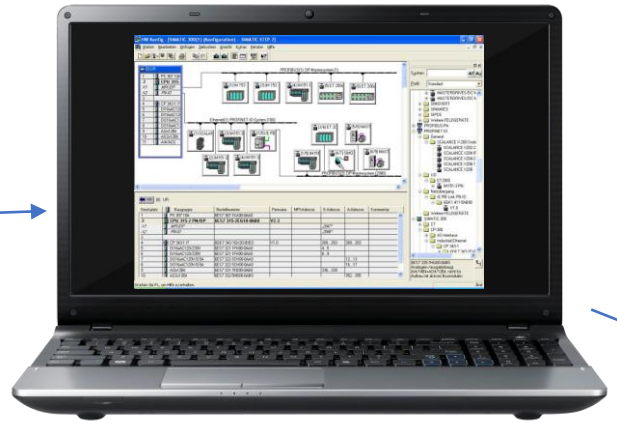
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Stuxnet

Infection → Expansion



CVE-2010-2772
CVE-2012-3015



Modified STL code

S7-417

S7-315

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

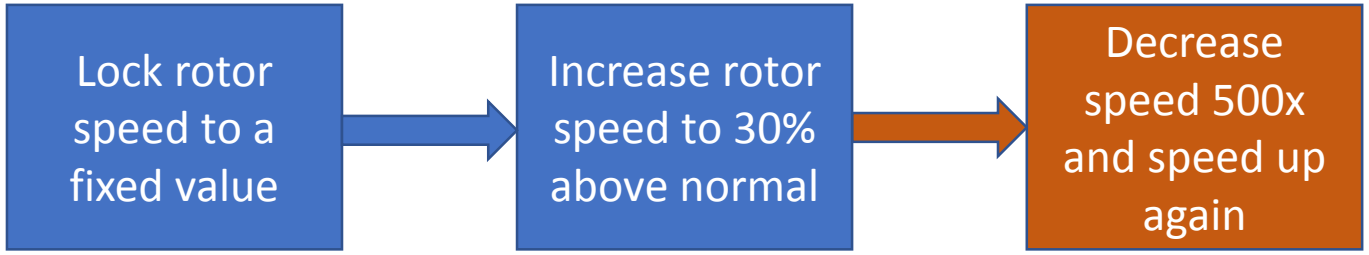
Famous examples: Stuxnet

Attack 1 – Centrifuge Overpressure Protection System

S7-417

Attack 2 – Centrifuge Drive System

S7-315

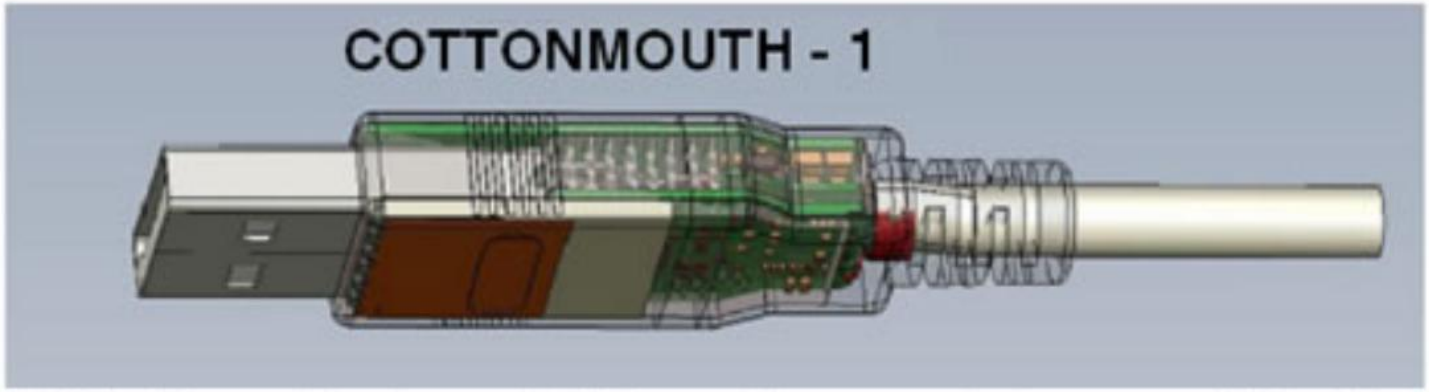


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: COTTONMOUTH

COTTONMOUTH-I

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



http://www.nsaplayset.org/turnipschool

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: COTTONMOUTH

COTTONMOUTH-I → COTTONMOUTH-II

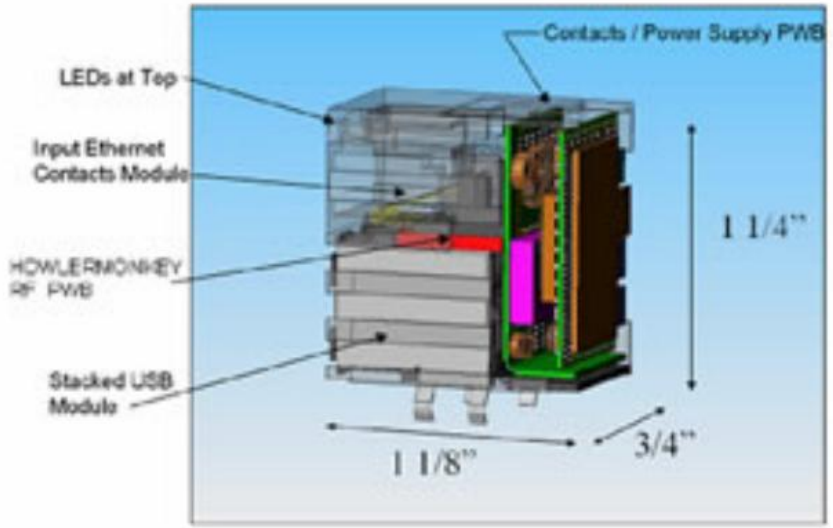
(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: COTTONMOUTH

COTTONMOUTH-I → COTTONMOUTH-II → COTTONMOUTH-III

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant, which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Brutal Kangaroo

Infection

Brutal Kangaroo

Drifting Deadline (infection)	Shattered Assurance (expansion)	Broken Promise (postprocessor)	Shadow (persistence)
None (Manual)	EZCheese (CVE-2015-0096)	Lachesis (autorun.inf)	RiverJack (library-ms)

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Brutal Kangaroo

Brutal Kangaroo

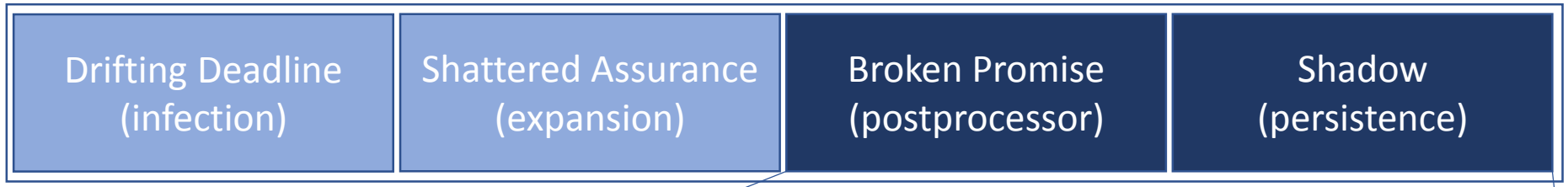
Drifting Deadline (infection)	Shattered Assurance (expansion)	Broken Promise (postprocessor)	Shadow (persistence)

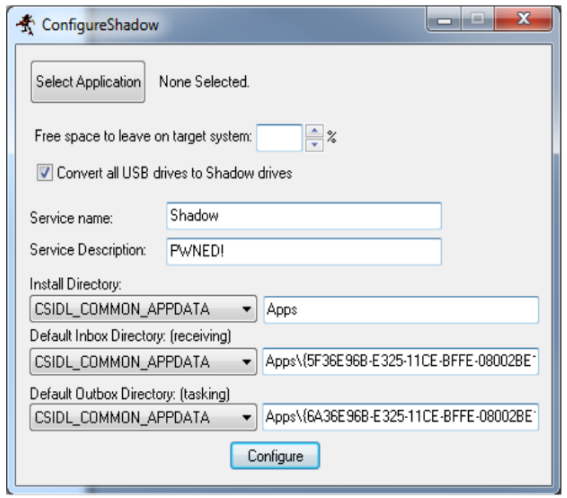
Shattered Assurance: A server tool that handles automated infection of thumbdrives and the primary mode of propagation for the Brutal Kangaroo suite. Shattered Assurance utilizes Drifting Deadline for the individual infection of thumbdrives

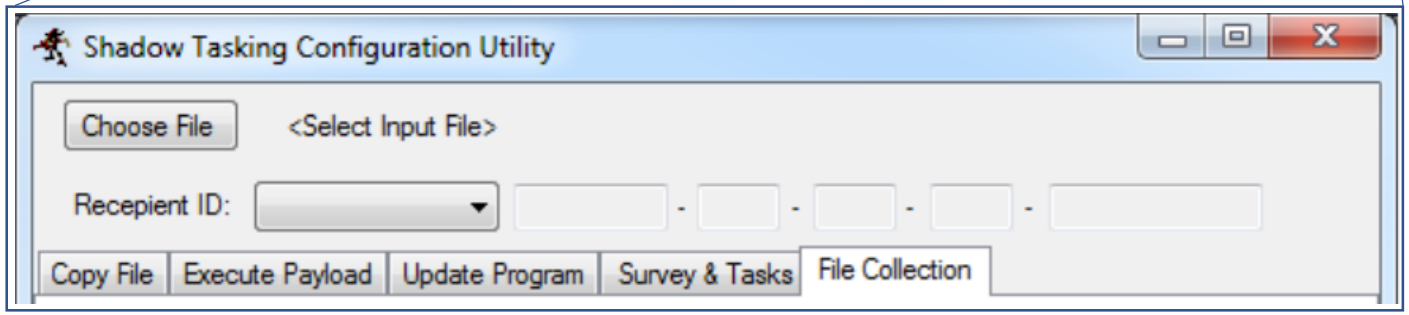
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Famous examples: Brutal Kangaroo

Brutal Kangaroo







Nemanja Nikodijevic <nemanja@micropsi-industries.com>

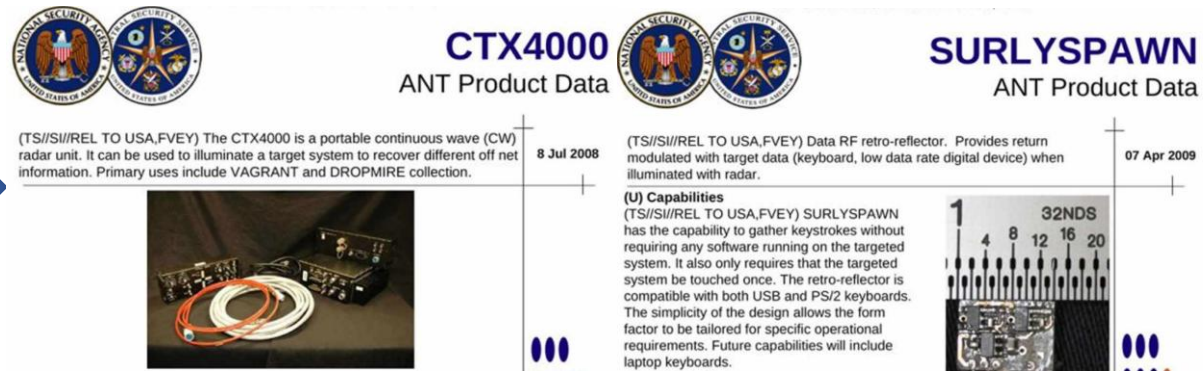
Agenda

- Motivation
- Attack scenario
- Famous examples
- Academic research
- Future attack vectors

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

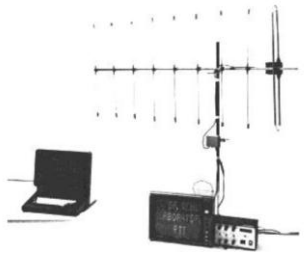
Research: Covert-channels

Electromagnetic

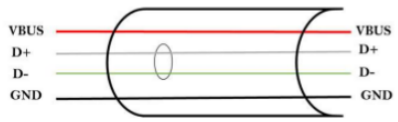


FOSDEM ‘16
JM Friedt
http://bit.ly/2wTsXGs

Van Eck Phreaking



USBee, AirHopper, GSMem (Guri et al.)

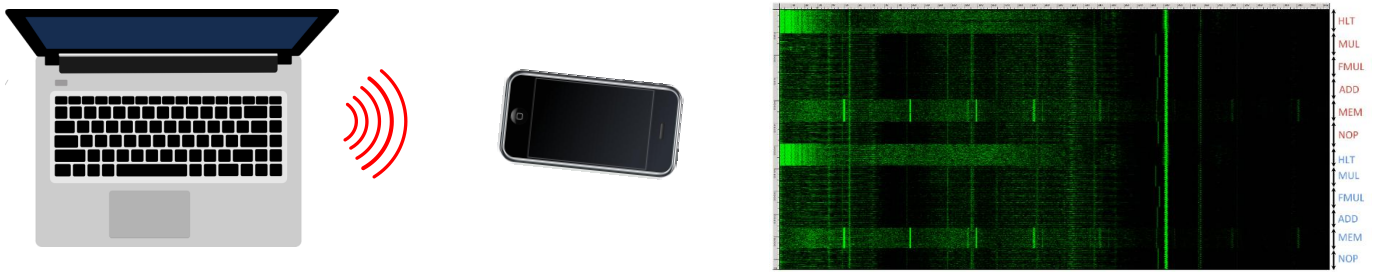


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Research: Covert-channels

Electromagnetic | Acoustic

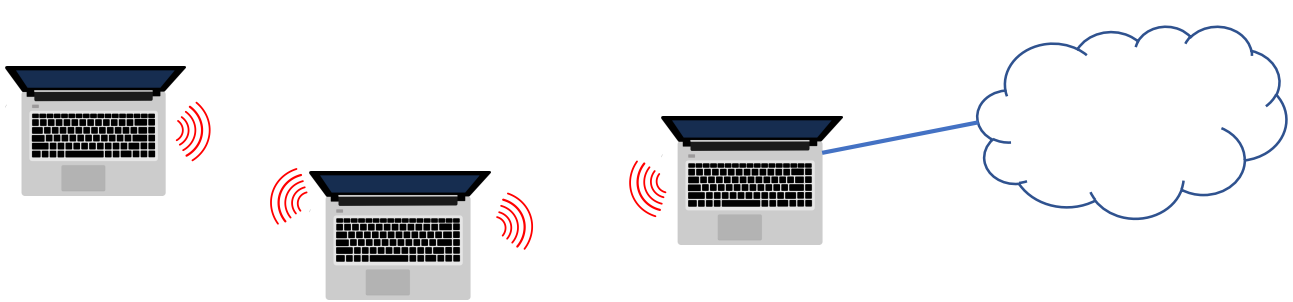
RSA Acoustic Cryptanalysis (Genkin et al.)

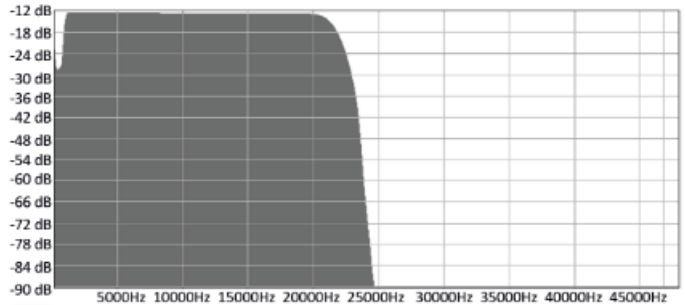


badBIOS

?

On Covert Acoustical Mesh Networks in Air (Hanspach and Goetz)





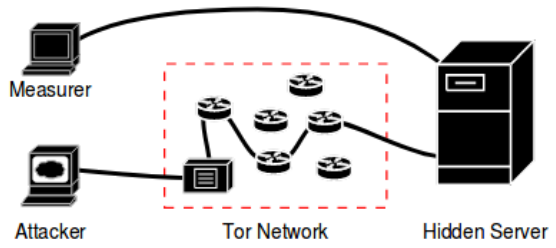
BALCCON2K17
U CNT CTRL ME

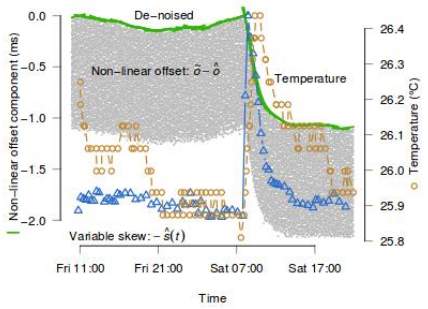
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Research: Covert-channels

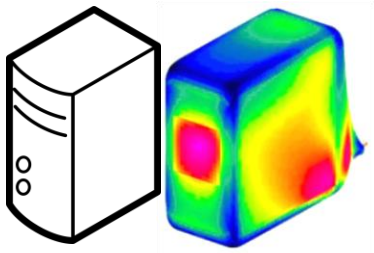
Electromagnetic | Acoustic | **Thermal**

Revealing Hidden Services by their Clock Skew (Murdoch)

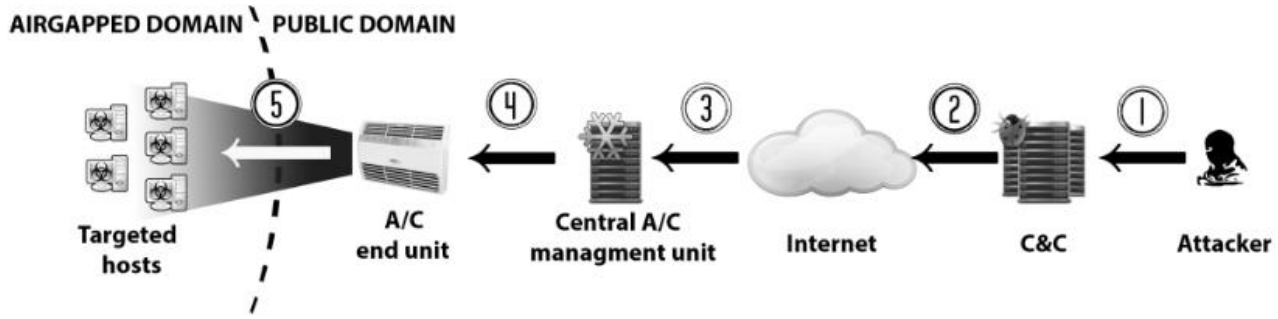




BitWhisper (Guri et al.)



HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System (Mirsky et al.)

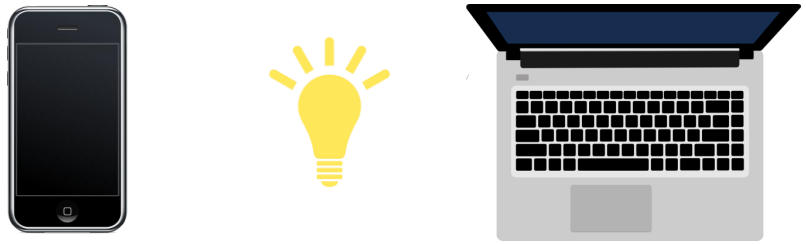


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Research: Covert-channels

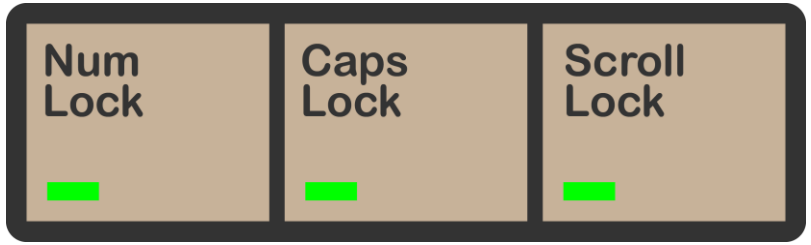
Electromagnetic → Acoustic → Thermal → Light

Ambient Light Sensors (Hasan et al.)



xLED (Guri et al.)

Information Leakage from Optical Emanations (J. Loughry and D. A. Umphress)



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Research: Covert-channels

Electromagnetic → Acoustic → Thermal → Light → Other

Seismic

Magnetic

Sensing-Enabled Channels for Hard-to-Detect Command and Control of Mobile Devices (Hasan et al.)

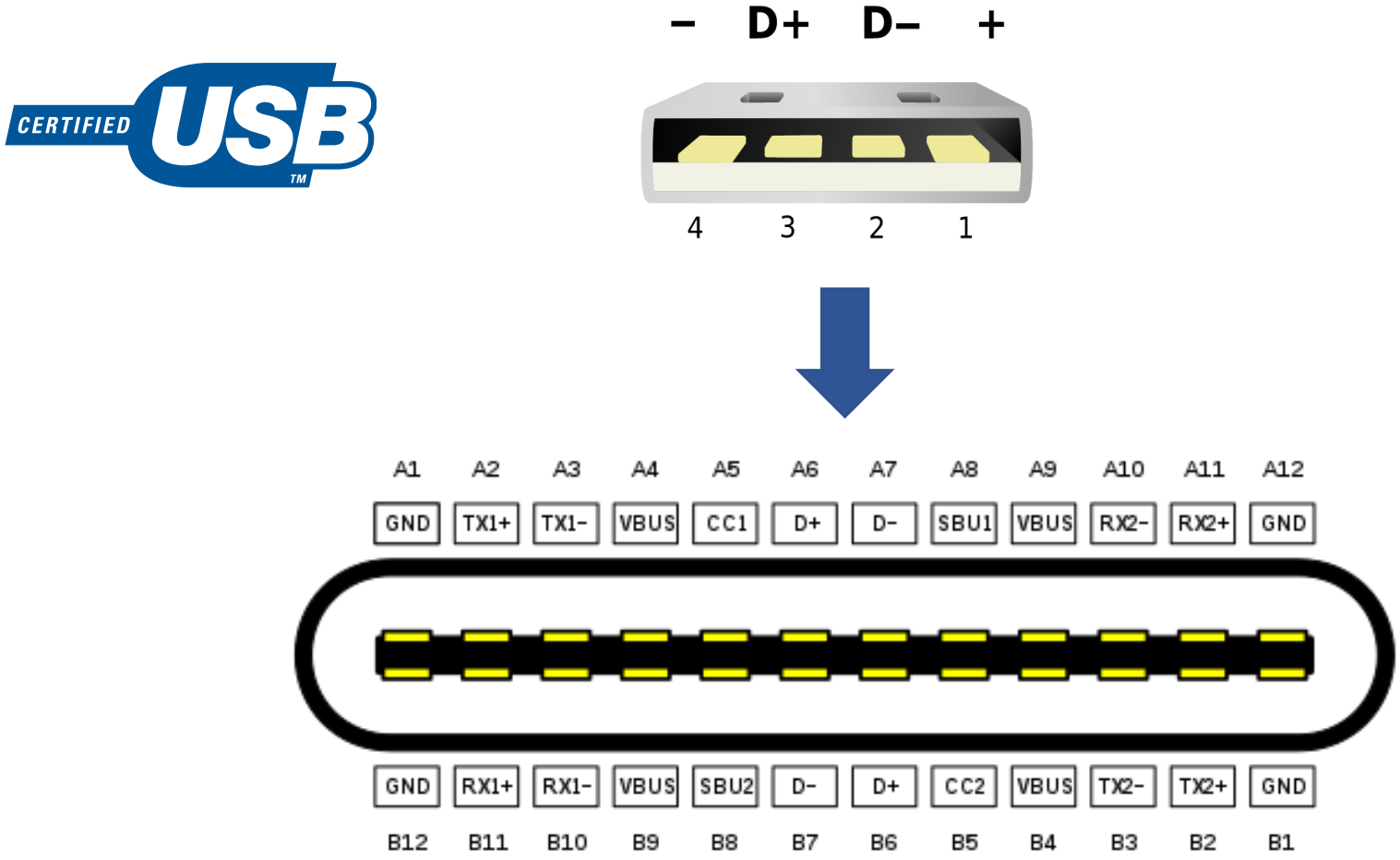
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Agenda

- Motivation
- Attack scenario
- Famous examples
- Academic research
- Future attack vectors

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

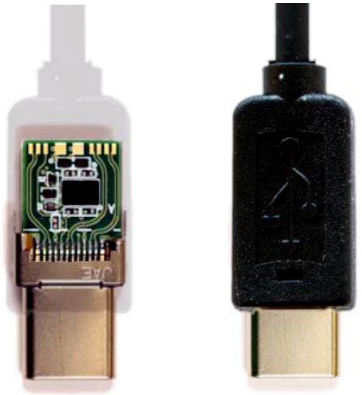
Future?



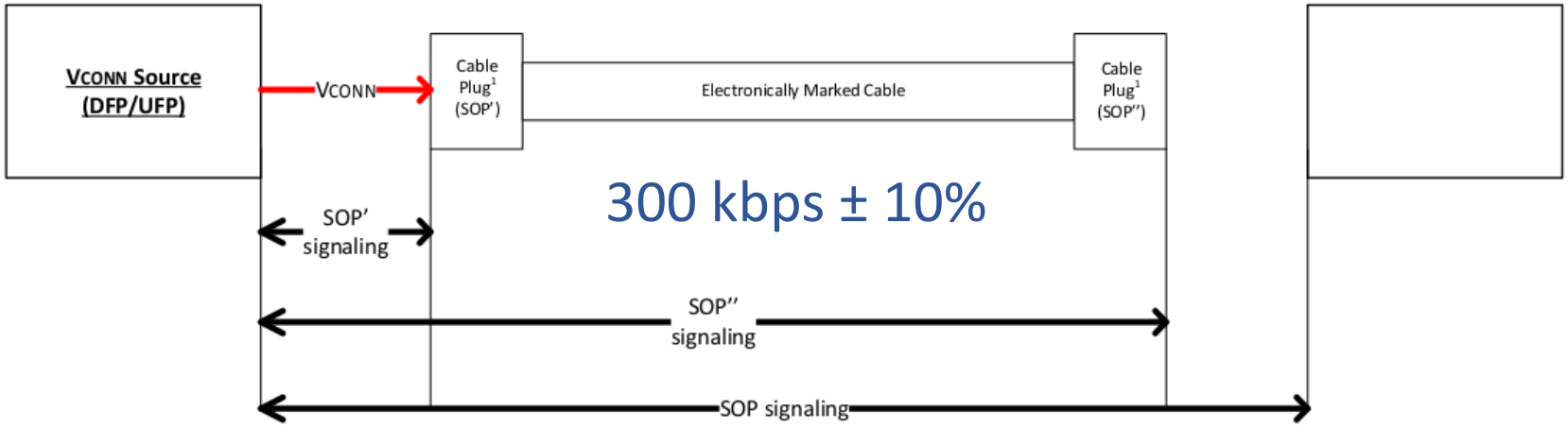
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Example attack vectors

Evil Cable



EMCA



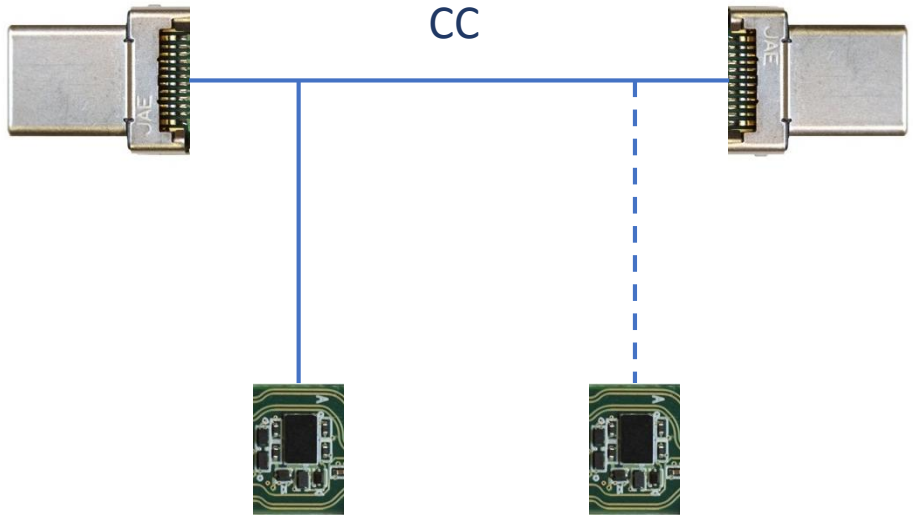
6.4.4 Vendor Defined Message

The ***Vendor_Defined*** Message (VDM) is provided to allow vendors to exchange information outside of that defined by this specification.

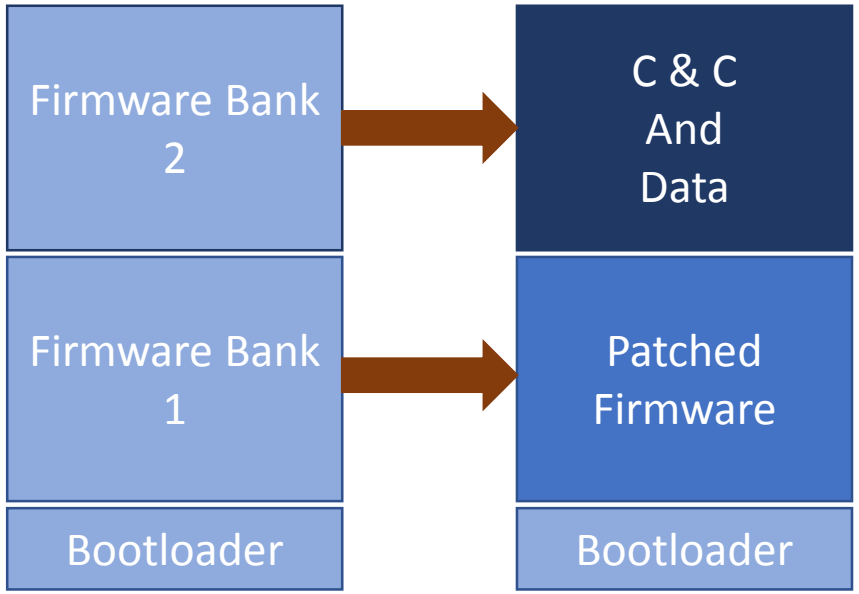
Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Example attack vectors

Evil Cable



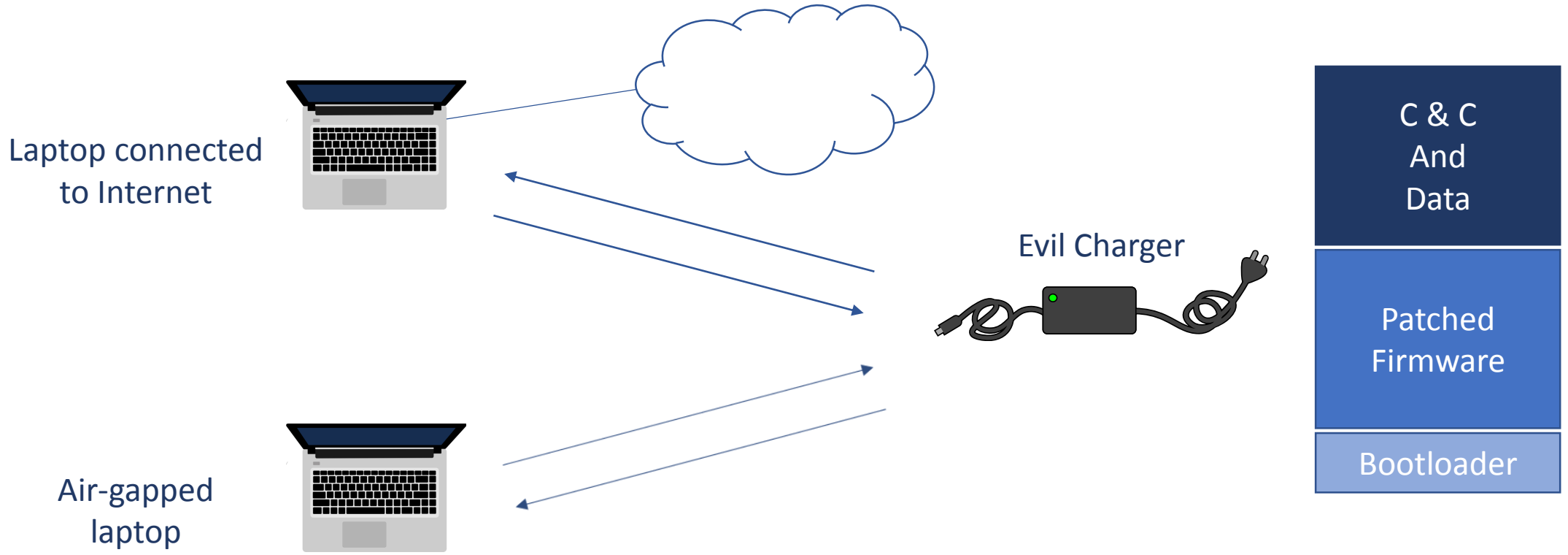
OS fingerprinting?



Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Example attack vectors

Evil Cable → Evil Charger

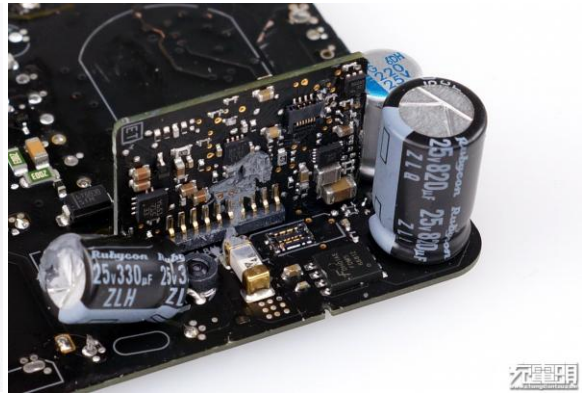


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Example attack vectors

Evil Cable | Evil Charger

http://www.chongdiantou.com

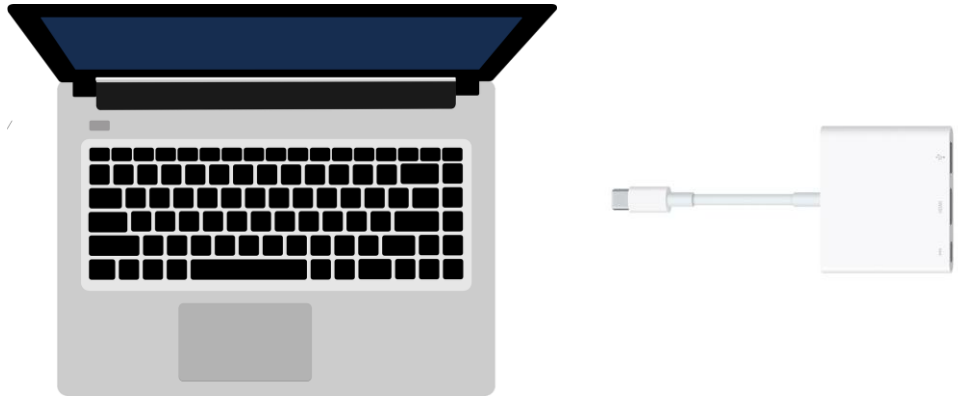


Nemanja Nikodijevic <nemanja@micropsi-industries.com>

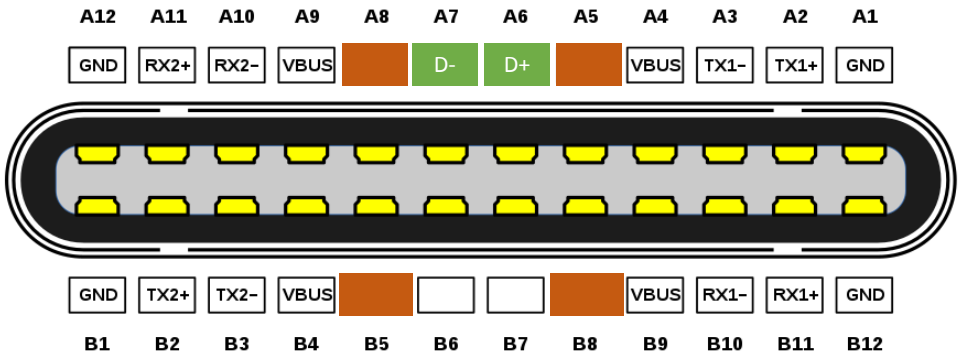
Example attack vectors

Evil Cable → Evil Charger → Evil Dongle

BadUSB scenario on an HDMI dongle



SBU1 CC



VCONN SBU2

WorseUSB

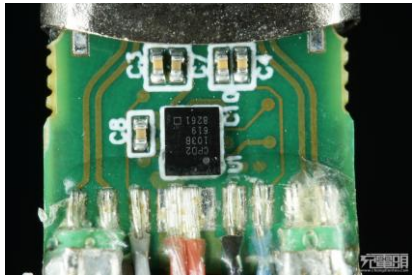
BALCCON2K17
U CNT CTRL ME

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

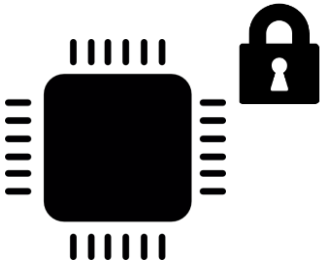
Countermeasures?

Superglue in a USB port?

Disabling firmware upgrade?



Firmware signing?



USB Type-C Authentication Specification

Table 2-1: Summary of Cryptographic Methods

Method	Use
X509v3, ***DER*** encoding	Certificate format
ECDSA using the ***NIST P256, secp256r1*** curve, uncompressed point format	Digital signing of Certificates and Authentication Messages
SHA256	Hash algorithm

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Bridging the air-gap: Takeaways

- USB is the most frequent air-gap attack vector
- USB-C introduces new methods for bridging the air-gap
- Proposed countermeasures are not yet widely implemented

Nemanja Nikodijevic <nemanja@micropsi-industries.com>

Thanks for your attention!

Questions?

Nemanja Nikodijevic <nemanja@micropsi-industries.com>