Industrial Radio Controllers

Safety, Security, Vulnerability

Jiří Gogela, R&D Manager
Trend Micro EMEA, Ltd.

Research team

- Trend Micro FTR (Forward looking Threat research)
  - M.Balduzzi, J. Andersson, S. Hilt, P. Lin, F. Maggi, U. Akira, and R. Vosseler

Responsible disclosure

- ZDI contacts with vendors via email / web-forms
- 5 business days? ZDI contacts with vendors by phone / intermediary
- 15 business days? Public advisory
- 120 days Security patches and mitigations
- Extensions Depends
- Transparency Enforced

- Mobile / IoT / IIoT needs more time to deploy patches
- Certification is necessary in some sectors*
- Collaboration >> lawsuits
- Win-win

Industrial controllers

Industrial controllers

Typical use cases for radio controllers

Typical use cases for radio controllers

Typical use cases for radio controllers

Vendors

JP Circuit Design

TW SAGA + Telecrane

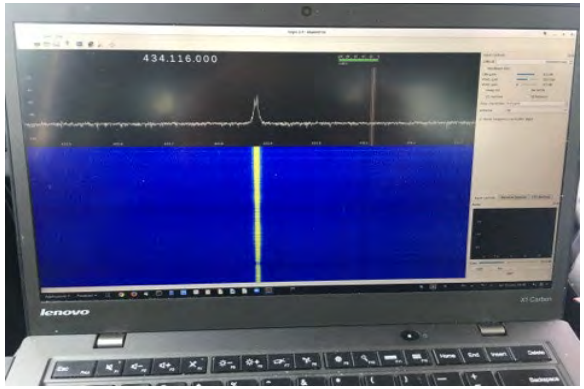
TW Juuko IT

IT ELCA

IT Autec

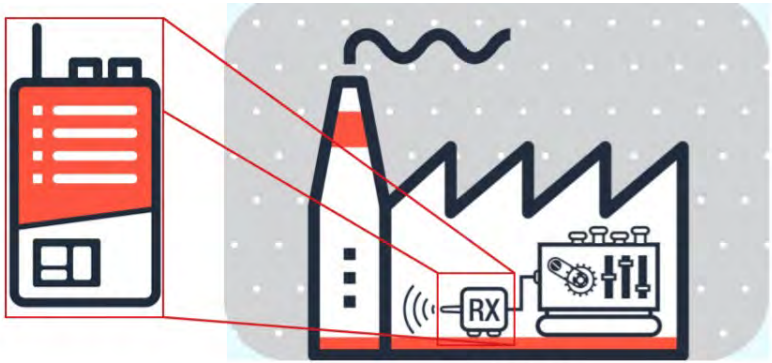
DE Hetronic International

Research on site…

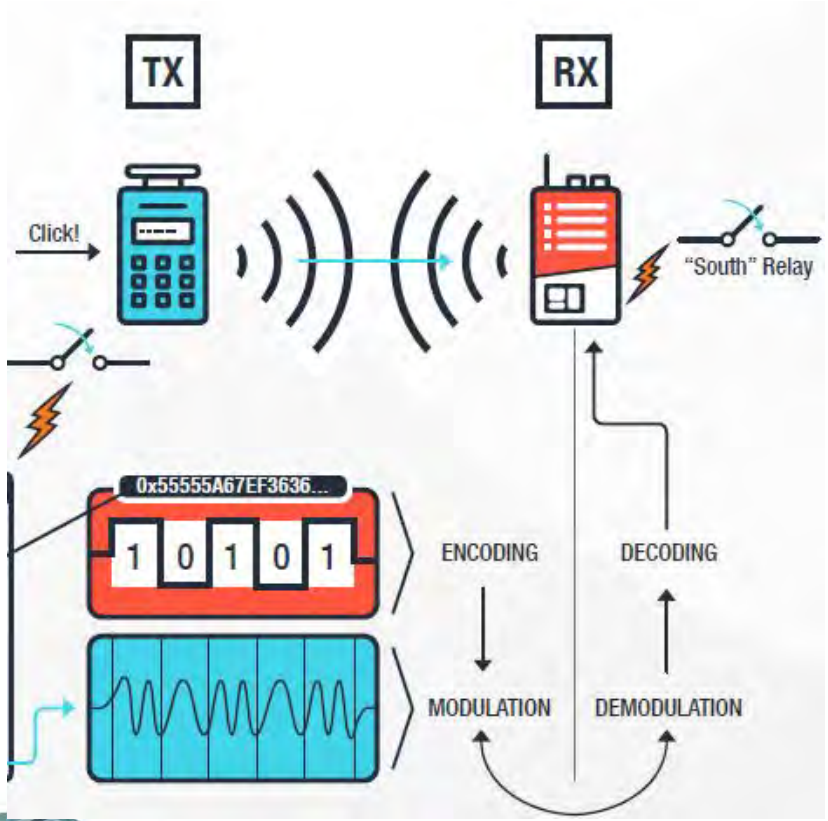


TREND MICRO™

How does it work?

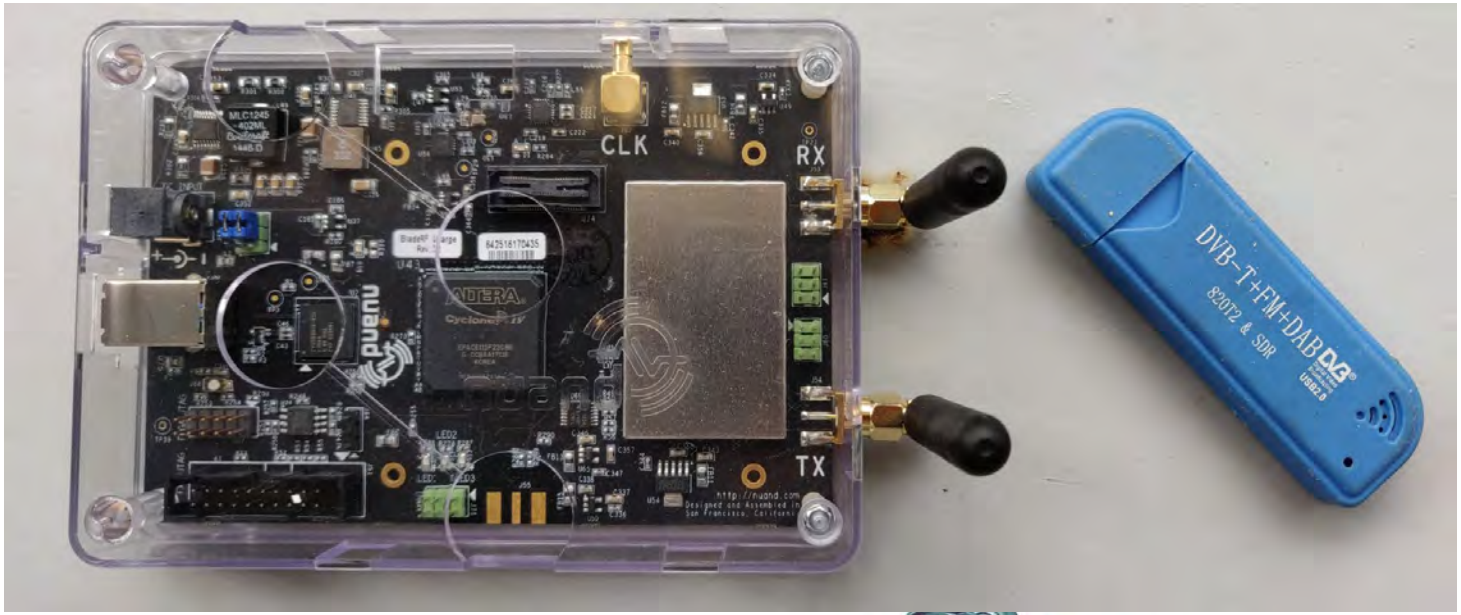


More in detail



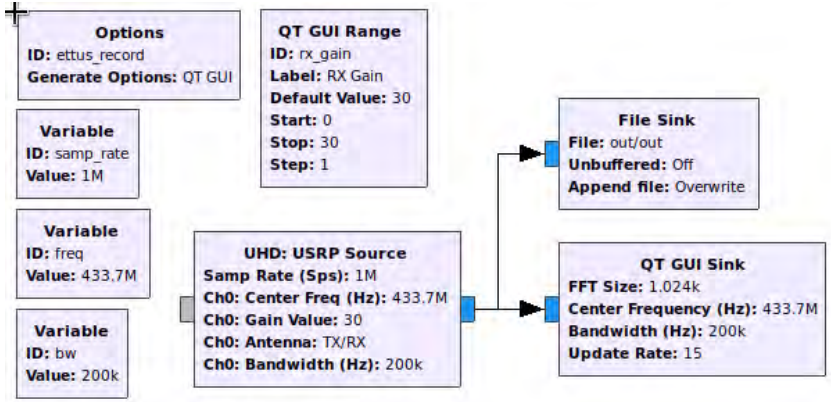
How to hack it?

- SDR (software defined radio)

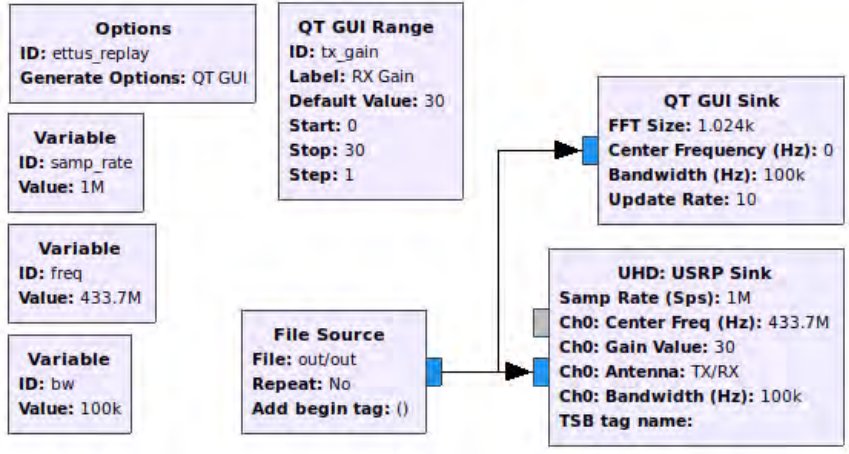


How to hack it?

- GNU Radio Companion

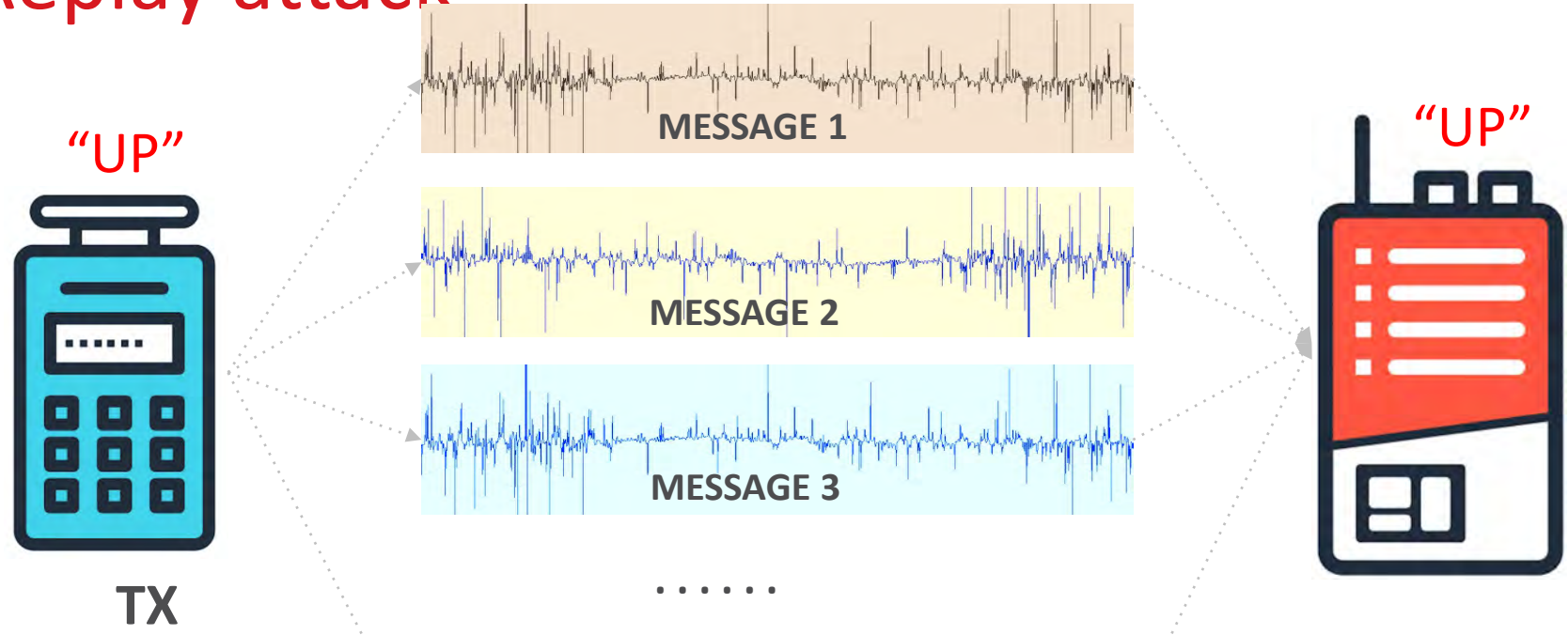


RECORD



REPLY

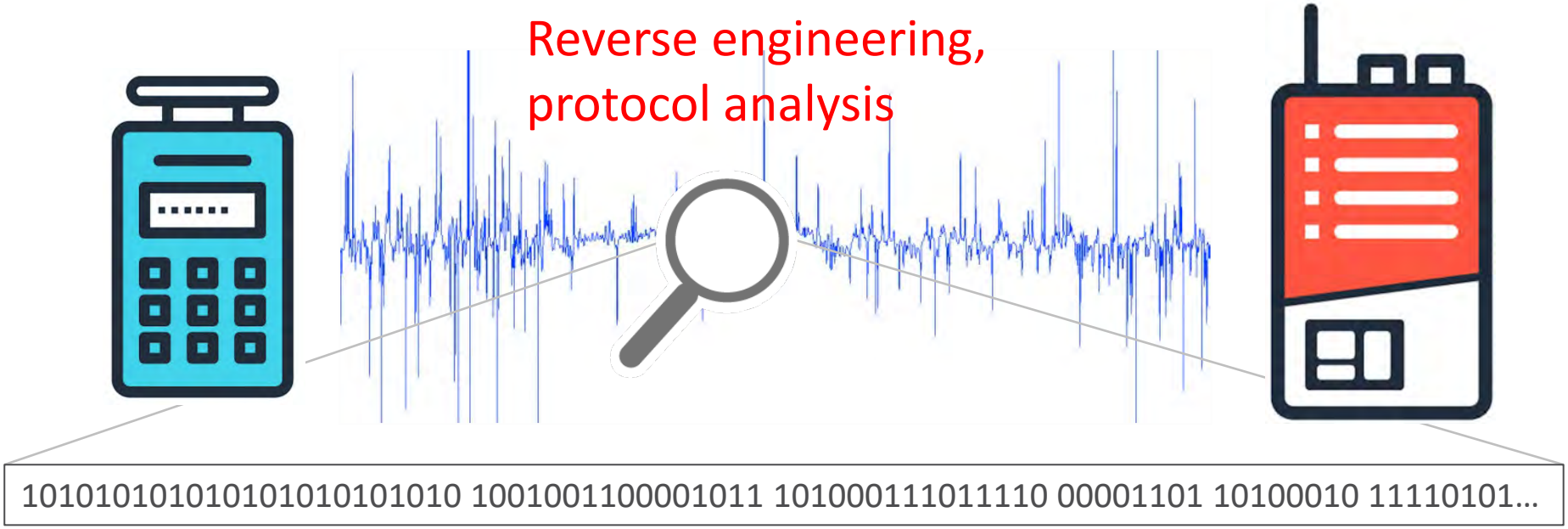
Replay attack



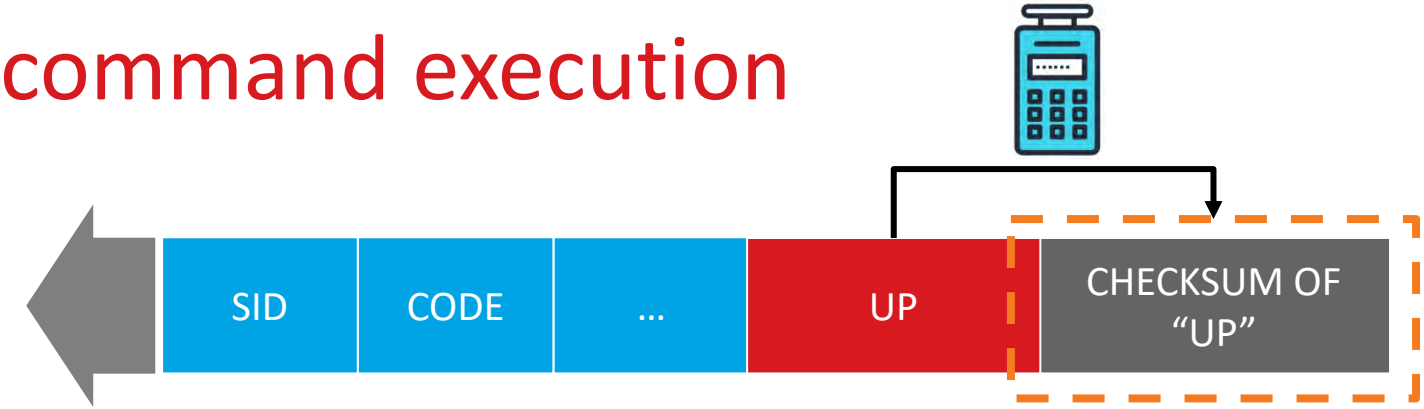
ATTACKS		Vendors	Difficulty	Cost
1: Record & Replay		ALL		$$$$

TREND MICRO

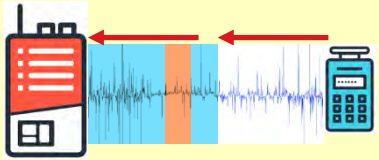
Arbitrary command execution



Arbitrary command execution

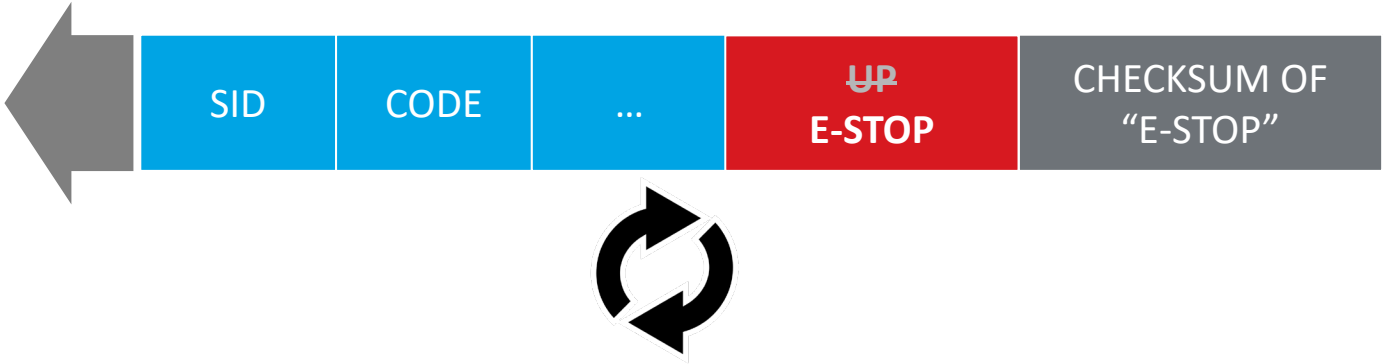


E-Stop Button

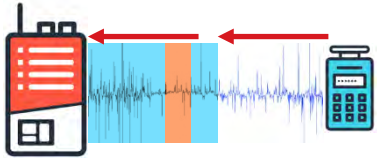
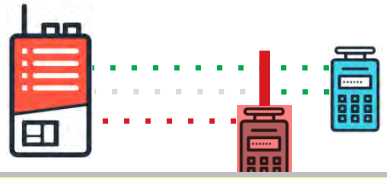
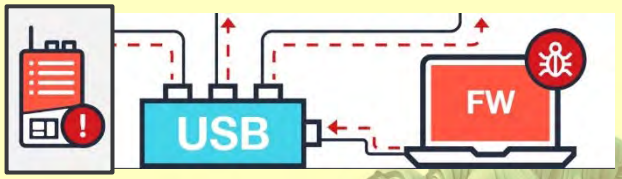
ATTACKS		VENDORS	DIFFICULTY	COST
1: Record & Replay		ALL		$$$$
2: Command Injection		ALL		$$$$

TREND MICRO

Arbitrary command execution



PRODUCTION ‘DoS’!

ATTACKS		VENDORS	DIFFICOLTY	COST
1: Record & Replay		ALL		$$$$
2: Command Injection		ALL		$$$$
3: E-Stop Abuse		ALL		$$$$
4: Malicious Re-pairing		PART		$$$$
5: Malicious Re-programming		PART		$$$$

TREND MICRO

So the attacker needs to be on site in person, right?

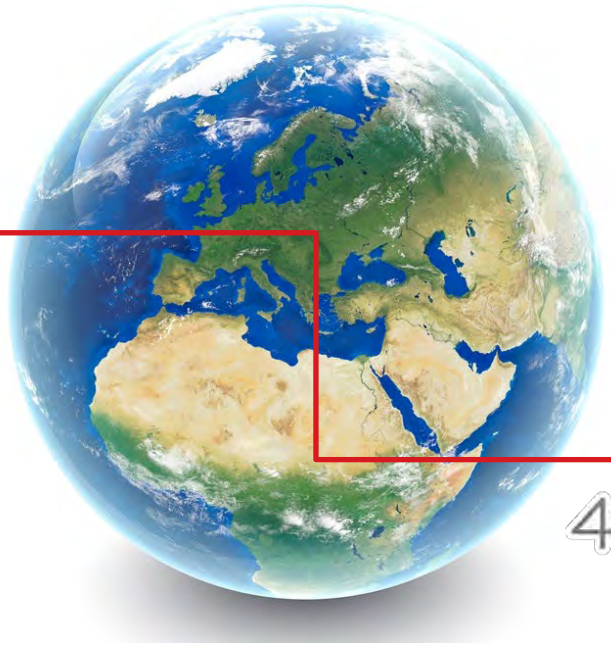
- No, not really…

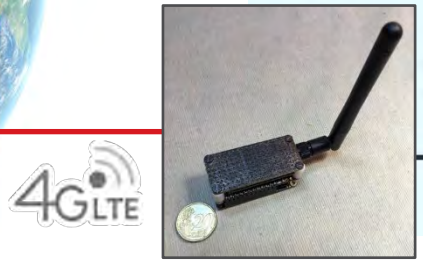
Remote, stealthy,…

TARGET

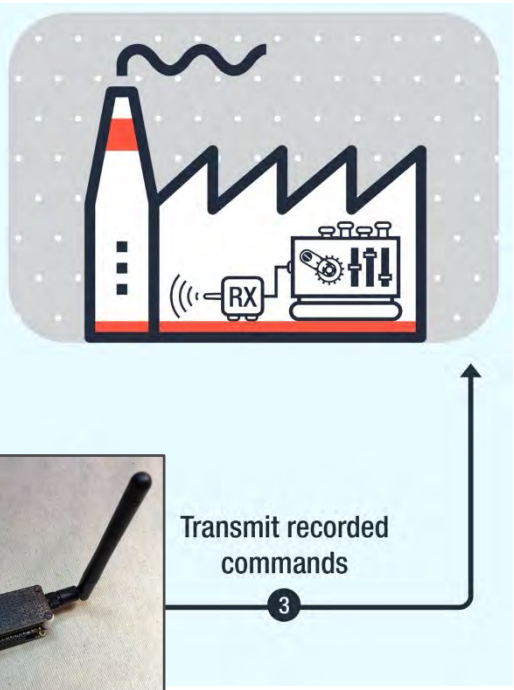
RFQuack

REMOTE ATTACKER





4G LTE



LOCAL BRIDGE

$40

TREND MICRO

Vendor actions

Vendor	CVE-ID	Status
Circuit Design	ZDI-CAN-6185 (replay attack)	Closed (No fix)
SAGA	CVE-2018-17903 (replay attack / command forgery) CVE-2018-20783 (malicious pairing) CVE-2018-17923 (malicious firmware upgrade)	Patch Released Patch Released Patch Released
Telecrane	CVE-2018-17935 (replay attack)	Patch Released
Juuko	ZDI-18-1336 (replay attack) ZDI-18-1362 (command forgery)	0day (No response) 0day (No response)
ELCA	CVE-2018-18851 (replay attack)	Closed (EOL)
Autec	ZDI-CAN-6183 (replay attack)	Closed (No fix)
Hetronic	CVE-2018-19023 (replay attack)	Patch Released

Conclusions

- Patterns of Vulnerabilities
  - No rolling-code
  - Weak or no encryption at all
  - Lack of software / firmware protection
- Need for security programs / awareness in the field of IIoT

TREND MICRO™

THE ART OF CYBERSECURITY

Threats detected and blocked globally by Trend Micro in 2018. **Created with real data by artist Daniel Beauchamp.**