Kyberfyzické útoky v případech

Rudolf Marek
SYSGO s.r.o.*

* Pracuju tady, ale obsah přednášky je slavným „krokem stranou“

Osnova přednášky

- Kyberfyzické útoky
  - Historický přehled
  - Současnost
- Útok na německé „HDO“
- Co když výrobce zařízení „zlobí“ ?

O mně...

- Pracuji ve společnosti SYSGO s.r.o. [9]
  - R&D centrum v Praze
  - PikeOS – separační / virtualizační realtime mikrokernel / operační systém [9]
  - x86 expert, na starosti x86 architekturu
- Opensource
  - Linuxové Kernel Drivery pro HWMON a I2C
  - Opensource BIOS - coreboot
- Hacking
  - Pro radost z poznání, hodně low level / firmware
  - AMD procesory
    - SMU AMD hack [0]
    - Nahlášeny různé security problémy + jeden v Linuxu
  - Intel procesory
    - CVE-2018-3646 [19]
    - Zkoumám mikrokód / UROM Pentia II, III, M a rodiny procesorů core2 duo

Kyberfyzické útoky
Historický přehled

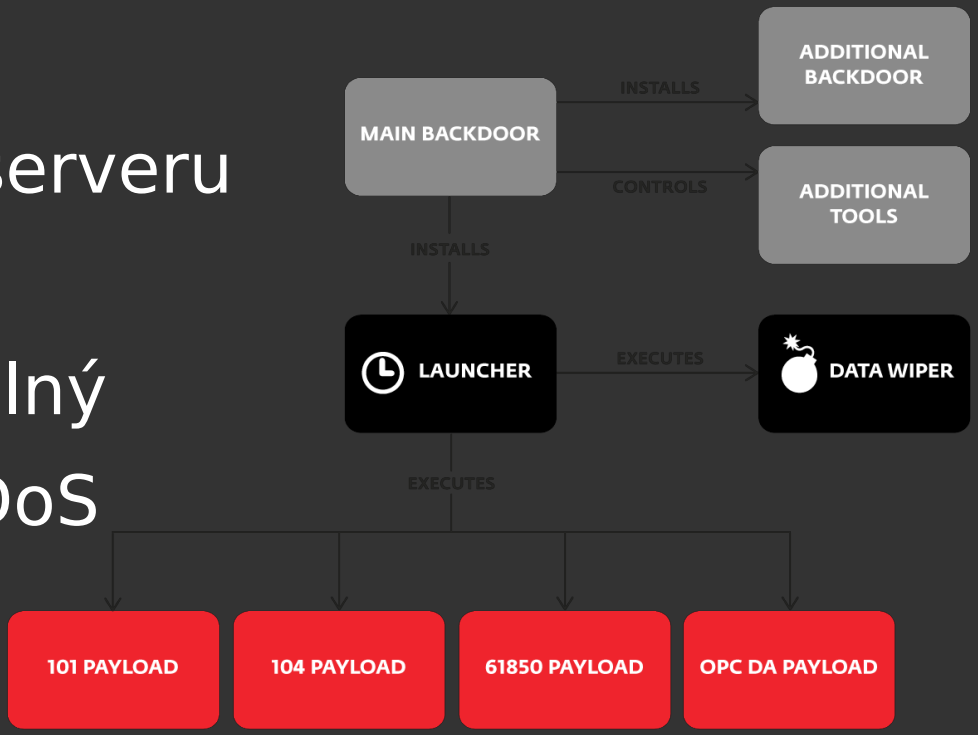
- 2006++ Stuxnet
  - Iránský jaderný program, Windows + Siemens PLC
- 2014
  - Německá slévárna [13]
    - Phishing attack & sofistikovaný útočník dle BSI
  - Industroyer [11]
    - Kyberútok na ukrajinskou energetickou infrastrukturu
- 2015 Konference Black Hat
  - Internet Facing PLCs A New Back Orifice [1]
  - Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion [2]
  - Switches Get Stitches: Episode 3 [3]

Kyberfyzické útoky
Historický přehled

- Konference: Chaos Communication Congress
  - The Great Train Cyber Robbery [4]
  - Unpatchable - Living with a vulnerable implanted device [5]
  - (In)Security of Embedded Devices' Firmware – Fast and Furious at Large Scale [6]
- Remote Exploitation of an Unaltered Passenger Vehicle [7]

Industroyer [11]

- Spearphishing
  - VPN přístup do vnitřní sítě ukraden
- Malware
  - Připojuje se k C&C serveru
  - Sofistikovaný
  - Velmi konfigurovatelný
  - Paleta „payloadů“ DoS



Internet Facing PLCs A New Back Orifice [1]

Internet-Facing PLCs - A New Back Orifice

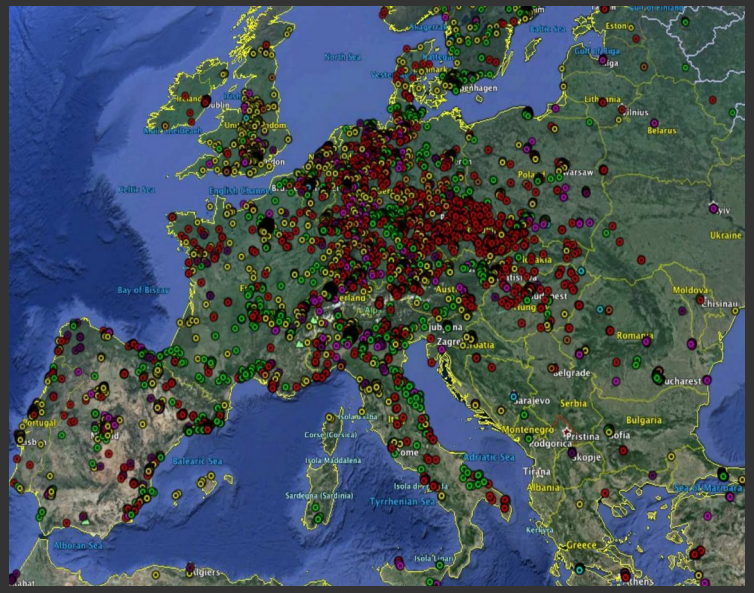
Johannes Klick, Stephan Lau, Daniel Marzin,
Jan-Ole Malchow, Volker Roth

<firstname>.<lastname>@scadacs.org

AG Secure Identity
Department of Mathematics and Computer Science
Freie Universität Berlin
www.scadacs.org

SCADACS

1 / 100



Kyberfyzické útoky na chemický provoz [2]

Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion

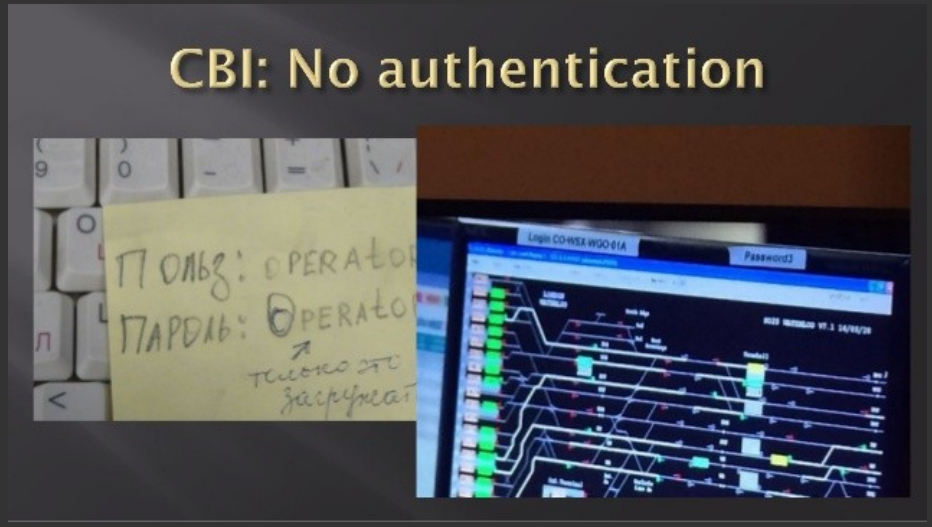
Marina Krotofil

Black Hat, Las Vegas, USA
06.08.2015

Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion [2]

- Velmi podrobná přednáška
- **Motivace** - peníze
- **Přístup** – přes internet pomocí známých chyb...
- **Objevy** – špionáž, zvědavost
- **Převzetí řízení**
  - Sabotáž, ekonomické škody
  - Jak ovlivnit chemický proces a “nebýt viděn”

The Great Train Cyber Robbery [4]

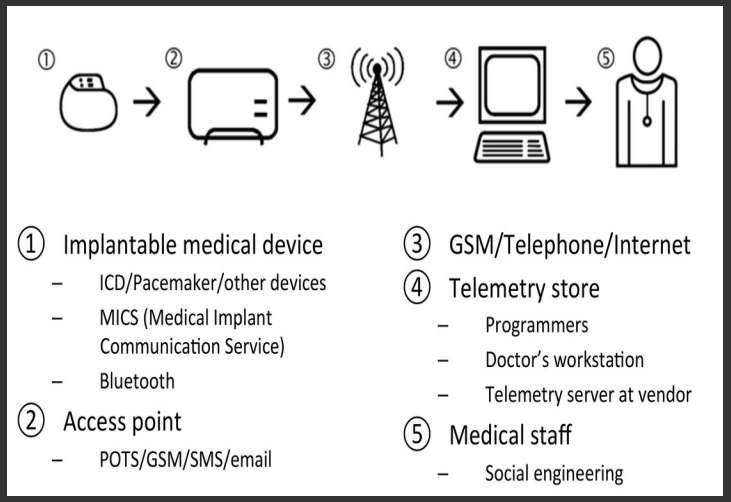


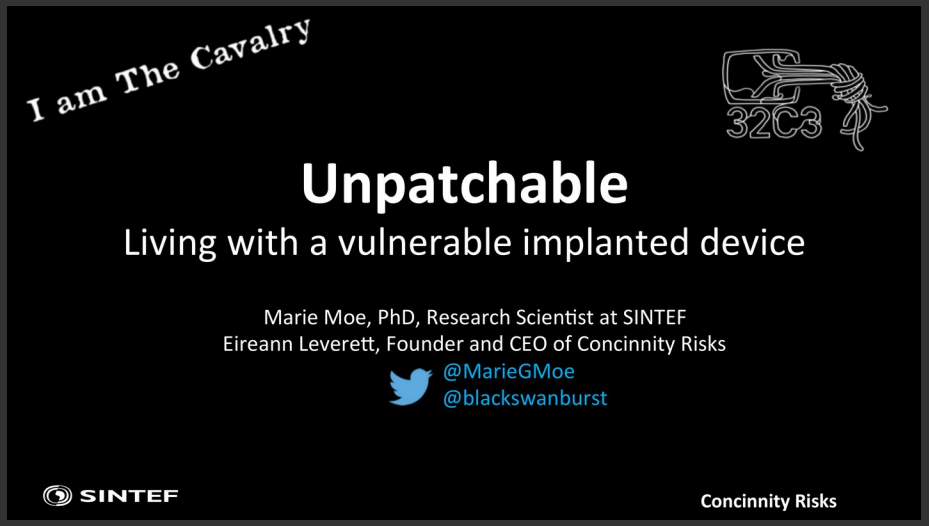
The Great Train Cyber Robbery [4]

- Podobné problémy:
  - Vše propojeno (I na Internet)
  - Možnost kyber-fyzických útoků
  - Privátní klíče ve firmwaru (i pro vzdálený přístup)
  - GSM-R
    - Zdá se že útoky z GSM nepoučily GSM-R
  - Útoky na modem → útok na zařízení
- Odkazy na starší přednášky

Zranitelní lidé [5]

- Unpatchable - Living with a vulnerable implanted device
  - Život se srdečním implantátem co má bezpečnostní díry
  - Člověk nedobrovolnou součástí IoT

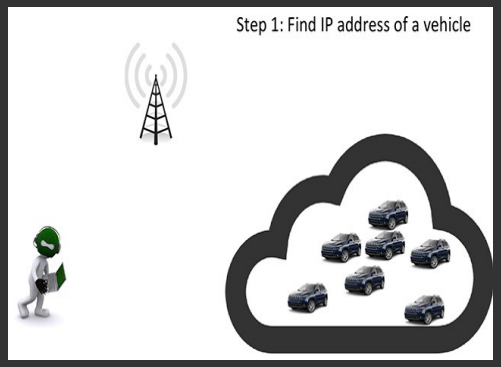


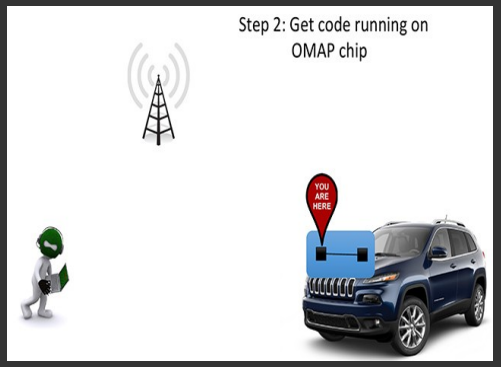


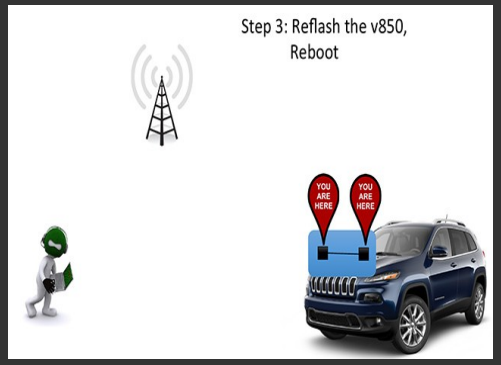
Remote Exploitation of an Unaltered Passenger Vehicle [7]

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)







Remote Exploitation of an Unaltered Passenger Vehicle [7]

- 3 letý výzkum
- vzdálený útok na jedoucí auto (v USA)
- funguje bez modifikace auta
- útok na řízení a brzdy
- nedostatečná separace systémů

Mezihra:
Poučení z „historie“?

- Stále stejné problémy
  - Vše propojené a kritické
  - Hraniční zařízení umožňující průnik
  - Pohyb ve vnitřních sítích
  - Útoky i v rámci jednoho zařízení – nedostatečná separace
  - Bezpečnostní díry, zařízení bez updates
- Zlepšilo se něco?
  - Cyber Resilience Act, CRA
  - Co výrobci a backdoory?

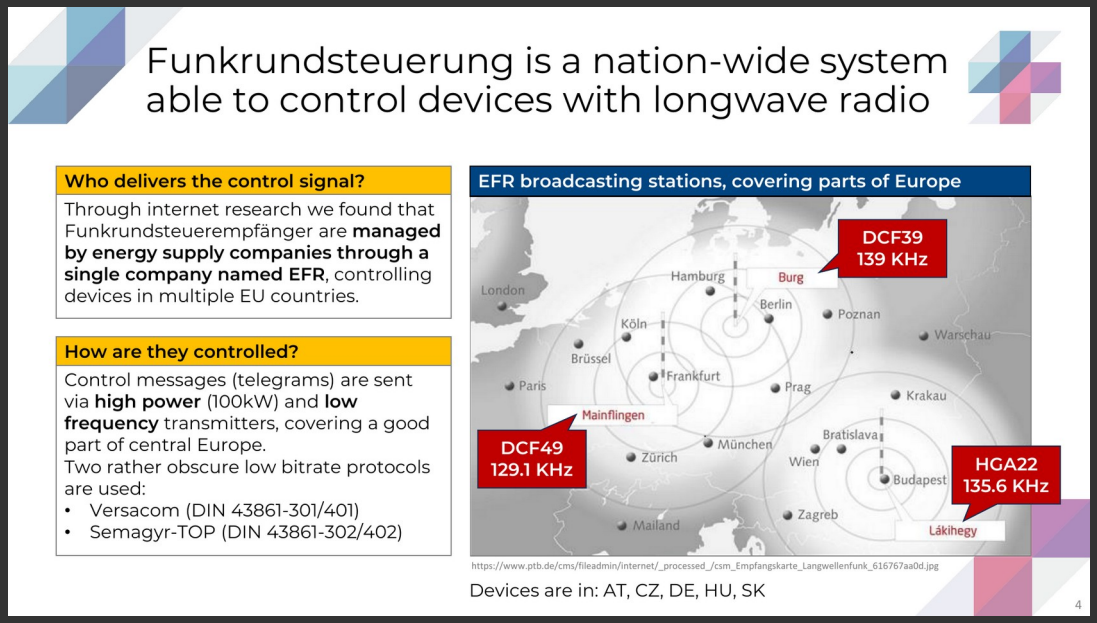
Mezihra: Budoucnost energetiky ?

- 2022: Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on Offshore Wind Farms [18]
- 2025: Simulation of multi-stage attack and defense mechanisms in smart grids [17]
- Jak je na tom z bezpečností české HDO?
- Mají už malé FVE:
  - dost velký výkon
  - Zranitelnost co umožňuje odpojení / řízení přes Internet?

Kyberfyzické útoky Současnost

- 2022
  - Industroyer2: Industroyer reloaded [8]
  - Satellite cyber attack paralyzes 11GW of German wind turbines [12]
- 2023 - Konference: Chaos Communication Congress
  - „Hujer ví o lokomotivě“ co se umí rozbít když výrobce „chce“ [10]
- 2024 - Konference: Chaos Communication Congress
  - BlinkenCity: Radio-Controlling Street Lamps and Power Plants [14]
  - Lokomotiva co se umí rozbít když výrobce „chce“ reloaded [15]
- 2025
  - Trolejbusy v Norsku jdou nejspíš vzdáleně „vypnout“ [16]

BlinkenCity: Radio-Controlling Street Lamps and Power Plants



BlinkenCity: Radio-Controlling Street Lamps and Power Plants

An attacker controlling power sources and loads could cause power grid instabilities

Device adoption growth

Meaningful power at stake

EFR lists several GigaWatts of both controlled power loads and power sources.
Example figures from 2009:

Customer	MW Controlled	Comment
e.on edis	2,100 MW	Wind Generation
e.on Avacon	600 MW	Wind Generation
WEMAG AG	25 MW	Wind Generation
energiequelle	230 MW	Wind Generation
e.on Bayern	2,500 MW	Heating Systems
	20 MW	Street Lighting
All Companies	500,000 households	Tariff Switching
enviaM	900 MW	Wind Generation, Solar & Biogas systems

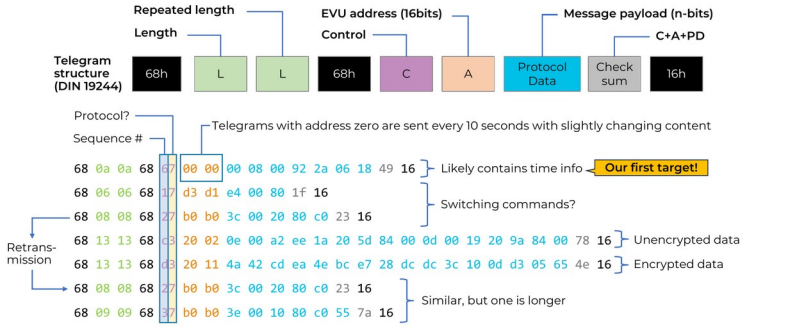
Blackout risks

Major blackouts happened in the US, and there are reports of growing instabilities in the EU grid

Following the current worldwide political tensions and cyber attack strategies, **how likely can this ecosystem be abused to cause a power outage?**

https://www.sigidwiki.com/images/a/ab/EFR_Metering_Billing_CIS_America.pdf
https://www.vox.com/climate/23893057/power-electricity-grid-heat-wave-record-blackout-outage-climate

Telegrams share a common header & trailer, but inner contents follow different standards



Publicly available PDFs disclose the relation between address bits and power plants

Searching the internet we found documents that **describe the device addressing and use cases**

Classification of power plants by type and size

Nomenklatur

Eindeutige Kennzeichnung der Parametrierung: X_Y_Z (z. B. 2_III_45134)
X Energieart (im Beispiel: Energieart 2 Deponiegas)
Y Leistungsklasse (im Beispiel: Leistungsklasse III <500kW)
Z Postleitzahl (im Beispiel: Postleitzahl 45134 Essen)

Leistungsklassengrenzen/Energieart
Alle Angaben in kW

Leistungs-klasse	Energieart 1 Windenergie	2 Deponiegas Grubengas Klärgas Biomasse	3 Wasserkraft	4 Solare Strahlungs-energie (PV)	5 BHKW-/KW-	6 Geothermie
I	≥ 10.000	≥ 2.000	≥ 1.000	≥ 500	≥ 1.000	≥ 5.000
II	≥ 1.000 und < 10.000	≥ 500 und < 2.000	≥ 500 und < 1.000	≥ 100 und < 500	≥ 100 und < 1.000	≥ 500 und < 5.000
III	< 1.000	< 500	< 500	< 100	< 100	< 500

Mapping of address bits to relay#, device type & location

Adressierungsebene A
Unterscheidung der Energiearten:
A1 Windenergie
A2 Deponiegas, Grubengas, Klärgas, Biomasse
A3 Wasserkraft
A4 Solare Strahlungsenergie (PV)

Adressierungsebene B
Unterscheidung der Relais und Leistungsklassen:
B1 Relais 1, Leistungsklasse I
B2 Relais 2, Leistungsklasse I
B3 Relais 3, Leistungsklasse I
B4 Relais 4, Leistungsklasse I
B9 Relais 1, Leistungsklasse II
B10 Relais 2, Leistungsklasse II
B11 Relais 3, Leistungsklasse II
B12 Relais 4, Leistungsklasse II
B17 Relais 1, Leistungsklasse III
B18 Relais 2, Leistungsklasse III
B19 Relais 3, Leistungsklasse III
B20 Relais 4, Leistungsklasse III

Adressierungsebene C + D

C \ D	1	2	3	4	5	6	7	8
1	45897	45881	45883	45884	45886	45888	45889	45891	45892	45894	45896	45897	45899
2	46236	46238	46240	46242	46244								
3	45964	45966	45968										

German postcode

EVU values for different zones and energy providers

Anwenderadresse
Netzgebiet Nord - BOB1 Region A und B
Netzgebiet Süd - BFB1 Region A und B
Netzgebiet Süd - BFB2 Region C und D

Anwenderadresse ELE
BFB9

Association between relay# and power reduction

100% keine Reduzierung (K1)
60% Reduzierung auf maximal 60% der Leistung (K2)
30% Reduzierung auf maximal 30% der Leistung (K3)
0% Reduzierung auf 0% der Leistung – keine Einspeisung möglich (K4)

This attack can be used to disconnect real photovoltaic systems from the grid

BlinkenCity: Radio-Controlling Street Lamps and Power Plants

Three conditions need to be met to cause grid instabilities

Now, radio ripple control telegrams have been reversed: **is that sufficient to cause a blackout?**

We are not experts, but we imagine that at least these 3 conditions have to be met:

A large enough amount of power has to be involved +

- How much power is controlled via radio ripple receivers?
- How much power would need to be taken away to cause trouble?

The radio control signal has to be overcome/hijacked +

Two options:

- Overpowering EFR signal with antennas in multiple areas. This seems not an easy task, but we will do a feasibility study on it
- Gain control of EFR's transmitters, either by hacking their IT infrastructure, or by physically breaching into the tower sites

Optimal timing has to be chosen

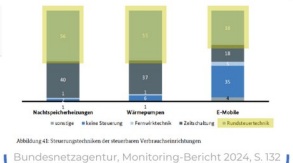
Some elements can affect the damage produced by the attack:

- How utilized are the controlled plants?
- Is there any real-time information about the current grid status?

38

Our **estimate** is that **40 GWp of supply** and **20 GW of load** are controlled with FREs

We collected and correlated information from various sources to **estimate FRE-controllable power**



Bundesnetzagentur, Monitoring-Bericht 2024, S. 132

Power generation | **Energy loads**

Estimate!	Estimate!	Estimate!
Solar (<30kW): 4 GWp Solar (30-100kW): 10 GWp Solar (>100kW): 6 GWp (?)	Wind: 20 GWp (?) (extrapolating only the 5 wind production companies that were mentioned with numbers by EFR, unconfirmed if FREs are still in use)	Night storage heating: 10 GW Heat pumps: 8 GW Wallboxes: 2 GW

The overall controlled load is **hard to estimate** exactly, **but** it is a **significant** portion.
For comparison, Germany has ~70 GW peak energy usage and 250 GW of installed production.
(This estimate does not consider energy types other than solar/wind and countries other than Germany)

43

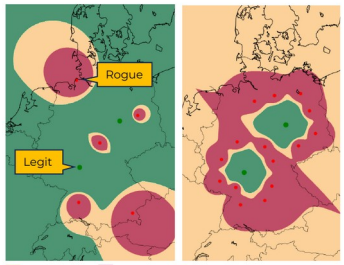
Multiple deployment strategies can be leverag to create a network of decentralized transmitt

How to overpower EFR transmitters?

Our calculations (together with a longwave expert) suggest that with:

- **550m** antenna
- **10kW** radio amplifier (~500€)
- **10kWp** power station (~100€/day)
- **300km** distance to EFR tower

the legitimate signal can be sufficiently **overpowered within 70-240 km**



Antenna mount option		Length	Price (€)	
High floor	A tall building from which one can drop a cable	50-150m	100	Fixed location
Kite	Kite models designed for aerial photography (KAP)	**Full size (550m)**	500	Requires wind
Balloon	Tethered weather balloons filled up with helium	**Full size (550m)**	1K	Helium refill, low wind
Drone	Heavy duty commercial or custom drones	**Full size (550m)**	3-30K	Short operational time
Trailer with mast	Civil or military trailers with a telescopic mast	40m	10K (used) 200K (new) 60/day	Slow to move, availability

45

BlinkenCity: Radio-Controlling Street Lamps and Power Plants

Takeaways

- **Cities** with radio controllable street lights can be turned **into cool art installations** (if allowed)
- Radio ripple receivers can be **locally abused for fraud** (tariff switching, no power limitations)
- Compromising receivers at scale could result in **grid instabilities and potentially blackouts**
- **iMSys rollout should speed up** to replace radio ripple control devices in large power plants
- In general, all **legacy systems need scrutiny** by security experts, so **go and find the next one!**

Our wish, if you're on the receiving side: **Collaborate with good-faith researchers** instead of threatening to sue them

60

Breaking “DRM” in Polish Trains [10][15]

Recap: the story so far

- Trains have to be serviced
- KD and their 11x 45WE
- Warranty period ends
- Public tender for P3.2 service
- SPS Inowrocław
- Something is not right

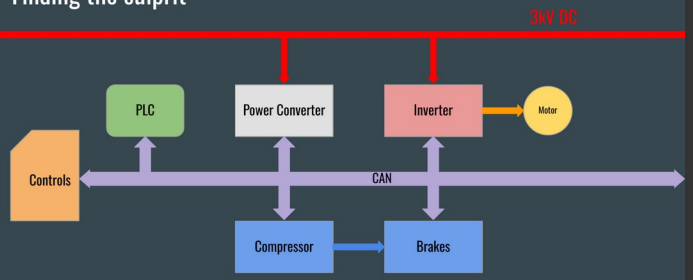
Hujer

Recap: the locking mechanism

- Inactivity detection
- Serial number checks
- Geolocation lock
- Date checks
- Secret key combinations to unlock the trains

Breaking “DRM” in Polish Trains [10][15]

Finding the culprit



CAN all the way down

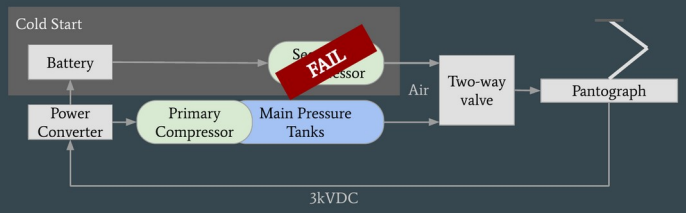
All communication performed over CAN/CANopen.

What’s the difference between a working and locked up train?

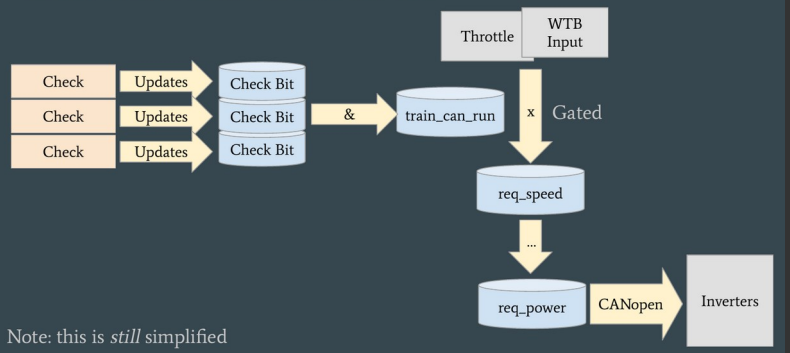
Train	CANopen traffic
45WE-022 *Working*	ID: `0x0212` Payload: `01 1f 0b 0b 0b 0b 52 00` Sent by CPU on CAN1
45WE-023 *Locked up*	ID: `0x0212` Payload: `01 0f 00 00 00 00 52 00` Sent by CPU on CAN1

Lockup mechanisms: ‘Compressor failure’

Secondary kind. Found only in a single Polregio train.



Lockup mechanisms: Force power to 0



Note: this is *still* simplified

Breaking “DRM” in Polish Trains [10][15]

Lockup triggers: Lack of movement + geofencing

```
check1 = 53.13845 < var1 && var1 < 53.13882 && 17.99011 < var2 && var2 < 17.99837;
check2 = 53.14453 < var1 && var1 < 53.14828 && 18.00428 < var2 && var2 < 18.00555;
check3 = 52.17048 < var1 && var1 < 52.17736 && 21.53480 < var2 && var2 < 21.54437;
check4 = 49.60336 < var1 && var1 < 49.60686 && 20.70073 < var2 && var2 < 20.70840
       && (var3 & 1);
check5 = 53.10244 < var1 && var1 < 53.10406 && 18.07817 < var2 && var2 < 18.08243;
check6 = 50.12608 < var1 && var1 < 50.12830 && 19.38411 < var2 && var2 < 19.38872;
check7 = 52.77292 < var1 && var1 < 52.77551 && 18.22117 < var2 && var2 < 18.22724;
```

Code sample: Compressor failure

Polregio ED78-010 / 31WE-015
SHA256: 0411b9af468331e0593674b03acd1a06ede2aef90f553704405da1806d231638

```
[...]
G_181_get_current_time(cur_time);
sr->SET1 = 21 <= cur_time->day
       && 11 <= cur_time->month
       && 21 <= cur_time->year_lo;
sr->RESET = ton_reset->Q;
SR(sr);
me->is_date_after = sr->Q1;
[...]
```

```
[...]
r_trig_odo->CLK = 1000000 < reg_odometer_km;
R_TRIG(r_trig_odo);
trigger_lock = r_trig_odo->Q
            || (car_?_udpcan_input.lock_train & 1)
            || me->is_date_after;
rs_lock->SET = trigger_lock;
RS(rs_lock);
me->is_train_locked = rs_lock->Q1;
// [...]
rs_lock2->SET = trigger_lock;
rs_lock2->RESET1 = ton_reset->Q;
RS(rs_lock2);
NVRAM_lock_enabled = rs_lock2->Q1;
[...]
```


onet WIADOMOŚCI

SZUKAJ

WOJNA W UKRAINIE | KRAJ | ŚWIAT | PREMIUM | TYLKO W ONECIE | HISTORIA | POGODA

WIADOMOŚCI › KRAJ

Jesteś w strefie premium — Korzystaj ze wszystkich tytułów w wyjątkowej ofercie. KUP TUTAJ

Nowe fakty o skandalu na kolei. Pociąg Newagu znowu stanął, bo nadszedł 21 grudnia

ŁUKASZ CIEŚLA | TOMASZ MATEUSIAK | 21 grudnia 2023, 16:19

FACEBOOK | X | E-MAIL | KOPIUJ LINK

Specjaliści od cyberbezpieczeństwa zarzucili spółce Newag, że celowo wprowadzała cyfrowe blokady w swoich pociągach, aby potem zarabiać na ich naprawach. Jedna z wprowadzonych blokad polegać miały na tym, że pociąg jeżdżący dla spółki Polregio w woj. lubuskim stawał 21 listopada i 21 grudnia. Jak dowiedział się Onet, pociąg rzeczywiście stanął w tych datach.

Odkazy

- [0] https://events.ccc.de/congress/2014/Fahrplan/events/6103.html https://app.media.ccc.de/v/31c3_-_6103_-_en_-_saal_2_-_201412272145_-_amd_x86_smu_firmware_analysis_-_rudolf_marek
- [1] https://www.blackhat.com/us-15/briefings.html#internet-facing-plcs-a-new-back-orifice
- [2] https://www.blackhat.com/us-15/briefings.html#rocking-the-pocket-book-hacking-chemical-plant-for-competition-and-extortion
- [3] https://www.blackhat.com/us-15/briefings.html#switches-get-stitches
- [4] http://scadastrangelove.blogspot.cz/2015/12/talk-on-32c3.html https://media.ccc.de/v/32c3-7490-the_great_train_cyber_robbery
- [5] https://events.ccc.de/congress/2015/Fahrplan/events/7273.html https://media.ccc.de/v/32c3-7273-unpatchable
- [6] https://events.ccc.de/congress/2015/Fahrplan/events/7252.html https://media.ccc.de/v/32c3-7252-in_security_of_embedded_devices_firmware_-_fast_and_furious_at_large_scale
- [7] http://illmatics.com/Remote%20Car%20Hacking.pdf
- [8] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
- [9] https://www.sysgo.com/products/pikeos-rtos-and-virtualization-concept/
- [10] https://fahrplan.events.ccc.de/congress/2023/fahrplan/system/event_attachments/attachments/000/004/431/original/Train_DRM_-_37C3-1.pdf https://media.ccc.de/v/37c3-12142-breaking_drm_in_polish_trains
- [11] https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf
- [12] https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/
- [13] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile
- [14] https://fahrplan.events.ccc.de/congress/2024/fahrplan/media/38c3/submissions/HSNZGR/resources/20241228-BlinkenCity-38c3_53qew19.pdf https://media.ccc.de/v/38c3-blinkencity-radio-controlling-street-lamps-and-power-plants
- [15] https://fahrplan.events.ccc.de/congress/2024/fahrplan/media/38c3/submissions/HTWLCG/resources/38C3_-_Weve_not_been_trained_for_this__life_after_the__l2nzRjV.pdf https://media.ccc.de/v/38c3-we-ve-not-been-trained-for-this-life-after-the-newag-drm-disclosure
- [16] https://ruter.no/en/ruter-with-extensive-security-testing-of-electric-buses
- [17] https://www.sciencedirect.com/science/article/pii/S1874548224000684
- [18] https://www.sciencedirect.com/science/article/pii/S0029801822012720
- [19] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

Otázky?

Řešení separace v systémech? → PikeOS

Děkuji za pozornost!

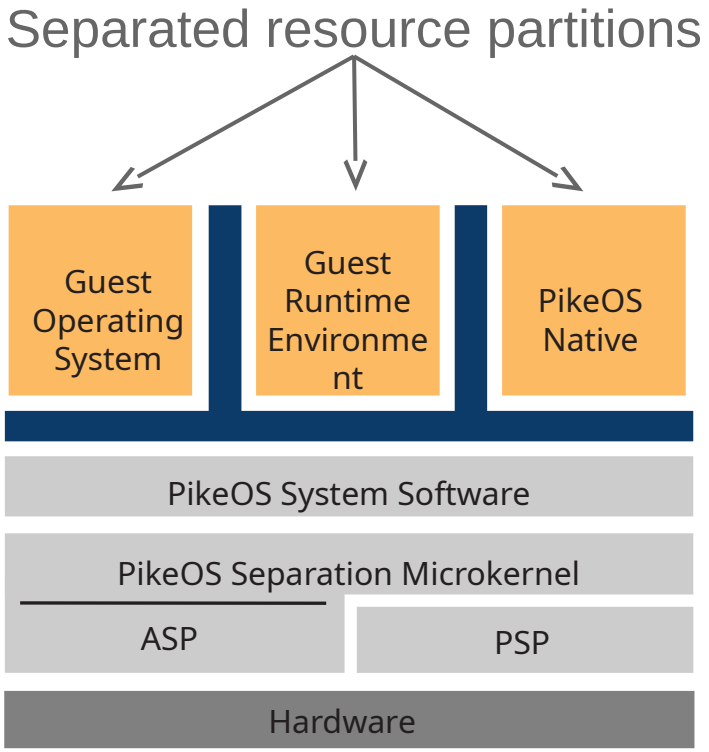
rudolf . marek @ sysgo.com

Separace Systémů s PikeOS

- PikeOS
  - vyvíjený firmou SYSGO
  - Real-time operační systém, hypervisor
  - prostorová i časová separace nezávislých kontejnerů
  - Ruzně kritický software současně
  - Mikrokernel
    - modulární, rozumná komplexita
    - zdrojový kód není velký
    - certifikovaný - DO-178B, IEC61508, EN50128
    - certifikovatelný - DO-178C, ISO26262, IEC62304, CC EAL 5/6

PikeOS

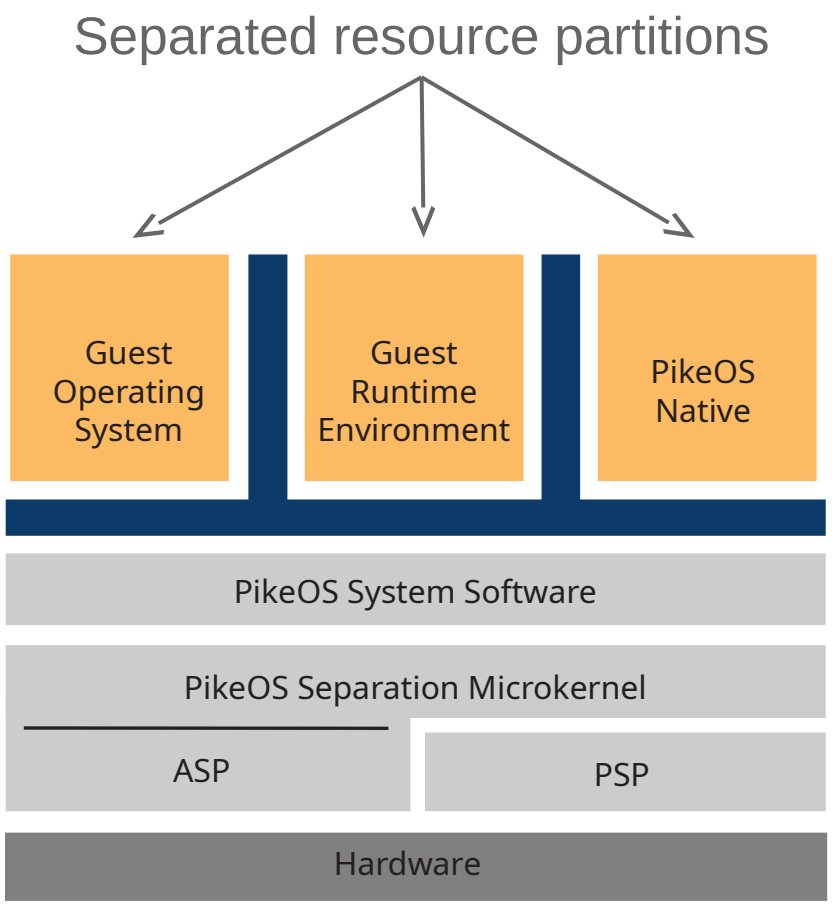
- **Operační systém**
  - **Hard real-time**
  - **Embedded / Mikro -**
  - **Preemptivní**
- **Partitioning / Separace**
  - Separované kontejnery (partitions)
  - Programy běží garantovaně nezávisle
  - jiné operační systémy mohou běžet v rámci partitions
  - Hlavní principy bezpečnosti
    - Možnost provozování různě kritických systému najednou
    - Certifikovaný / telný



PikeOS
RTOS and Hypervisor v jednom!

PikeOS - separace prostorová

- Statická alokace systémových zdrojů
- Aplikace mají garantován přístup ke zdrojům ve vlastní partition
- Aplikace nemohou používat zdroje jiných partition
- Nefunčnost jedné partition neovlivní další
- Ochrana paměti s použitím MMU
- Všechny partition běží odděleně jako uživatelské procesy



PikeOS - separace časová

- **Statická konfigurace toho co kdy a jak dlouho poběží**
- **Deterministic Hard Real-time**
- **Nejrychlejší doba odezvy**
  - Možné vlákno s nejvyšší prioritou
- **Nejlepší využití CPU**
  - Time Partition ‘0’
  - Vlákna s nejvyšší prioritou mohou být upřednostněna před jinou partition
  - Vlákna s nizkou prioritou moho běžet pokud ostatní partition nevytěžují celý processor