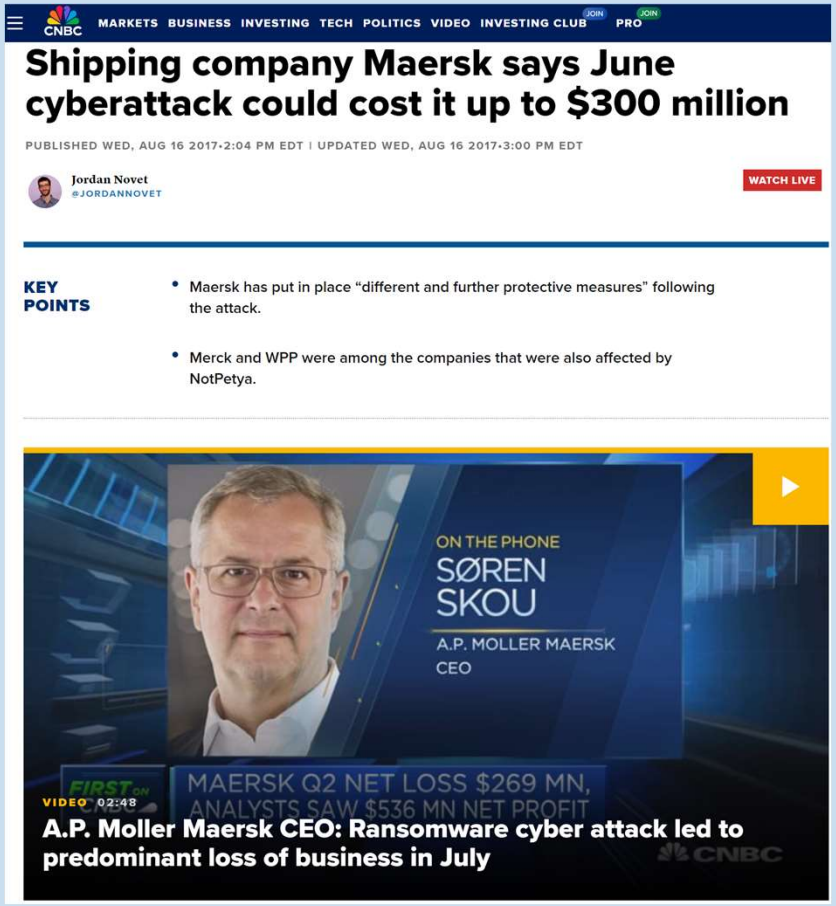
A Simple Strategy for Securing Devices Running Firmware

Monta Elkins – Hacker-in-Chief

foxguard

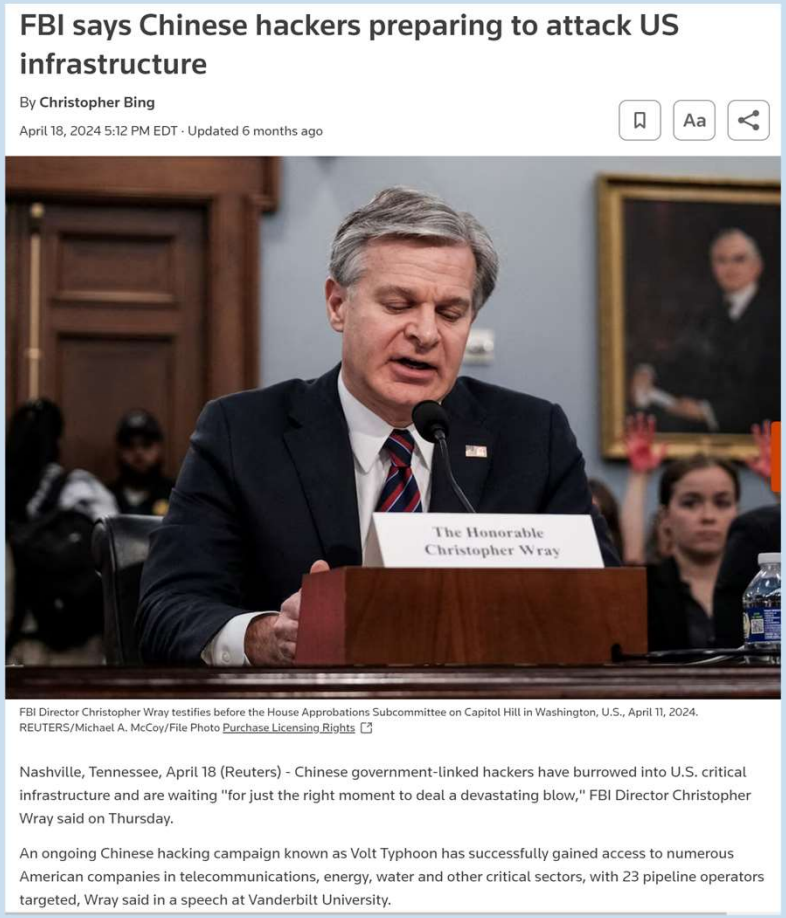
Who Would Attack Rail Systems?

- People who want money
  - Ransomware
    - Criminals
    - Foreign nations



Who Would Attack Rail Systems?

- Political differences
  - China
  - North Korea
  - Russia
  - Iran



FBI says Chinese hackers preparing to attack US infrastructure

By **Christopher Bing**

April 18, 2024 5:12 PM EDT · Updated 6 months ago

FBI Director Christopher Wray testifies before the House Approbations Subcommittee on Capitol Hill in Washington, U.S., April 11, 2024. REUTERS/Michael A. McCoy/File Photo Purchase Licensing Rights

Nashville, Tennessee, April 18 (Reuters) - Chinese government-linked hackers have burrowed into U.S. critical infrastructure and are waiting "for just the right moment to deal a devastating blow," FBI Director Christopher Wray said on Thursday.

An ongoing Chinese hacking campaign known as Volt Typhoon has successfully gained access to numerous American companies in telecommunications, energy, water and other critical sectors, with 23 pipeline operators targeted, Wray said in a speech at Vanderbilt University.

Why Protect Devices?

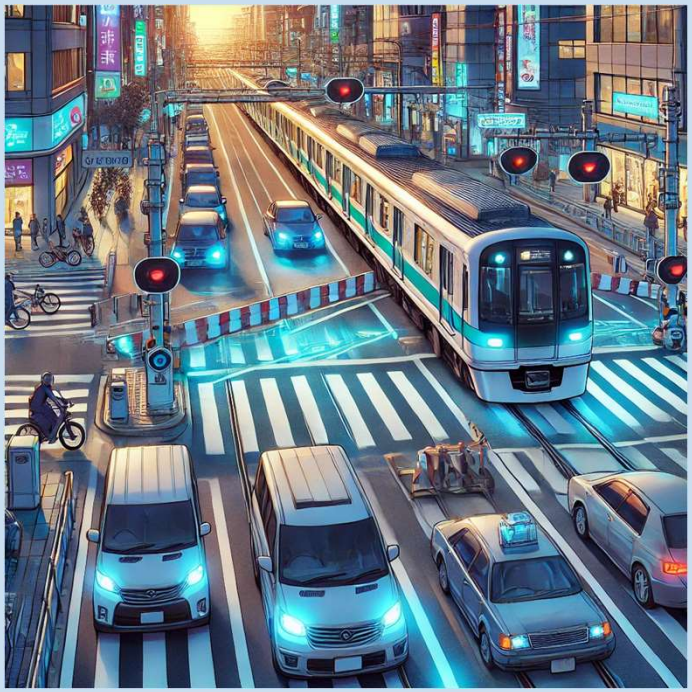
- On Time Performance
  - If someone else controls your system, it's only as punctual / reliable as they want it to be.
  - Electronic safety systems shutdown trains sometimes by accident. It could be much worse if it was intentional.

It Only Stays Up If Hackers Don't Bring It Down

foxguard www.FoxguardSolutions.com @MontaElkins www.linkedin.com/in/montaelkins

Why Protect Devices?

- Safety
  - There are many redundant systems to keep rail traffic and the public safe. If some of those safety systems were compromised, accidents would be more likely.



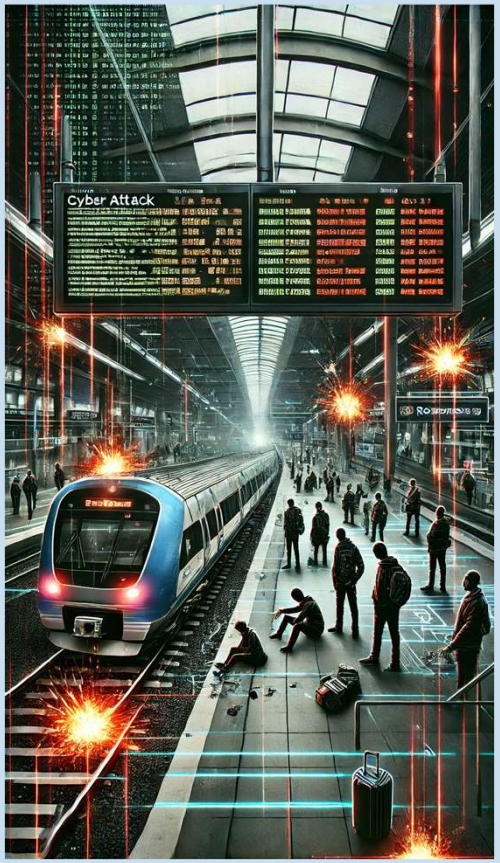
It’s Not Safe If It’s Not Secure

Cyber Attacks Can Cause Physical Damage

- The Aurora demonstration showed the destruction of a diesel powered electrical generator from a remote cyber attack in 2007. Some parts of the generator landed 80 feet away.
- https://en.wikipedia.org/wiki/Aurora_Generator_Test

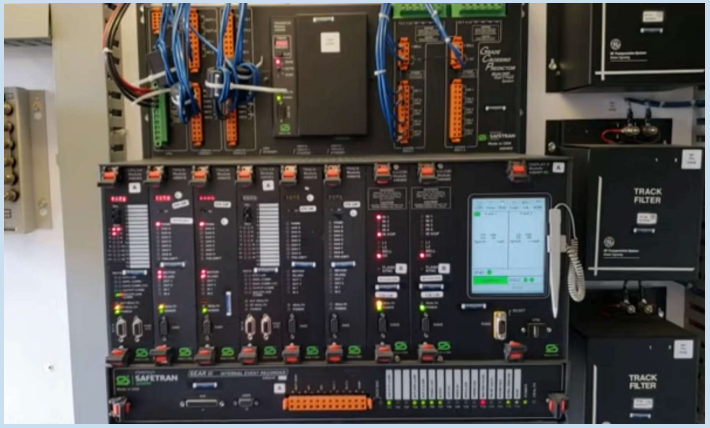
Some Rail Attacks

- **San Francisco Municipal Transportation Agency (SFMTA)**
  - Date: November 2016
  - Targeted System: Ticketing and customer service systems.
  - Impact: Service disruptions and loss of revenue.
- **German rail operator Deutsche Bahn Cyber Attack**
  - Date: May 2017
  - Targeted System: Electronic Station Boards
- **Italy's Trenitalia Cyber Attack**
  - Date: March 2022
  - Targeted System: Ticketing and operational scheduling systems.
- **Montreal Metro Cyber Attack**
  - Date: October 2020
  - Targeted System: IT systems, website, and customer support, door-to-door paratransit service, affected ~1,000 of 1,600 servers
- **Poland Railway System**
  - Date: August 2023
  - Targeted System: 20 trains stopped by "Radio_Stop" command



Redundancy: Failure vs Attack

- Grade crossing predictor
- 20 second signal at crossing
- All units have standby cards



Attack on Performance vs Safety

- Electronic Brake Units (EBUs):
  - Utilize electronic signals to manage braking across locomotives and railcars.
- Components of an EBU:.
  - Electropneumatic Interface: converts electronic signals into pneumatic actions.
  - Redundancy Systems: EBUs often include redundant circuits and failover mechanisms.

Remote Attack on Devices

HACKADAY

POLISH RAILWAYS FALL VICTIM TO CHEAP RADIO ATTACK

by: Lewin Day

41 Comments

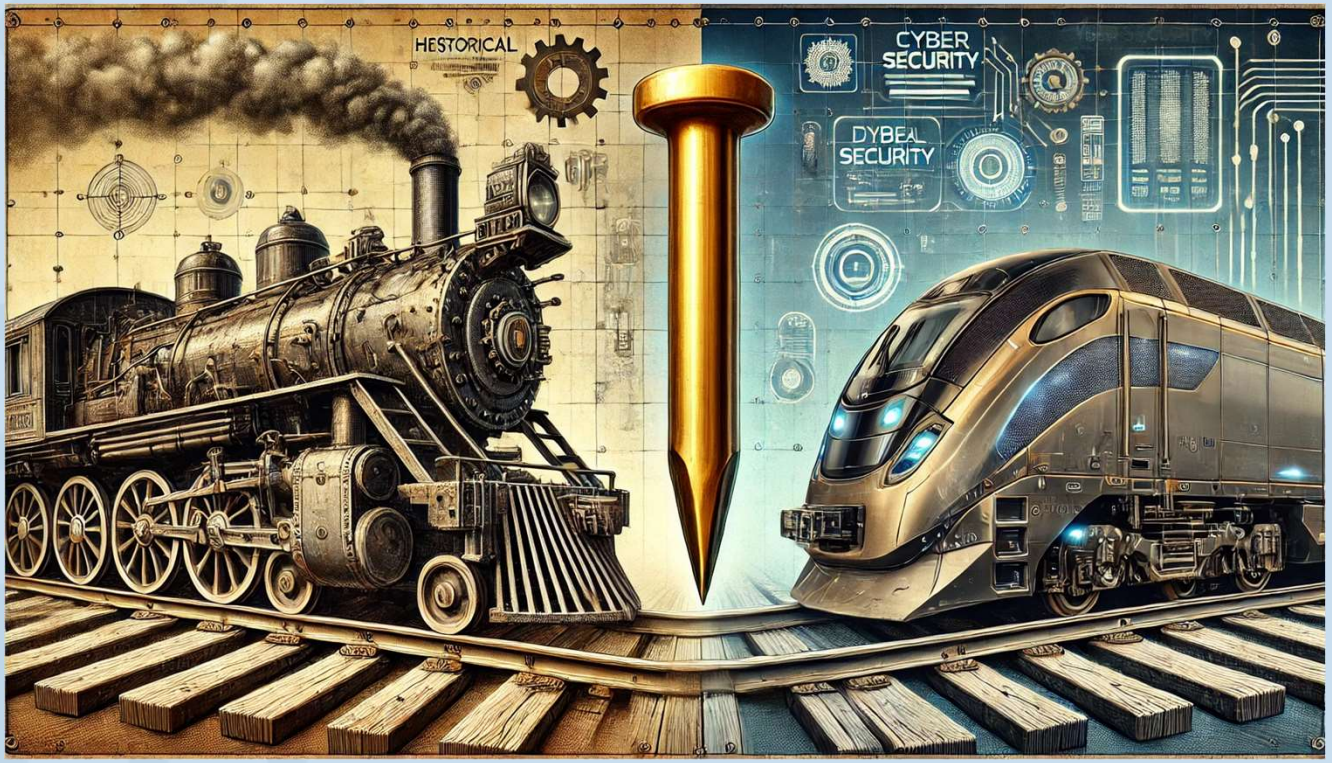
August 29, 2023

Poland's railways have recently come under a form of electronic attack, as reported by Wired. The attack has widely been called a "cyber-attack" in the mainstream media, but the incident was altogether a more simple affair pursued via good old analog radio.

The attacks were simple in nature. As outlined in an EU technical document, Poland's railways use a RADIOSTOP system based on analog radio signals at around 150 MHz. Transmitting a basic tone

foxguard www.FoxguardSolutions.com @MontaElkins www.linkedin.com/in/montaelkins

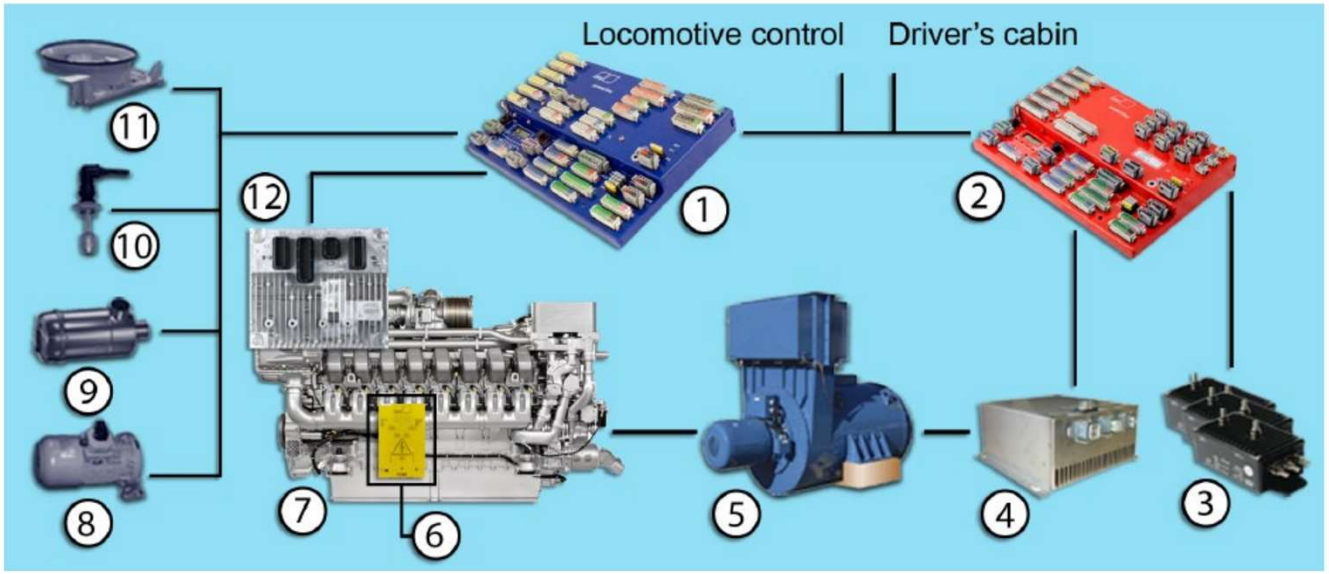
Slow Movement is Hard to See



Things Change

Electronic Devices “Buried” in Locomotives

Fig. 2: **System overview of dieselelectric AC/DC locomotives**



1	PAU Engine	7	MTU Series 4000Rx4
2	PAU Traction	8	Fuel management
3	Current-voltage convertor	9	Air filter management
4	Power output stage	10	Coolant level monitor
5	Traction generator	11	Cooler fans
6	POM	12	ECU (engine control unit)

Devices with Easier Access

- Cabinets that used to be full of relays now contain computers
- Are cabinet alarms enabled?
- Are they investigated?

What is a Broader Category for “Device”

- What are these things?
- What do they have in common?
- What do they do at a very high level?
- What common category do they all reside in?

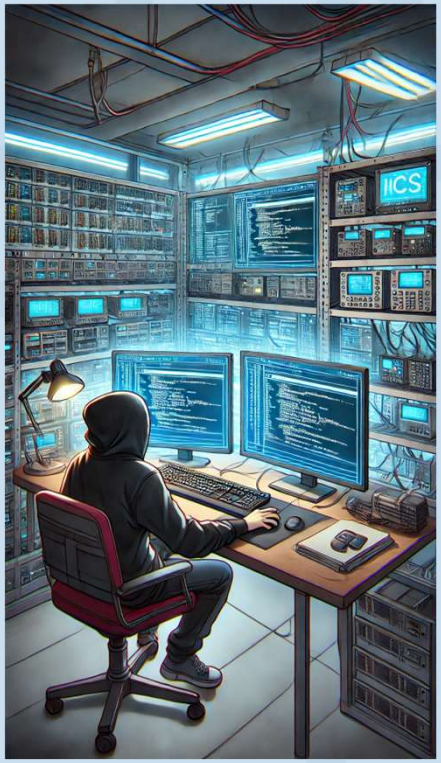
They Are All Computers!

- The have a CPU
- They have RAM
- They have a file system
- They have I/O
- They run firmware or software

What is the Difference Between Firmware and Software?

- From a security point of view, what is the difference between firmware and software?

Differences Between Firmware and Software

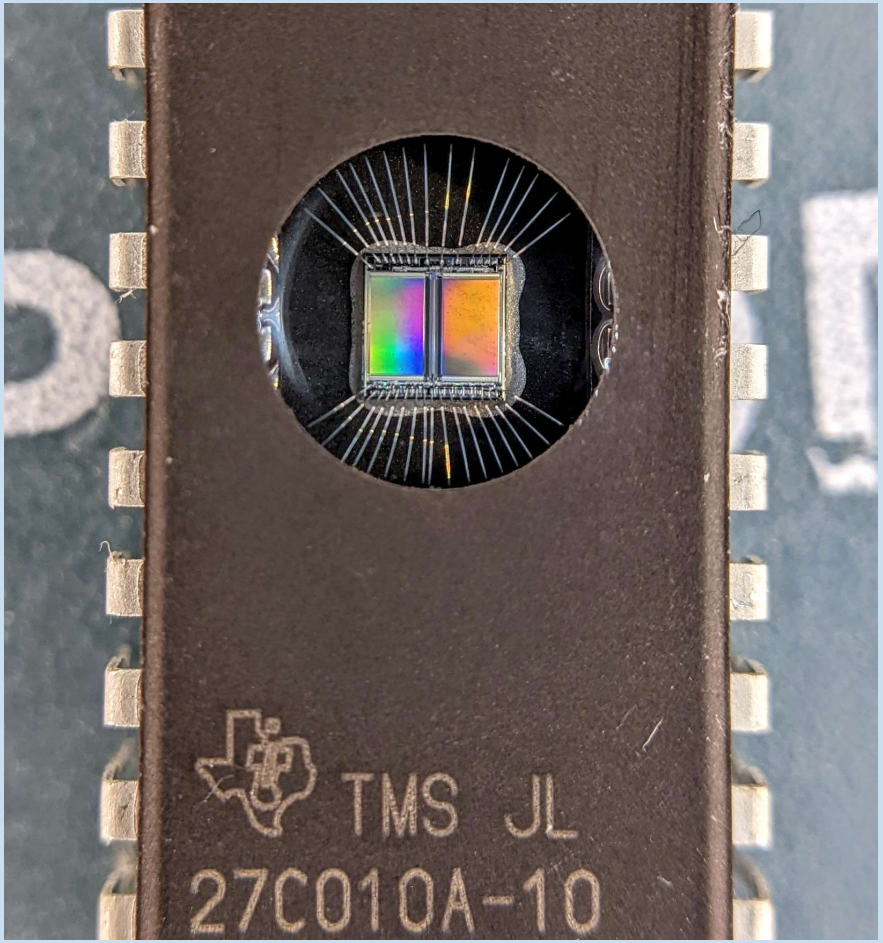


- Firmware
  - Single package
  - Harder to update / verify / hash / manage
  - May have vulnerabilities just like software
  - Myths
    - Firmware is somehow perfect
    - System security is affected by it
    - There is nothing you can do about it
    - You don’t have to update or patch it
- Appliances
  - Refer to myths listed above

Programming Firmware and Software

Immutable?


OFF
ON
1
2
3
4
5
6
ON
OFF
EPROM 擦除器
Zenith Data Systems
Boot ROM NE2000


TMS JL
27C010A-10

What Is This Thing?

- Demo

What is This Thing?

- A drill
- A small Industrial Control System
- A VFD with sensors
- A computer running software that may be vulnerable
- And plays music

Is This Device Important?

Is it exposed?

Your “Air-gap” Isn’t Perfect

- Vendors
- Contractors
- Employees
- Visitors
- Mobile devices like laptops
- Technical Documentation, patches, A/V updates, and other file movements
- USB thumbdrives, harddrives, SSDs, Cell phones
- Stuxnet
- Usually imaginary

You still need to do security

Tesla employee offered $1 million to insert an infected USB stick

Wireless in Rail

- **Positive Train Control (PTC)**
  - **Frequency**: 220 MHz in the U.S.
    - I-ETMS (Interoperable Electronic Train Management System)
    - ACSES (Advanced Civil Speed Enforcement System)
  - **Purpose**: Manages train speed and track conditions using RF communication between trains, tracks, and control centers.
- **Digital Mobile Radio (DMR)**
  - **Usage**: Low-bandwidth voice and data communication between train operators and dispatch centers.
- **Terrestrial Trunked Radio (TETRA)**
  - **Application**: Secure, trunked radio for emergency and operational communications, widely used in rail networks globally.
- **Global System for Mobile Communications – Railway (GSM-R)**
  - **Specialization**: A GSM variant for rail, providing voice and data services, supporting signaling and dispatch.
- **Wi-Fi and LTE (4G)**
  - **Onboard Use**: Provides internet access and operational communication for real-time monitoring.
- **Satellite Communication**
  - **Coverage**: Supports GPS tracking and data transfer in remote regions where terrestrial networks are unavailable.

Wireless in Rail

- **VHF and UHF Radios**
  - **Purpose**: Short-range communication for emergency and maintenance operations.
- **Automatic Train Control (ATC) Systems**
  - **Function**: RF-based management of train speed and positioning, ensuring safety and operational efficiency.
- **Broadband Radio Communication Systems (BRCS)**
  - **Capability**: High-speed data transfer for diagnostics and multimedia applications.
- **European Train Control System (ETCS) Level 2**
  - **Integration**: Uses GSM-R for continuous train-to-track communication, replacing traditional line-side signals with digital signals.
  - **Advancement**: Forms part of the UK's strategy to modernize rail through the Digital Railway program.
- **Future Railway Mobile Communication System (FRMCS)**
  - **Successor to GSM-R**: Set to use 5G technology, enhancing data bandwidth and supporting applications like predictive maintenance and enhanced signaling.
  - **Deployment**: Planned as a global standard under the European Union Agency for Railways (ERA).
- **Wi-Fi**
  - **Passenger Connectivity**: Provides internet access and entertainment services onboard.**Operational Use**: Real-time data transfer for diagnostics and maintenanceTITANICGLOBAL RAILWAY REVIEW.
- **Bluetooth**
  - **Short-Range Communication:** Connects onboard devices and trackside infrastructure

Wireless in Locomotives

- ElectroMotive Diesel Inc. Intellitrain
  - fault history, geofencing, automating the software upload process to push software updates
- MotivePower Central Diagnostics System (MPXCDS) (Wabtec)
  - CDS transmits data securely through an on-board modem to the server site
- Wabtec RailConnect 360 Remote Monitoring & Diagnostics
  - locomotive health, geofencing
- Lat-Lon L.L.C.'s Locomotive Monitoring Unit (LMU)
  - full automatic engine start/stop system with over-the-air programmable capability for rapid adjustments, GPS
- Wi-Tronix L.L.C. offers the Wireless Processing Unit (Wi-PU)
  - maximum authorized track speed, including slow orders and temporary speed restrictions, are sent to the on-board Wi-PU

When Will Your Devices Be Attacked?

- When they are the easiest target
- When they are on the edge of your network
- When they protect your cyber infrastructure
- When they communicate over untrusted network infrastructure
- When there are known/published attacks for them

How do we protect devices running firmware?

You Have the Power

You already have the tools and procedures and policies in place to secure your important devices with this one simple trick....

You Have the Power

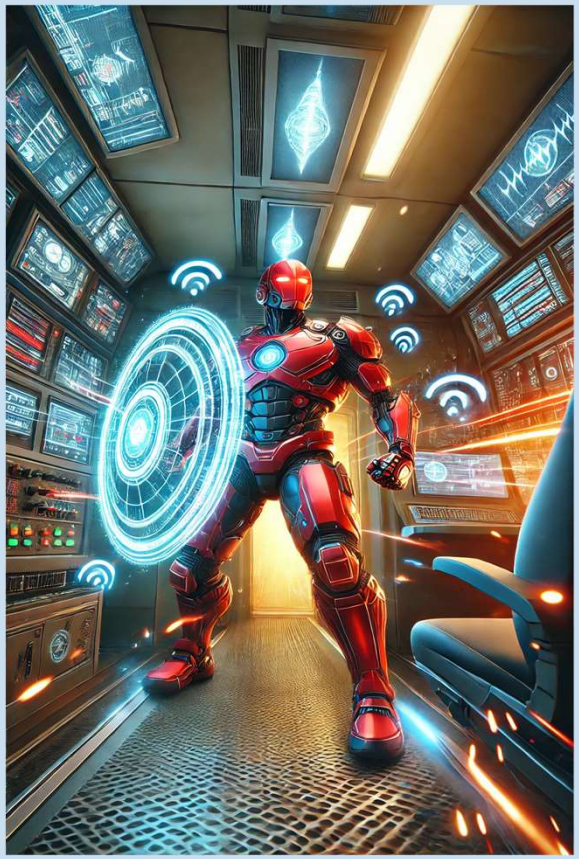
Call them computers running software!

How do we protect computers running software?

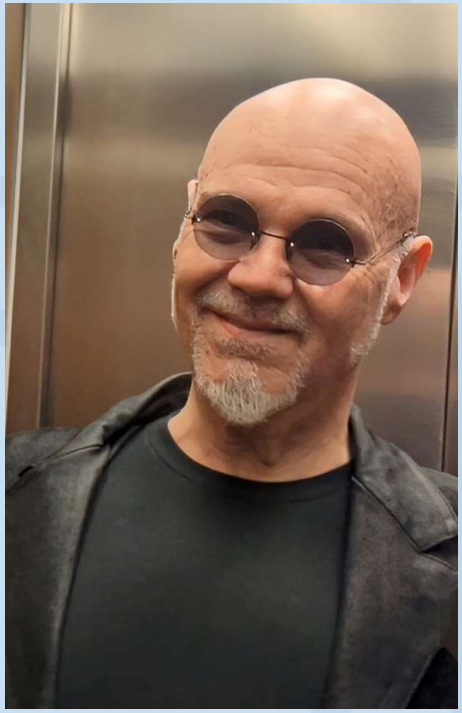
How to Protect Computers Running Software?

It's ok that not all methods apply to all computers.

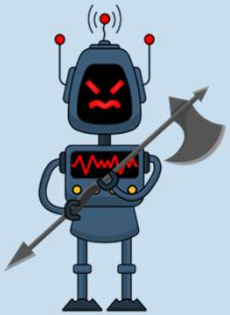
- A partial list
  - Physical access protection
    - Audit locks
    - Monitor & respond to cabinet / bungalow alarms
    - Rail Cars with communication channels
  - Application runtime control (signed firmware)
  - Patch devices with known vulnerabilities
  - Verify downloaded software - signed hashes
  - Supply chain attack prevention
  - Setup firewall rules or host based firewall
  - Monitor logs (use a SIEM)
  - Passwords (reset default, make strong, use two factor auth)
  - Harden, turn off unnecessary services
  - Least privilege role-based accounts
  - Monitor network / RF traffic
  - Network Segmentation
  - Regular Backups
  - Security Awareness Programs
  - Audit accounts and security settings regularly
  - Encrypted Protocols



For More Hardware Hacking Content



- Tips, Tricks, Events and Video on:
  - LinkedIn, X/Twitter
- Hardware Hacking Essentials Class
  - 5 days, lots of hardware included
- www.FoxguardSolutions.com
- SANS ICS410 SCADA Security Essentials
- **Follow me for this and more**
  - **@MontaElkins**
  - www.linkedin.com/in/montaelkins



foxguard