

Hillbilly BBQ

Your Rail Networks Put To Use To Facilitate OUR Party...

Blunt Statement:

This presentation took longer to put together
than it took to hack most of your systems.

Who Are We?

- The team:
 - **Chris** (Hairy thing stood in front of you...)
 - **Chester** (Hairy thing in the audience.)
 - **Jesse** (Hairy thing from Nebraska...corn fed...)
 - **Brett** (Hairy thing who's location was critical to this!)
 - **Kelsie** (Not hairy, but keeps us in order!)
 - **Jen** (Making sure we articulate accurately.)



Translation Note!

- I'm from parts of the UK, but left a while back
- I now live in the USA, which is why this is US-centric.
- I mix terms... (I'm not fully integrated into their culture!)
- Sorry
- Translations: www.railway-technical.com/us-uk.shtml

Why Are We Here?

- You Invited us here...blame James!
- Statistics:
 - USA: 2000 collisions a year on the railroads, a person dies ever 33 hours and is seriously injured every 11 hours....
 - UK: Proportional (shorthand for I don't have the numbers to hand) last time I checked you still manage to kill and mangle people.
 - <https://oli.org/about-us/news/collisions-casulties>
- The collective you (that is the rail industry) have issues, we want to help.
- It makes a welcome change from continually breaking into banks.

Balance And Collaboration

- There IS a need for responsible disclosure...
- There IS a desire for change...
- There HAS to be acknowledgement from the industry that there are issues.
- There NEEDS to be a pathway to change involving ALL parties.
- There HAS to be communication, your silence and lawyers sucks.
- If this happens we have balance AND a path forward.
- If not then researchers end up frustrated and your railways grind to a halt.

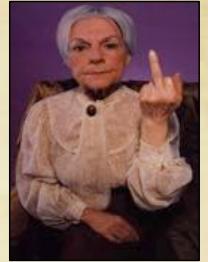
Step *AWAY* From The Lawyers

Collaborative Options...



- Positive collaboration:
 - We ALL discuss things in an open forum (yea utopia and unicorns.)
 - It's acknowledged that the current status HAS to change.
 - Someone calls GE, Siemens and Alstom and gives them the bad news.
 - Everyone bands together to force change from the vendors.
 - We ALL get a timeline in place that makes sense AND stick to it!
 - Someone lets the government know we're working on it.
 - Someone ELSE deals with the ensuing red tape ☺
 - Nobody bloody bans me from trains!
 - Oh, and I can still go to and from the UK/USA without grief...

Collaborative Options...



- Alternatives to collaboration:
 - Nothing is discussed in open forums, everyone's in their own silo.
 - Nobody wants to admit that things have to change.
 - Nobody hauls GE, Siemens and Alstom over the coals..
 - The vendors are hit one at a time and pander to you individually.
 - Everyone is on their own timeline and nothing gets done for years...
 - The Government gets wind of this and puts “regulations” in place.
 - Someone has to deal with auditors and more bloody lawyers...
 - I get banned from trains.
 - I sneak into the UK via Iceland and Scotland, too much hassle!



Why Are We Here?

No1. Blame The School System!

41. Two stations A and B are 100 km apart on a straight line. One train starts from A at 7 A.M. and travels towards B at 20 km/h speed. Another train starts from B at 8 A.M. and travels towards A at 25 km/h speed. At what time will they meet?

- (a) 10.30 A.M.
- (b) 11 A.M.
- (c) 10 A.M.
- (d) None of these

A freight train leaves a station traveling at 32 km/h. Two hours later, a passenger train leaves the same station traveling in the same direction at 52 km/h. How long does it take the passenger train to catch up to the freight train?

- a. 5.2 hr
- b. 4.2 hr
- c. 3.2 hr
- d. 2.2 hr

Question #18

A passenger train starts from rest and leaves a station with a constant acceleration. During a certain time interval, the displacement of the train increases to three times the value it had at the start of that interval. During that same time interval, determine the increase in the train's velocity. Let v represent the speed of the train at the end of the time interval; and v_0 represent the speed at the beginning of the interval.

- a) $v = v_0$
- b) $v = 1.4v_0$
- c) $v = 1.7v_0$
- d) $v = 2.0v_0$
- e) $v = 3.0v_0$

No2. Those School Safety Videos!



Modern Version Of That Safety Video



Thanks to the team that put the “Dumb ways to die” video’s together!!

No3. You Carry Cargo We Target...

- Several years ago researched how to stop food getting to the table..
 - You are part of the food chain.
- Got asked IF we could stop electricity from being produced a while back...
 - Aside from hacking the grid, YOU carry the coal.
- There's a number of groups who don't like GMO...
 - You carry the products, you are THEIR target.
- You have antiquated computing systems covered in cobwebs...
 - What better way to prove a point than to grind London to a halt?

No4. The OSI Model Gone Wrong...

- PTC has been designed to be a secure application.
- All the security is handled BY the application.
- The application “runs at layer 2”
- Therefore the application is secure...
- WTF !!?
- This IS the mentality we’ve been dealing with, hence WE ARE HERE ☺

Ok, Squirrel Moment Over



On With The Show...

- Scenario:
 - We watch, we observe, we learn and we want to help before it gets messy.
 - To illustrate how broken things are, we're throwing a BBQ...
 - It's the USA... Go Big or Go Home...
- Status:
 - Worked a LOT on agriculture and locomotives back in 2014-2016
 - Worked with a couple of teams (represented here) in 2016 and early 2017
 - This work EXCLUDES that team research from 2016/2017
 - These Attacks were researched and planned in 48 hours period...

That 48 Hour Attack Period..

- Several willing and able researchers.
- 200 foot of Cat5 cable.
- Numerous devices to monitor over-the-air signals.
- Couple of specific connector types.
- Close proximity to a number of waysides...
- Very close proximity to a rail yard
- Potential access to numerous locomotives.
- A comprehensive set of lock bypass tools.
- A few bottles of GOOD single malt.
- Enough batteries to keep us happy.
- Safety shoes (mustn't forget those.)
- No bloody orange/yellow vests.



Breaking You Down...(Literally)

- Locomotives
- Rail cars
- Lineside structures (signals, switches, wayside, etc.)
- Dispatch (controller, back office)
- Yards (rail and intermodal)
- Physical infrastructure (bridges, tunnels, etc.)
- Ballast, ties and tracks

BBQ Ingredients List

- Food, given it's a BBQ primarily dead animal of choice.
- Drink, we found wine, beer and OJ on the railcars...
- Snacks
- Seating, this one's interesting, found sofas AND deckchairs...
- Cover fire (this IS going to attract attention...)
- People, lots of them.
- Heat sources (cooking and warmth for people.)

Technical Tools (Needed For BBQ)

- Ha! We are safe, the railroad is complex and unique tools are needed...
 - Not so much these days:
 - Laptop (the very same one being used for this presentation.)
 - Cat5 cable (same stuff we use in the office.)
 - Antenna (readily available on Amazon!)
 - 12mm pin cable to RJ45... Yep got the pin-outs and made our own.
- But! Our software is proprietary, and our signal stuff is complex!
 - Google YouTube for “GE and PTC and bootcode.”
 - Google “GE and ElectroLogIXS and password.”
 - You get the hint, ALL your vendors and partners give you away.

Where IS The Food?

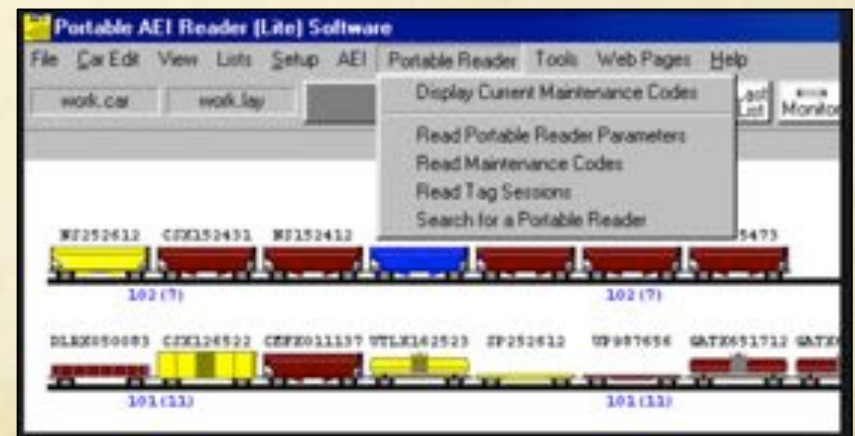
- ORBCOMM (Satellite or cellular on the move)
 - Thanks to some badly handled SQL queries we can track all your cargo.
- TransCore (RFID in motion or in yard)
 - Once again the SQL issues bites back, now we can organize your cargo.
- Softrail (railcars in the yard...where's my snacks?)
 - Thankfully the software can be readily downloaded and reverse engineered to allow full access.
 - We can now built YOUR train to OUR specifications.
- For cooking the BB! we will need TRANSCOM.
 - Thank goodness the same developers seem to have made the same mistakes!
 - Now we can track the nuclear stuff and all other things that go bang in the night.

Ah, There's The Food...



Once we've arranged them all nicely (notice the variety of carriers) we can simply stack them in the necessary order for the picnic/BBQ menu.

Thankfully there's software to help us work out both where our individual rail cars are, AND how/where we need to move them...



This Country Is Too Big!

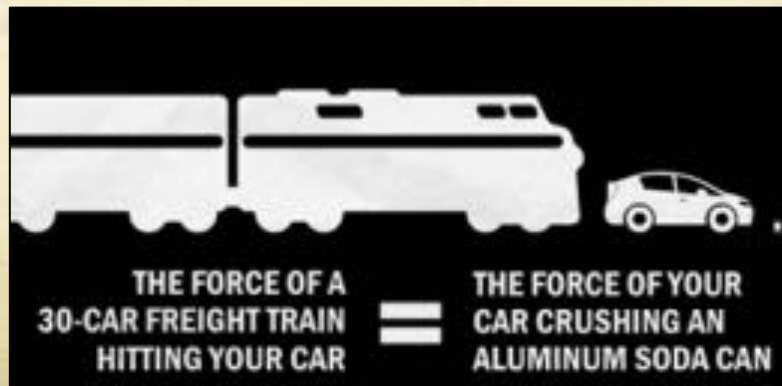
- Picnic train thanks to a mix of GE's intermodal software and Softrail's inventory tools.
 - We need refrigeration units with dead animal (BBQ) from CO or ID.
 - Molasses will be sourced from Chicago and Florida.
 - Florida's got the OJ too...need some of that for the kids.
 - We need beer from the Midwest (we will ignore it's not finished)
 - We will grab the wine train on the West Coast.
 - We will grab the combustible material from the West.
- So, we know where the railcars are (intermodal and rail cars in 6 different locations) we know who owns them (aside from us...) Now we need to work out HOW to get them to us...AND have it all arrive at the right time!
- This is the ONE single use for that bloody school math problem!

Intermodal, This Just Got Painful...

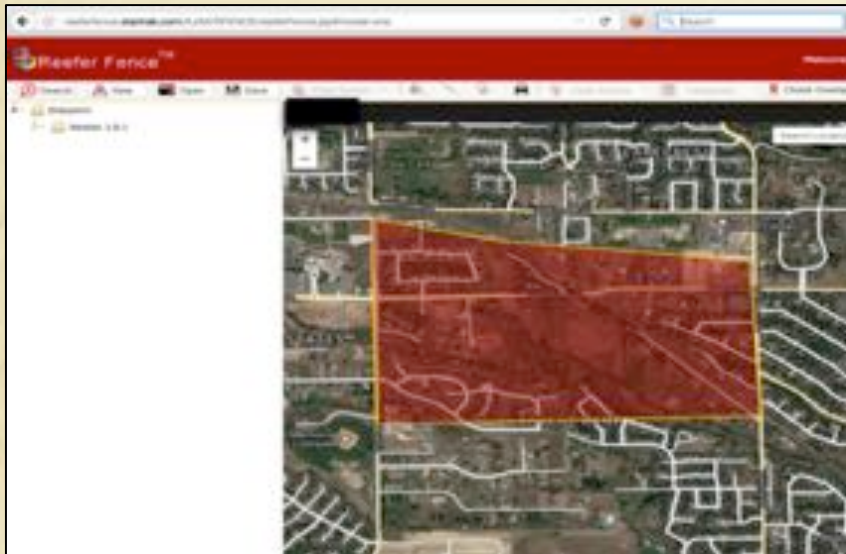
- Just to throw something out at this juncture...
 - We've NOT touched shipping.
 - We've not touched YOUR cranes.
 - We've not looked at the lorries (trucks).
 - We've yet to break the DOT system that manage the weigh stations.
 - We've looked at the autonomous container systems...
 - We've really poked at the technology used to scan those containers...
- Yea, that whole infrastructure is next on the hit list, and it's not pretty.
 - Sorry Freightliner, maritime & friends.

HOW Do I Get The Food To Me?

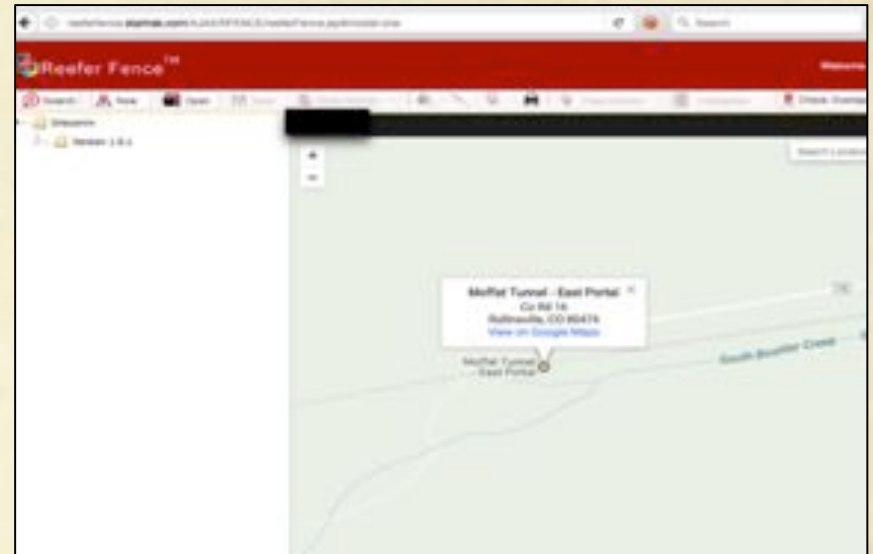
- All YOUR locomotives belong to us...
 - GE
 - GM-EMD
 - ALCO (DLW)
 - GE PowerHaul (We haven't forgotten the UK ones...)
 - Vossloh
 - Siemens



Reefer Fence, For Wandering Railcars...



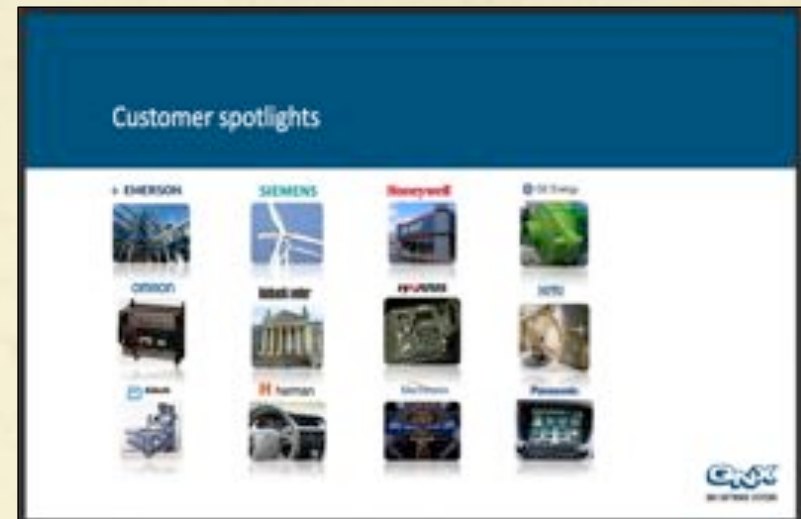
Reefer Fence is used to ensure correct assets are in the right place at the right time, above, we used Jesse's and Brett's house as the staging point for the East Side locomotives and rail cars...



Above, the Moffat tunnel East portal being "fenced" to ensure we deliver the dead animal, molasses and other ingredients at the right time...

GE Locomotives...

- Modern locomotive supplier
 - Not so modern outlook on security
- Multiple attack vectors across the systems
 - Engine (ECU attack vectors)
 - Thermal protection sensors
 - Diagnostic data feeds
 - Cooling system attack options
 - GE LocoCAM I see what you see...



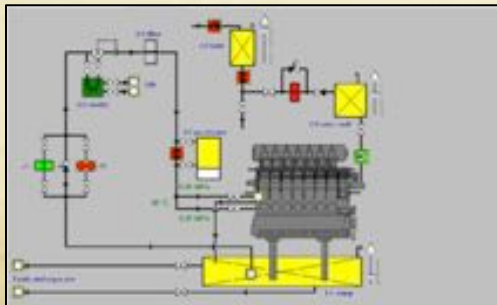
GE & QNX...a marriage of vulnerabilities

All YOUR Data Belongs To Them...

- A brand-new Evolution features 250 sensors that pull in 150,000 data points per minute turning the locomotive into a "rolling power plant."
- With the sensors measuring so much real-time information ~ weather, oil pressure, temperature, speed, and so on ~ the idea is to be able to determine how the locomotive is performing at any given moment.
- That up-to-date mechanical health check is going to be crucial to customers like BNSF or Union Pacific who lose a lot of money when there is downtime.

GM-EMD Locomotives...

- Electro-Motive diesel (H-Engine)
 - Up to 6,300hp (you can see why I like it)
- Failed in US, loved in China, AUS and India.
 - 3rd party (vendor) software support
 - In-house software development...
 - Remote “support” IF you know ID/PWD
 - Hint...try “000000”



ALCO Locomotives...

- First off, excuse the cobwebs!
- Then, dust off the “shop” PWD
- Older code
 - In many cases NO passwords.
 - In all cases, NO encryption.
 - Thankfully (for us) lots of comments left IN the code.
- For the most part these are attacker-present vectors we can exploit.

Feature/Parameter	Range	Default
ECM Master Password - Parameter	2-6 characters	None
ECM Reset Password - Parameter	2-6 characters	None
ECM Adjustment Password - Parameter	2-6 characters	None
Vehicle Speed Sensor Anti-Tampering	Enable/Disable	Disable
Vehicle Speed Sensor Maximum Engine Speed wo/VSS	1400 - 2500 rpm	2500 rpm

PowerHaul ☺

- This was relatively simple:
 - See GE ☺
 - Or admin : admin
 - Or monitor Telnet...
- Failing that:
 - Network sniffing and replay attack
 - QNX once again fails badly
 - Application layer attack
 - Defaults in place in code/app
- Attacker-present attack, but quick insert of tools would allow full remote access.



Still To Work On...

Ansaldo-Breda
Bombardier
CNR
CSR
Kawasaki Rail
Kinki Sharyo
Hyundai Rotem
Von Roll





In North America alone 100% of all railcars in interchange service are required to be equipped with TransCore tags, since the Association of American Railroads adopted the RFID technology as the standard for automatic equipment identification in 1991.

Got Railcars, Got Locomotives...next?

Signals!

- Signaling
 - CAF
 - Vossloh
 - Alcatel
 - Alstom
 - Bombardier
 - CESS
 - GE (again....) Global Signaling
 - Nippon Signal
 - Westinghouse Rail Systems
 - Wabtec
- Switching
 - Mitsubishi
 - Vossloh

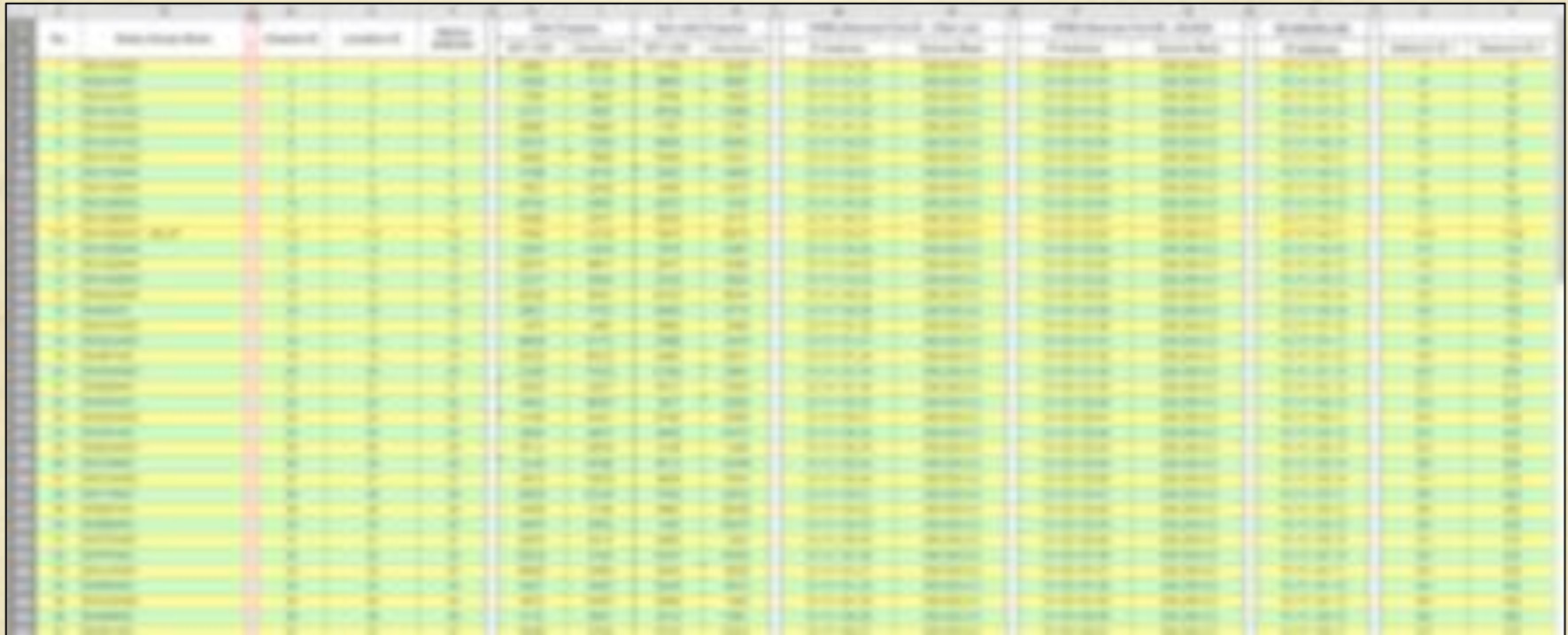


Signals Researched

- <https://www.youtube.com/watch?v=qO-Yl-zwNAs>
 - All about your ElectroLogIXS ☺
- <https://www.youtube.com/watch?v=vxxfzHxbnFU>
 - And this tells you how to get into them, upgrade and use them ☺
- Research Wabtec, Schneider and ALL the others.
 - Defaults
 - Insecure protocols
 - Replay attacks
 - Buffer overflow attacks
 - Etc!



Enough Research Hack The Damm Things..



No	Relay house	Location	VITAL CRC	Checksum	IP addresses	ALL VLANS	ALL along our Picnic route
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							
65							
66							
67							
68							
69							
70							
71							
72							
73							
74							
75							
76							
77							
78							
79							
80							
81							
82							
83							
84							
85							
86							
87							
88							
89							
90							
91							
92							
93							
94							
95							
96							
97							
98							
99							
100							

Relay house, location, VITAL CRC and Checksum along with IP addresses for ALL VLANS, ALL along our Picnic route..

Signals Hacked

```

Enter Password->harmon
GETS Global Signaling LLC VHLC ACP Software (c) 2003
Genisys Unit : Version 2.2      VLP : Version 1.13 M/ALT CODE 5

Top Level
0: Diagnostic Port Logging
1: Display Memory Log
2: Memory Log Logging
3: Reset Statistics
4: Date and Time
5: Setup Info
6: Local Control
7: Code Line Maintenance
8: Display Logic Variable
9: Log Off Menu
10: Debug Menu

--:up /:top menu *:toggle menu on/off T:display menu
ACP> 1

```

- GE Transportation Global Signaling
- Passwords transmitted in the clear
- Sniff the traffic (over air or on wire)
- Scrape out the necessary handshake...
- Replay attack
- Job done, now own Signals
- On we go with the picnic train

Thanks to OSINT we find file servers like this ALL over the Internet..

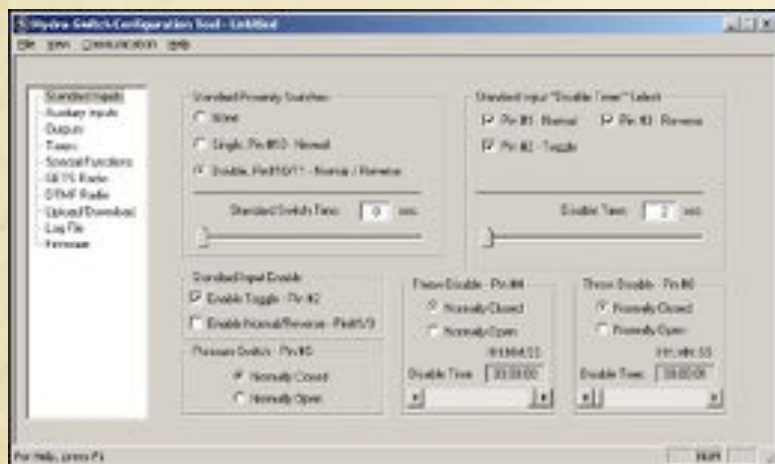
Pretty much each folder has both the instruction manuals AND the passwords (If they have been changed from default...)

Upside: As our picnic train goes through this section of track we will have NO problem with it stopping ☺

- Communications Equipment
 - Catalog Cut RuggedComm RS900 Ethernet Switch
 - RuggedSwitch RS900 Family - Installation Guide
 - FASTRACKS RTD West Corridor Fiber Optic Network Drawing
 - Dataprobe RSS Series Redundancy Switch Systems Installation and Operation Manual
- ElectroLogIXS XP4
 - ElectroLogIXS XP4 System Operation and Maintenance Manual (100323-010)
- Gate Mechanism
 - Western-Cullen-Hayes Model 10 Signals Equipped with Series 3590 Gate Mechanism Service and Installation Manual

Folders	
00 Site Plans	▶
01 ElectroLogIXS VLC EC5	▶
02 E2C	▶
03 Cab 101	▶
04 AFTAC	▶
05 PF Track Circuits	▶
06 EPIC Track Circuits	▶
07 Switch Controller	▶
08 GRS 5F Switch Machine	▶
09 TWC	▶
10 Wayside Signals	▶
11 Comm Equip	▶
12 ElectroLogIXS XP4	▶
13 Gate Mechanism	▶
14 Crossing Appliances	▶
15 Switch Heater	▶
16 Battery Chargers	▶
17 Power Supplies	▶
18 Other Equipment	▶
19 System Level Topics	▶

Switches Hacked



Hydra-Switch configuration software in action. In this instance it's being configured to run remotely (thanks to the initial access with the RS232 cable and some modifications to the box below (remote radio access))

One of several options for local/remote switch access depending upon manufacturer AND country.



Evolution Of Waysides & Lineboxes...



Hacked...



Mostly hacked...



Um, Nope!

Wayside Hacked

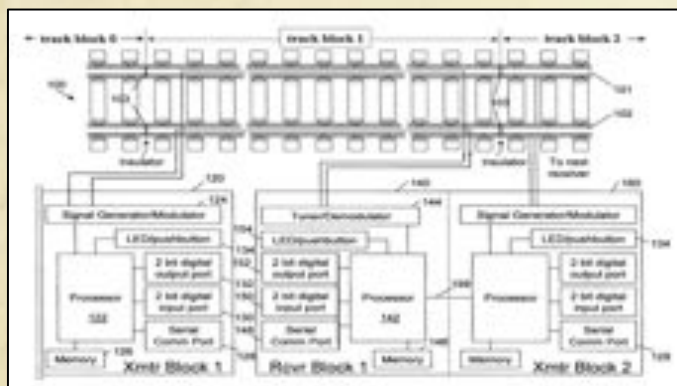
- Lock picks or bump keys, 30 seconds of work...and we're in.
- Cisco, Alstom (ElectroLogIXS), and Siemens (RUGGEDCOM) are our targets here...
- 200 foot of CAT5 cable (or similar) OR a Raspberry Pi and some Velcro.
- Several readily downloadable tools from YOUR partners or open source.



Bonus: Remote Replay Attack

Human Not-Present

Some Research...



Your vendors and partners are quick to explain on public forums and other electronic (open) mediums about how wonderful their technology is.

Leaving those of us looking for attack vectors some wonderful opportunities to explore the systems.

For those of you concerned that all I've been doing is plugging into YOUR networks...

Here's one I prepared earlier...thanks to the wonders of eBay, your own ElectroLogIXS system.



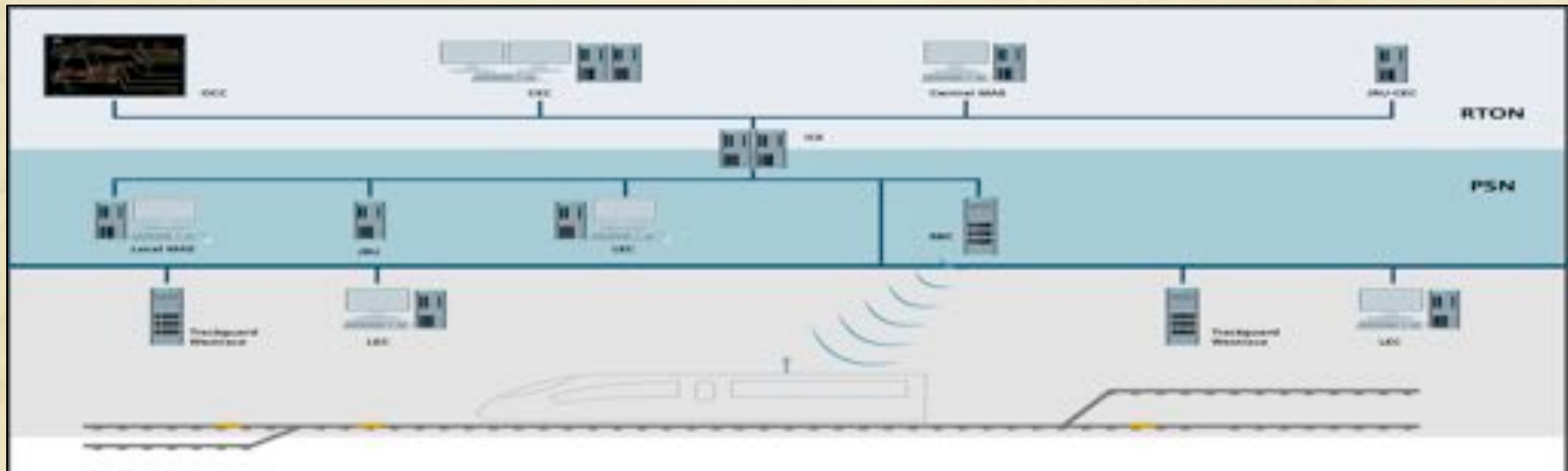
Not Present Attack Scenario

- Take the concept of a MitM (Man in the Middle) attack used across the InfoSec industry and apply it to signaling.
- System: Leave lights green as picnic train comes into upcoming signal path.
- Wayside/lights/crossing: Need to lower/drop/flash/validate (please.)
- Attack: MitM “Sure” here’s the legitimate packets to cover to both ends...
- Wayside/lights/crossing: Got it, go-ahead and pass friendly picnic train...
- Locomotive: Thanks too, picnic train passing through.
- Wayside/lights/crossing: No problem, happy to oblige...

MitM Result:



Focus On Europe...

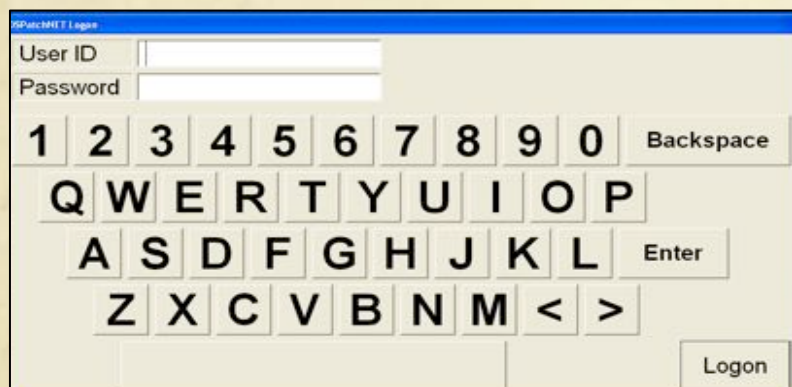


On-train, On-track and Off-train European version of PTC... Guess where we are going to focus next. Give us until this weekend and we should have a few more slides to add in here!

NOTE!

- All this is the HARD way to get our picnic stuff where we want it...
- A MUCH simpler method would be to hack the back office:
 - That way we can legitimately have our good delivered...
 - Not sure if dead animal, molasses, beer, wine and fuel would raise eyebrows though?
- This is the point where we should say “here’s one we made earlier”
 - HOWEVER as this is (ish) theoretical...
 - AND I want to come back to the UK
 - AND I want to get back INTO the US
 - Use your imagination!

Back Office Hack ☺



DSPatchNET Login

User ID

Password

1 2 3 4 5 6 7 8 9 0 Backspace

Q W E R T Y U I O P

A S D F G H J K L Enter

Z X C V B N M < >

Logon

Back office dispatching software login:

Upside: It's password protected

Downside: Defaults are in place

ID: Administrator

PWD: 0101010101... (you get the idea)

Failing that a bypass attack will crack open the DSPatchNET software if executed against the comms port.

Above is one of several back office attack vectors, the simple way to rationalize this is it's the same type of environment we've been practicing AND successfully breaking into for the last 15-20 years...

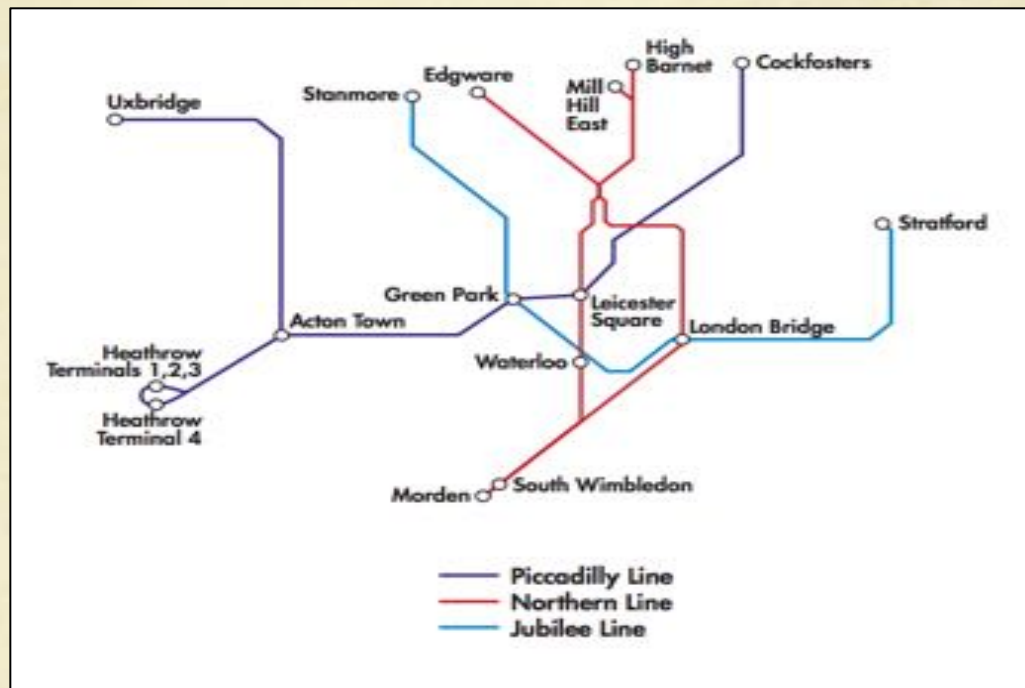
At This Point

- We have the food, we know where it is, we've gotten the locomotives hooked up and the drivers think they are delivering "their" stuff.
 - Note: We are not too sure we need the drivers, but we'll play safe 😊
- At this point, we've not had to break anything...
- Which is frustrating 😊
- Hence...



Squirrel Movement!

Hacking The Sponsors..



Dear Thales.....sorry about the planes from years ago, THANKS for the Underground...

Systems Researched

- We are using research in the title, that way the lawyers don't shoot...
 - SelTrac systems on the Northern line, those cables and antenna...
 - ATC system on the Central line, plenty to research on "NDF" errors
 - Train to wayside communications on Northern/Jubilee lines...
 - Emergency braking systems on several target trains.
 - NetTrac and the OTS systems it's implemented on, not good.
 - ComTrac and the implementation in some target systems (not London Underground in this case)

THALES IS EQUIPMENT AGNOSTIC

Our solutions work with all rolling stock: Thales is currently powering rolling stock manufactured by Alstom, Ansaldo-Breda, Bombardier, CAF, CNR and CSR of China Railway Rolling Stock Corporation, Kawasaki, Kinki Sharyo, Mitsubishi, Hyundai-Rotem, Siemens, Taiwan Rolling Stock Company (TRSC), Vossloh, Von Roll and more.

Yep, we know...you can install everyone's equipment in default mode...

Or with basic security...Please stop just letting the client dictate the bloody codes!

Sorry, couldn't help it...snuck this one past Chester...



Squirrel Movement Over

BBQ Options

- Slow cook (Briquettes)
 - Coal trains.
- Deep Fat (Turkey fryer)
 - Oil (preferably cooking grade, LPG at a pinch.)
- Smoker (ish)
 - Cedar logs combined with Liquid Oxygen...
- Microwave (ish)
 - Nuclear waste or nuclear enrichment.



ACALVIO

Putting It All Together

CYBER
SENATE

Moffat Tunnel (East Portal)

- East Portal has better access for guests
- East Portal has better containment for marinade
- Several track convergence close to the tunnel
- West portal will allow both Food and Fuel access
- Easy access to the infrastructure
- Tunnel systems not well protected

Ready to BBQ!



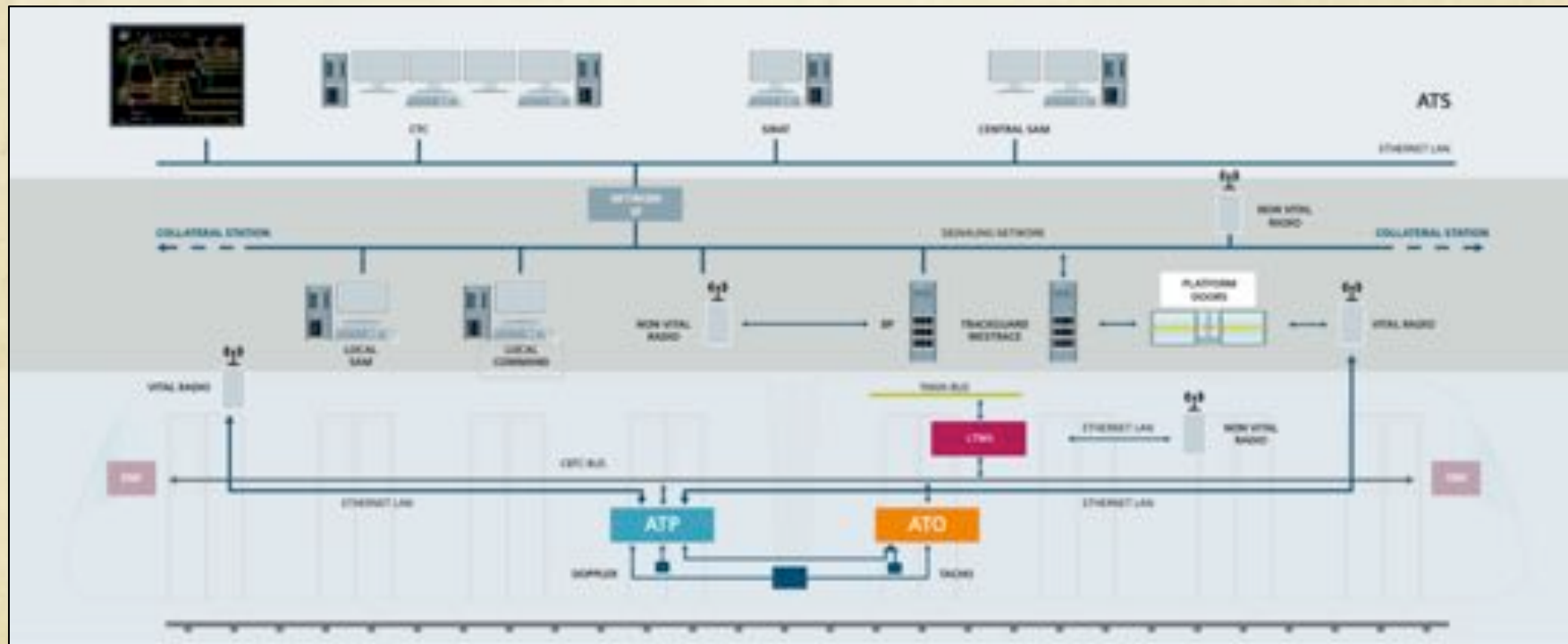
For the Americans...



For Me!



Hack The System To Get The People...



Status:

- East Train – En-route
- Midwest Train – Sitting at Jesse's
- West Train – Sitting at the West Portal of the tunnel
- Cooking Train – Nuclear is currently being “borrowed”
- Chef – Brett's on his way
- Location – Sorted 😊

How To Crash Trains (Deliberately)

- Signals
 - Green lights for passing through.
 - Advertise improper speeds though bends or other restricted areas.
- Breaking
 - Cause improper breaking in the safety systems to create unsafe conditions
 - Cause locomotive to stop while still at switch crossing.
- Switching
 - Modify the switch as the train is passing through it.
 - Switch the locomotive onto wrong track...

End Game.

ACALVIO



CYBER
SENATE



How we feel sometimes when stonewalled...



How we want to react to “it’s all fine...”



Reality...too many meetings NOT enough action

You Are FKED**



Mentality reset!

Reset Part 1

- Security IS NOT an afterthought.
 - Build it in from the very start of a project!
- Security IS NOT something to remember AFTER QA.
 - SDLC is not just a nice to have...make it a bloody priority.
- Security IS NOT left out because of budget issues!
 - Quit the free lunches and secure the bloody product instead!
- Security IS a mindset.
 - Welcome to 2017 and beyond, the hackers OWN it.
- Security IS the differentiator.
 - Your clients actually might thank you!
- Security IS our RESPONSIBILITY.
 - Because if it's not, guess who's going to rip your new toys to pieces.

Reset Part 2

- Vendors need to be held responsible for delivering secure products to ALL their clients ALL the time...not 3 years down the road IF enough people scream.
- Integrators need to be held responsible for educating partners AND vendors AND choosing wisely.
- Integrating “smart” devices into mechanical systems is difficult but can be done and can be done securely IF you take the time.
- Being secure is more than slamming product after product into the environment.
- This years blinky light isn't going to save you, last years didn't save you. Save your money and spend wisely...get a maturity model in place and use it!

Evolve Or Die

Thanks Packet Storm!

- The industry AND InfoSec have to autonomously learn their environment.
 - Adapt, emulate and bloody camouflage the security tools!
 - Learning behaviors should be built in.
 - Build something that can be physical OR virtual OR cloud.
- Anything we build has to be adaptive!
 - This IS a game of chess, why are we hampering ourselves?
- Security HAS to evolve beyond the reactive stack
 - Preventative (please!)
 - Predictive!
- Anything we build has to be intuitive...
 - PHD level installation instructions are BS!

More Consoles!?!?

- Seriously, another console and another 5 screens to review?
 - Integrate and stop building point solutions!
 - The GUI sucks if we can do more with bloody CLI.
- If it takes a month to roll it out it's going to fail!
 - Or ½ the staff is going to go back to their day jobs!
 - If it takes a dictionary to understand the instructions...
- Factor in the issue that leadership STILL has resource issues
 - We seem happy to throw \$\$ but not bodies?
 - We are happy to buy toys BUT not the installation OR support.

Passwords (Seriously!)

- Feel like we are flogging a dead horse....but it would be nice for once to NOT break into a company because defaults or outright dumb passwords are being used.
- Would be nice to break into somewhere where biometrics or smartcards are in widespread use, or two factor correctly deployed.
- The “cost” argument of deploying is BS... cost of remediation is 8x the cost of deployment; start fixing your passwords! (please)
- User education, user awareness, user understanding AND Executive buy-in...
- QUIT MAKING IT EASY! NO DEFAULTS! NO “Passw0rd!”

Something To Slow Us Down!

- As red team:
 - We don't want more default passwords.
 - We don't want hardcoded passwords/phrases.
 - We don't need shared keys that are badly encrypted.
 - We DO want a challenge...
- As blue team:
 - We don't want more screens to look at.
 - We don't need our users to find more insecure ways to work!
 - We want something intuitive.
 - We want help...not hindrance please.

With Thanks To...

- As I said earlier, the InfoSec community, for the most part wants to collaborate and see solutions, let us help.
- To James for inviting me here... go gentle on him.
- To Acalvio for allowing me to talk freely!
- To Chester for reigning me in on some of the slides...
- To EFF for continuing to put up with me.
- Eddie... for everything!
- Warner Bros. and Chuck Jones for Wile E. Coyote, Marvin, and his cohorts.
- The Minions, the squirrels, the cats, horse and polar bears...



HACKERS FOR CHARITY.ORG

“So long and thanks for all the fish”

Douglas Adams, you are missed.

