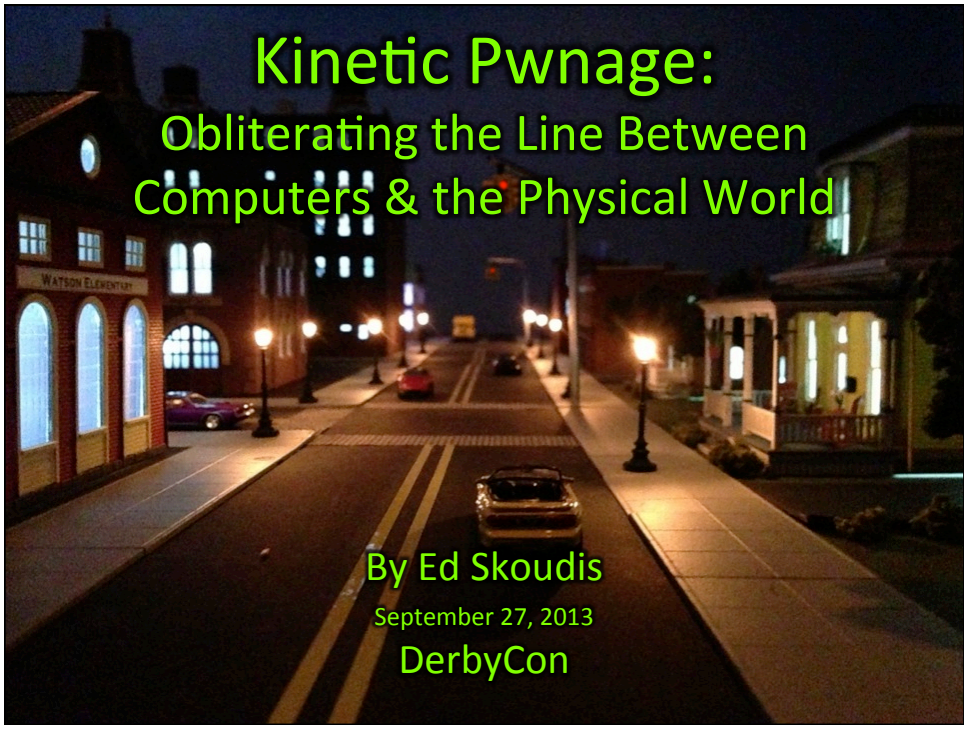


$ cut -f5 -d: /etc/passwd | grep -i skoudis

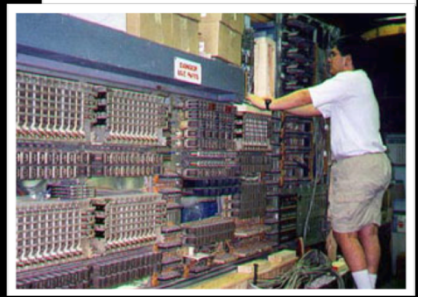
- Ed Skoudis - Started infosec career at Bellcore
- @edskoudis & ed@counterhack.com
- SANS Instructor and Author – 504 & 560
- Counter Hack Founder: Director of Cyber Foundations, Cyber Aces OnLine, Cyber Quests, NetWars, & CyberCity
- Researcher - Malware, Virtual Machines, Cyber Warfare Strategies and Tactics, Penetration Testing
- Blogger - CommandLineKungFu.com & pen-testing.sans.org/blog
- Books - *Counter Hack Reloaded* & *Malware: Fighting Malicious Code*

Outline

- A bit of historical grounding
- Central thesis
- Why is this so?
- Some implications
- The CyberCity project
- A (brief) manifesto
- A call to action – getting involved
- Conclusions

MIT's Tech Model Railroad Club

- Hacking didn't all begin with phones
  - Sorry, my phreaking friends
- Starting in 1946, hackers built an elaborate, machine-controlled train set!
  - The TMRC helped establish the hacker ethos and culture
- "*The TMRC layout was never very scenic. This being MIT, more efforts were focused on control systems than on scenery.*" – TMRC History
- Detailed beautifully in Steven Levy's book *Hackers: Heroes of the Computer Revolution*



Central Thesis

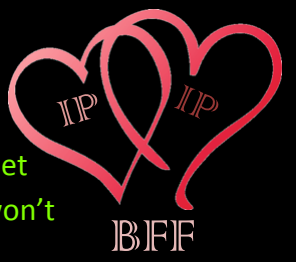
- We are entering the golden age of hacking software *and* hardware to achieve physical impacts
  - The hacker movement meets the maker movement
    - "Hardware is the new software" - Joe Grand
    - "Hack all the things" – Dual Core
  - Embedded systems, "Internet of things", wireless, mobile, "there's an app for that", jail-breaking, and hobbyist culture all combine to lead to AMAZING times for the hacking community and the world
- This is awesome, yet dangerous
  - Lots of opportunity for great research
  - Risk of people getting seriously hurt or killed
  - Is the infosec community ready to defend against this challenge?

Recent Talks at Hacker Conferences and Security Events

- HiTB Amsterdam 2013: Remotely hacking airplanes (controversy about realism and applicability, but still…)
- Defcon 2012: Talk on hacking trains in Spain
- Defcon 2013: Charlie Miller & Chris Valasek on hacking automobiles
  - Control car functions like steering & breaks via CAN
  - Additional 2012 research on wirelessly accessing car

IP Everywhere

- We are growing ever nearer to the dream of having everything IP addressable
  - Baby cams, thermostats, refrigerators, home automation…
  - Cash registers, grocery stores, shopping malls, commerce…
  - Critical electrical, water, sewage infrastructures…
  - Industrial and military equipment…
- Interconnectivity provides more functionality and saves money
- Lotsa things are directly on the Internet
  - Thank you, Shodan, for illustrating that!
- But, it's worse than that
  - Something on an intranet… is on the Internet
- And, even if it is on a *separate* IP network, it won't be separate forever

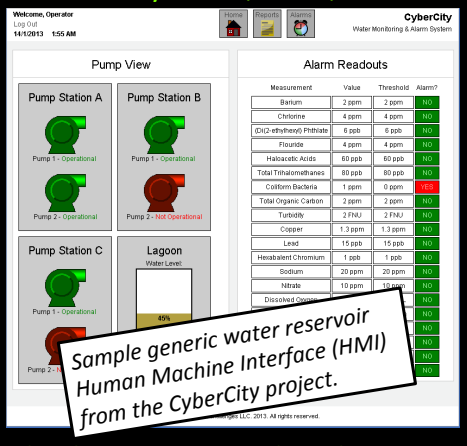


Air Gaps Will Save Us! NOT

- Proposed solution? Just air gap all the scary things
  - Get your wire cutters ready!
- But, air gaps disappear over time
- The person in your job after you won't understand the importance of your brilliant air gap
  - And the bean counters will likely never understand it
- Remember: IP loves IP and craves interconnectivity
  - Wireless exacerbates this, but it's also a wired issue
- If your security model depends solely on your system being air gapped, you will get pwned
  - And you may deserve to as well

Web Apps Everywhere

- WEBIFY OR DIE!
  - Security equipment: endpoint security suites, VPNs, vuln scanners, and more
  - HVAC systems
  - Power grid controls
  - Smart meters
  - Water systems
  - Automotive systems
- It's all web-enabled
- XSS, SQLi, XSRF, RFI, Command Injection, etc.
- To say nothing of pwning the box running the client
- WEBIFY *AND* DIE?

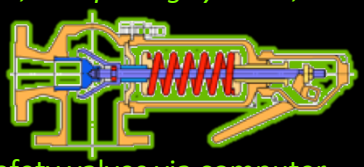


Infiltrating Operations Technology (OT) Environments

- "Is your OT environment connected to the Internet?"
  - Utility: "No. It isn't directly connected to the Internet."
- But, outbound access = inbound command and control
- Plentiful opportunities for jumping between utility IT environment and OT environment, for example:
  - ICS → Data Historian → Common Database on OT network → Replica on IT network → Workstation → Internet
  - Smart Phone → HMI PC → Pwnage
  - OT systems → DNS → IT environment → Internet
- See also: Stuxnet & USB

Overcoming Physical Limits and Human Checks

- Sometimes, we hear:
  - *"But, there are physical controls which override automated computer controls, like pressure valves, dampening systems, etc."*
  - *"And, we've got humans in the loop to stop bad things"*



- Four responses:
  - Purposely triggering those physical safety valves via computer action could be hugely harmful itself
  - The "physical" controls themselves are increasingly being computerized, so some aren't really physical at all any more
  - For low-cost operations of remote equipment, operators are increasingly far away, controlling things via IP networks and HMIs
  - By manipulating HMIs, attackers could trick human operators

Three Areas of Major Concern

1. Power grid
   - The mother of all critical infrastructures
2. Healthcare environments
   - Hospital systems
   - Medical devices
3. Weapons Systems
   - Disablement to neutralize them
   - Turning them on their owners and operators

- There are other areas as well (telecommunication, chemical production, aviation, etc.), but those listed above are a primary concern of mine

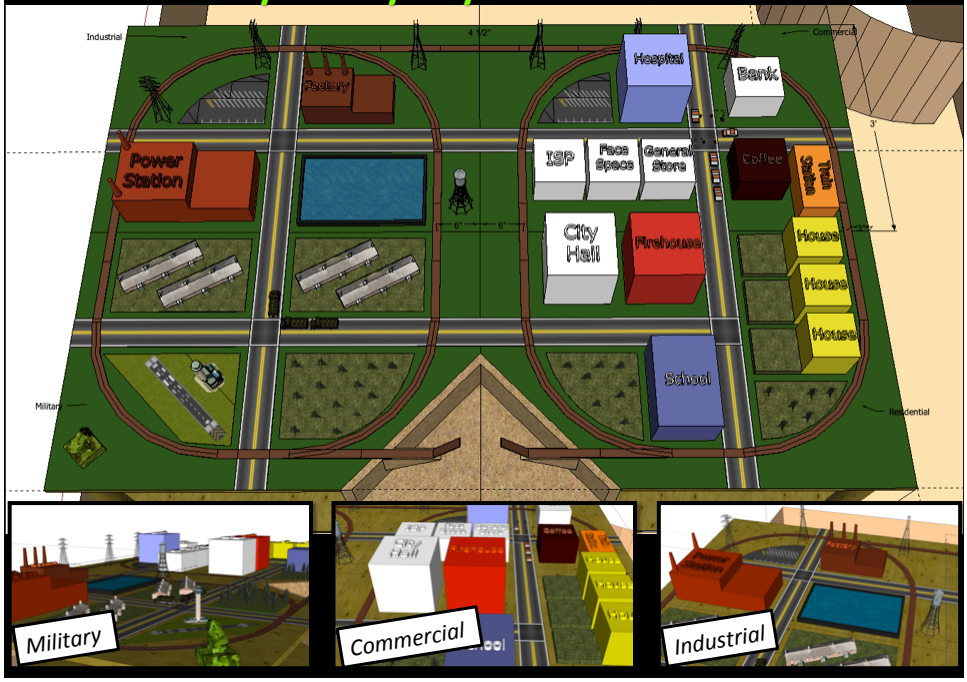
CyberCity: A Kinetic Impact Range

- If serious manipulation of the kinetic infrastructure is possible or inevitable, wouldn't it be cool to build a research platform, test bed, and training environment for it?
- Goal: Help defenders, cyber warriors, military leadership, and planners understand that cyber action can have kinetic impacts
- NetWars CyberCity was built to achieve this goal
  - A miniature city, 6' X 8', with a variety of kinetic assets
    - SCADA-controlled power grid, traffic system, water reservoir, train system, rocket launcher, etc.
    - ISP, hospital, bank, coffee shop, etc.
  - Participants (.mil, .gov, .com, .edu) are challenged to complete missions
  - Real-time streaming video to visualize kinetic impacts

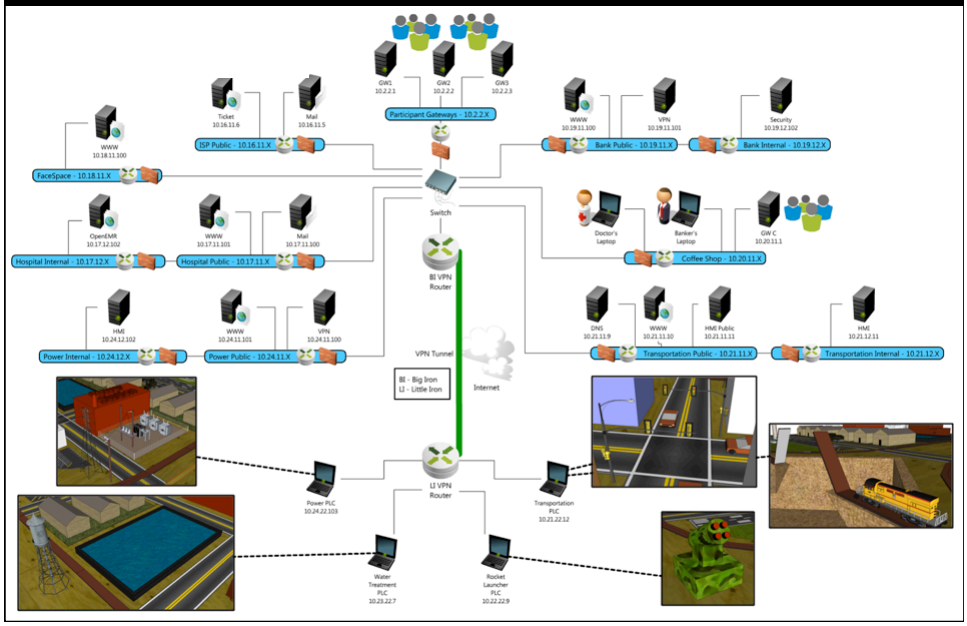
Props to Some Thought Leaders

- Several people have helped inspire and provided input to the CyberCity project:
  - Skip Runyan, US Air Force
  - Mike Assante, NBISE (current) & NERC (formerly)
  - Terry McCorkle, Technical Director at Cylance
  - Billy Rios, Technical Director at Cylance
  - Rita A. Wells, Idaho National Laboratory
  - Eric Bassel, SANS Institute
- CyberCity was built by Josh Wright, Yori Kvitchko, Tim Medin, Tom Hessman, and Ed Skoudis

CyberCity Physical Overview



CyberCity Network Overview



Sample CyberCity Missions

- Power Grid: Recover control of terrorist-compromised electric utility
- Transportation: Fix traffic lights after attackers turn them all green to cause mayhem
- Water reservoir: Ensure HMI properly reflects water quality so humans take proper actions
- Train system: Stop weapon egress by controlling rail system switches
- Weapons system: Prevent missile strike against commercial sector by gaining control of weapon and re-aiming it to fire harmlessly

MISSION: POSSIBLE

CyberCity Commercial Quadrant

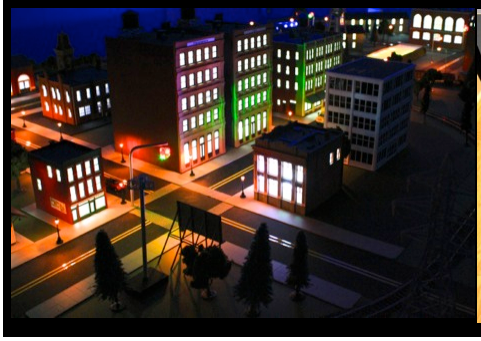
CyberCity Military Quadrant

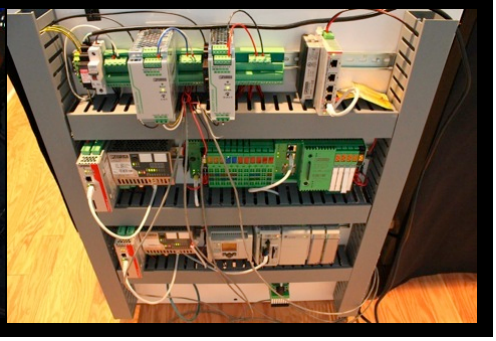
CyberCity Industrial Quadrant

CyberCity Residential Quadrant

CyberCity Power Grid

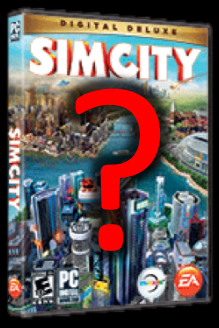
- Currently focused on distribution, not generation (yet)
- Each CyberCity quadrant has its own PLC
  - Allen-Bradley, GE, and Siemens
  - Controls residential and industrial lighting (building by building), street lighting (quad by quad), and railway switch junctions
- Wonderware HMI running on Win7 and WinXP
- Protocols: Modbus/TCP, DNP3, Profinet, Ethernet/IP





Why Not Simulate EVERYTHING?

- A frequent question – Just make SIM City on steroids, simulating everything including video
- Two problems with that approach:
  - Costs of doing it well – video game budgets are $$$$
  - Some in the military would dismiss it as not being "real"
- We can achieve reasonably realistic results using real equipment at lower costs
  - And, make a point about actual kinetic impacts of computer and network actions
- There is an art to deciding what to make real and what to virtualize



CyberCity Lessons Learned

- Everything we've deployed is far weaker than we expect
  - Vulnerabilities abound
  - XSS, SQLi, buffer overflows, cleartext protocols & more
- Hospital systems, Industrial Control Systems, and more
  - We've had to harden or even recode some things or else they are too trivial for a CtF mission…
  - Or, too brittle, just falling over constantly
- These components just haven't gotten the scrutiny that traditional IT systems have had… but they must get it now
- Huge issues with responsible disclosure and vendors not understanding the issues or impact - delightful

Why Haven't We Seen Massive Kinetic Impact… Yet?

- If kinetic damage via cyber attack is possible, why haven't we seen much of it to date?
- Many possible reasons:
  - Lack of effective criminal business model
    - Cyber criminals can't easily turn this into cash
    - World of hurt from law enforcement (or .mil) in this type of extortion
  - The geo-politics
    - It is in no one's interest to bring things down… right now
    - This could change instantly
  - It's harder than is anticipated
    - Skills for this type of attack are emerging and aren't yet widespread
- But, the battlefield is being prepped
  - Malware assets have been discovered, planted for long-term command and control inside critical infrastructure

The Bottom Line

- Over the last 25 years, we've done a horrible job of securing data and computer systems
  - Breaches, breaches, breaches
    - Rampant information theft, from PII to PHI to state secrets
    - From hobbyists to activists to criminals to nation state pros
  - Denial of Service is also a recurring problem
- If we don't do better securing computer control of kinetic infrastructures:
  - The Internet(s) will grow ever more militarized
  - People may get hurt
  - People may get killed

A Brief Manifesto: Vigorously Apply Our Lessons Learned

- We've had decades of learning how *not* to secure computers to protect data
- Defense in-depth, segmentation, filtering, strong authentication… resilient infrastructures are a MUST or, even better, anti-fragile infrastructures
- Design, design, design! Build security in from the start
- Testing, testing, testing! Quality assurance
- Responsible disclosure more important now than ever
  - And you'll get push back much harder than ever before
  - From vendors, interest groups, and others
  - Be responsible… but lawyer up! Props to the EFF

A Call To Action

- Start hacking all the things!
  - Responsibly, of course
  - Find and properly disclose flaws to help get fixes in place
- Pick an area, such as:
  - Power grid
  - Medical devices
  - Water control systems
  - Aviation

- Learn the foundational control protocols by deeply reading the specs
  - Example: Power grid – learn Modbus/TCP, DNP3, Profinet
  - Look for holes, options, and bad assumptions
  - In other words, view it like a hacker

Make Some Friends & Learn

- Read appropriate mailing list archives
- Subscribe to a mailing list
  - Lurk for a while
  - Who is who?
  - Learn the lingo
  - Focus on protocols, vendors, devices
- Reach out to like-minded people at a con
  - Attend talks on your chosen topic
  - Buy a speaker a drink
  - No talks? Have a Birds of a Feather session
- **Don't be intimidated – You DON'T need an EE degree to do useful work here**

And… Get Hacking

- Get real and practical: Procure some equipment
  - ***Get the manuals FIRST*** (might be free download or separate purchase)
  - eBay is your friend! So is PLCCenter (www.plccenter.com)
  - You may be able to get some interesting devices for < US $500
- Examples of items we have in CyberCity:
  - Siemens PLC Starter Kit, S7-1200 PLC
  - Allen Bradley L32 E Compact Logix Processor
- DO NOT ATTACK REAL PRODUCTION STUFF!

Sniff
- Wireshark & tcpdump
- Lots of dissectors
- You may need to create your own
- http://goo.gl/76k7c
- Great for learning
- Excellent experience

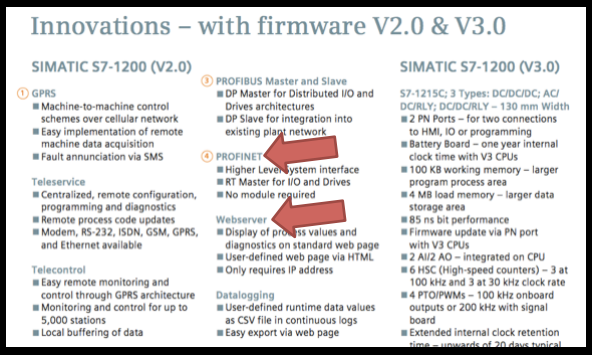
Inject
- Scapy
- Lots of protocols already defined
- You may need to create your own
- http://goo.gl/hJtxkK
- Excellent experience

Fuzz
- Sulley Fuzzer
- Peach Fuzzer
- Scapy extensions
- Good work going on in implementing fuzzers for common ICS protocols

About That Siemens Starter Kit

- Overview here: goo.gl/1M30TG
- Specs here: goo.gl/s0ajeF
- Buy 'em here: www.plccenter.com
- New Profinet scapy-based fuzzer by Dmitrijs Solovjovs & Tobias Leitenmaierhere: github.com/HSASec/ProFuzz

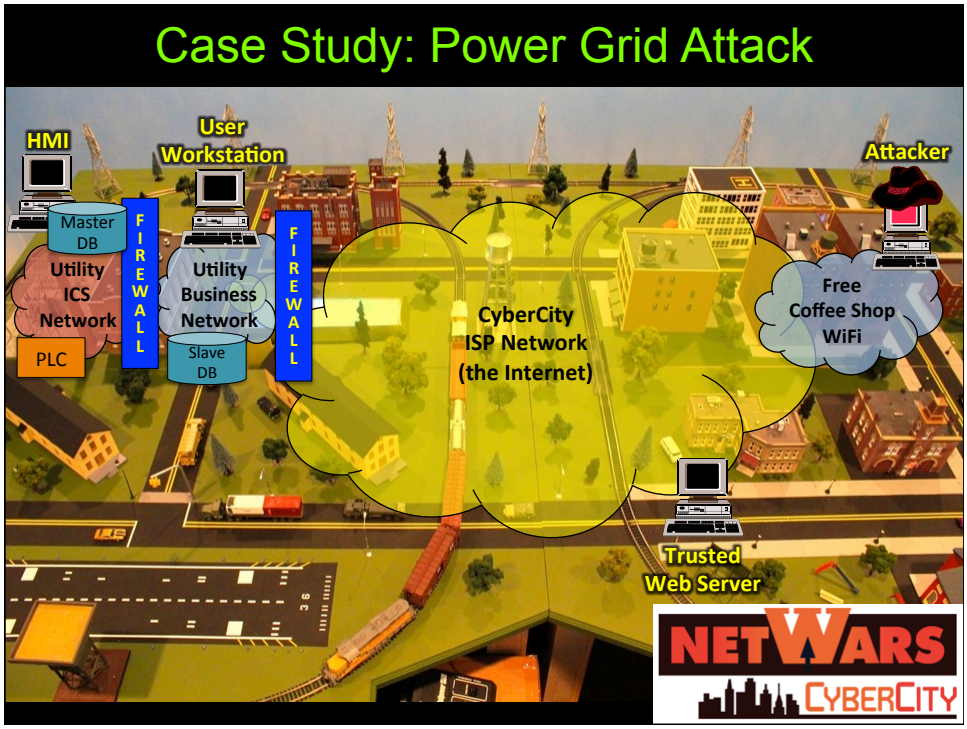
$ 430 NEW

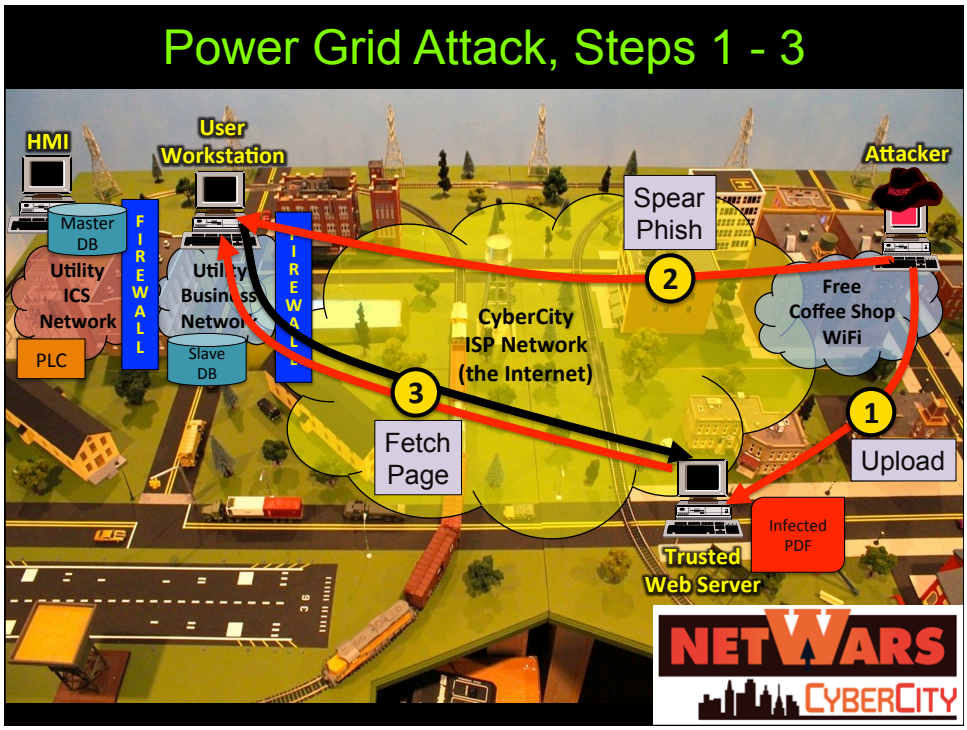


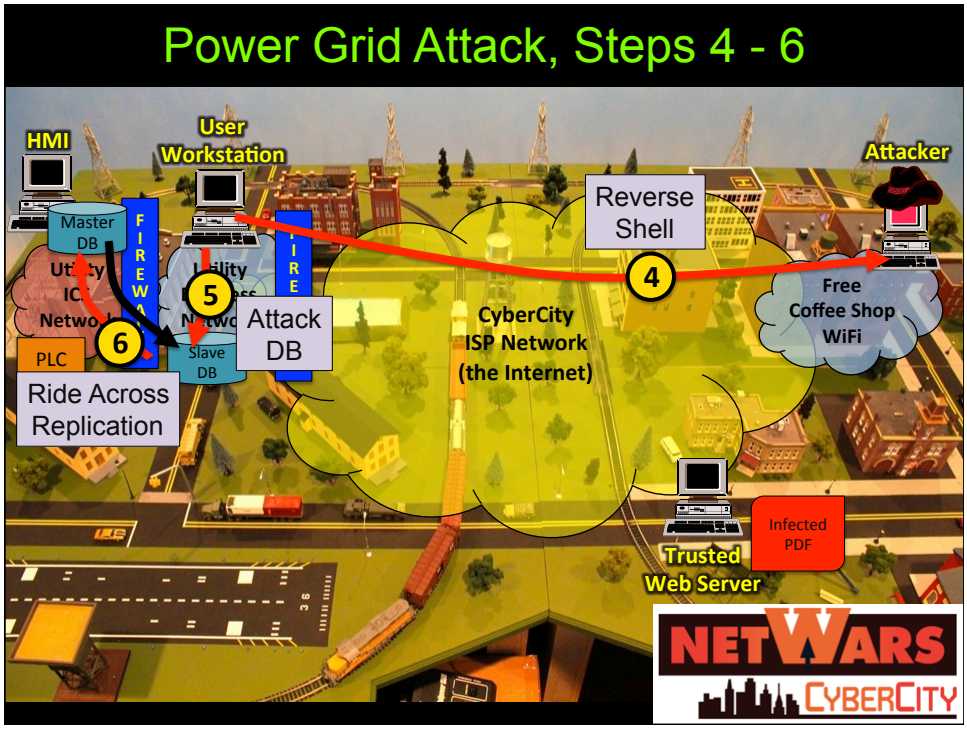
Conclusions: We've Come Full Circle

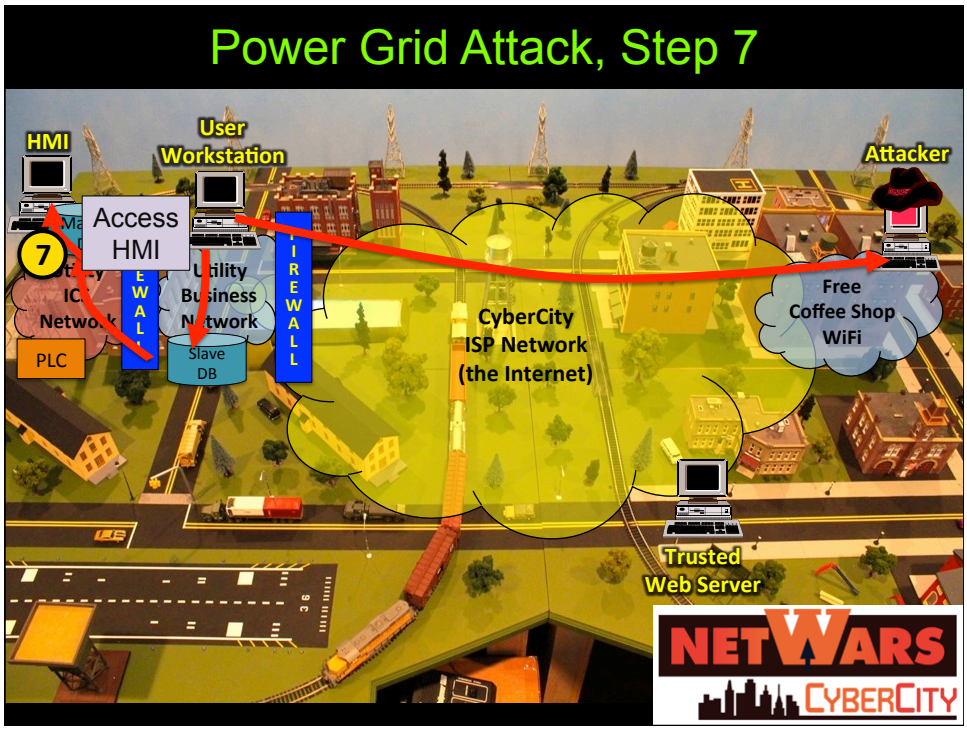
- MIT's Tech Model Railroad Club helped form the hacker ethic
  - They were a crucial early building block of the hacker community and our infosec industry
- Today, we're using train components to model kinetic impacts of major hacking incidents
- But, we as an industry have to really up our game, or else significant dangers await
- *There is a lot of work to do, but perhaps we were made hackers for just such a time as this*

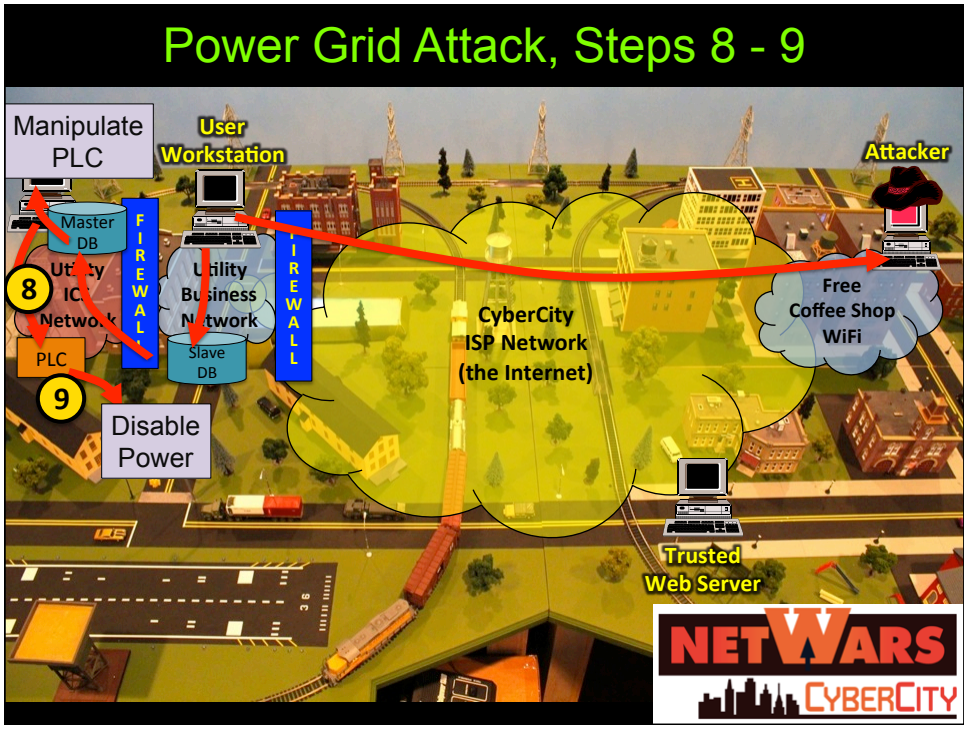
Case Study: Power Grid Attack


Case Study: Power Grid Attack
HMI
User Workstation
Attacker
Master DB
Utility ICS Network
PLC
FIREWALL
Utility Business Network
Slave DB
FIREWALL
CyberCity ISP Network (the Internet)
Free Coffee Shop WiFi
Trusted Web Server
NETWARS
CYBERCITY


Power Grid Attack, Steps 1 - 3
HMI
User Workstation
Attacker
Master DB
Utility ICS Network
PLC
FIREWALL
Slave DB
FIREWALL
Spear Phish
2
CyberCity ISP Network (the Internet)
Free Coffee Shop WiFi
3
Fetch Page
1
Upload
Infected PDF
Trusted Web Server
NETWARS
CYBERCITY


Power Grid Attack, Steps 4 - 6
HMI
User Workstation
Attacker
Master DB
Reverse Shell
4
5
Attack DB
6
PLC
Slave DB
Ride Across Replication
CyberCity ISP Network (the Internet)
Free Coffee Shop WiFi
Infected PDF
Trusted Web Server
NETWARS
CYBERCITY


Power Grid Attack, Step 7
HMI
User Workstation
Attacker
Access HMI
7
Slave DB
PLC
CyberCity ISP Network (the Internet)
Free Coffee Shop WiFi
Trusted Web Server
NETWARS
CYBERCITY


Power Grid Attack, Steps 8 - 9
Manipulate PLC
User Workstation
Attacker
Master DB
FIREWALL
Utility Business Network
FIREWALL
8
PLC
Slave DB
9
Disable Power
CyberCity ISP Network (the Internet)
Free Coffee Shop WiFi
Trusted Web Server
NETWARS
CYBERCITY