Security in knowledge

The Five Most Dangerous New Attack Techniques and What's Coming Next

Alan Paller

SANS

And SANS Technology Institute

Ed Skoudis

Counter Hack Challenges

And SANS Technology Institute

Johannes Ullrich

SANS Internet Storm Center

And SANS Technology Institute

RSA CONFERENCE 2013

Session ID: EXP-W22

Session Classification: Advanced

Ed Skoudis

Author of *Counter Hack Reloaded* and *Malware* books

Creator of NetWars and CyberCity

Security in knowledge

2012 Headlines

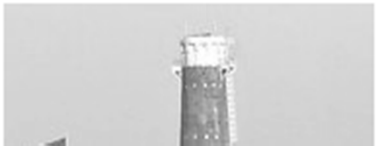
- Stuxnet
- Flame
- Gauss
- Olympic Games operation(s)
- Shamoon

The New York Times

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 360 Comments

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.



Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
REPRINTS

Skoudis Top New Threats / Attacks

- **Increasing militarization of cyber space**

The rise of offensive forensics and purposeful misattribution

Computer attacks resulting in kinetic impact

Cyber Space as a War-Fighting Domain

- Humans wage war in the domains we occupy
  - Land, Sea, Air, and Space
  - Cyber space, which actually now overlays and controls action in all of the other domains
- Military objectives are achievable via cyber means, often at lower cost and lower ***potential*** physical risk than traditional military strikes
- Governments around the world increasing their budgets for cyber operations, and we've glimpsed some of the results
- But, consider Sherman's warnings
  - "War is hell."
  - "Every attempt to make war easy and safe will result in humiliation and disaster."

A Prediction & Interesting Quotation

- Prediction: Every military mission will have a cyber component in the near future (or now)
  - At least defensive
- Aug 24, 2012 Washington Post contains quote from Marine Lt. General Richard P. Mills:
- *"I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact."*
- *"I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."*

The Washington Post | Politics | Opinions | Local | Sports | National

NATIONAL

US general says his forces carried out cyberattacks on opponents in Afghanistan

Gerald Herbert, file/Associated Press - File - USMC Lt. Gen. Richard Mills speaks during christening ceremonies for the USS Somerset at the Huntington Ingalls Industries shipyard Shipyard in Avondale, La., in this Saturday, July 28, 2012 file photo. The U.S. military has been launching cyberattacks against its opponents in Afghanistan, a senior officer said last week, making an unusually explicit acknowledgment of the oft-hidden

Skoudis Top New Threats / Attacks

Increasing militarization of cyber space

- **The rise of offensive forensics and purposeful misattribution**

  Computer attacks resulting in kinetic impact

The Rise of Offensive Forensics

- Digital forensics has traditionally been a defensive and reactive art
- But, we are starting to see the rise of offensive forensics (not merely anti-forensics)
  - Anti-forensics makes forensics analysis hard – destroying or manipulating evidence… offensive forensics is different
  - Offensive forensics applies forensics techniques to find info assets and extract them (with some anti-forensics mixed in)
  - Large-scale exfiltration may get you noticed, so there is real value in quietly finding the asset you need

Mis-Attribution

- Given that attribution of one malware asset could lead to attribution of other missions and the revelation of a given actor (cascading attribution)…
- The art of misattribution rises in importance
- How can you make malware assets that look like someone else created them?
  - Put language and other references for another culture
  - Add deliberate but unimportant errors in your work
    - Shamoon malware that targeted Saudi Aramco had several flaws: Date check, malfunctioning dropper, etc. -- Therefore, it couldn't have been a nation state
  - The more blatant it is, the more questions and confusion it will raise

Skoudis Top New Threats / Attacks

Increasing militarization of cyber space

The rise of offensive forensics and purposeful misattribution

- **Computer attacks resulting in kinetic impact**

Cyber Action for Kinetic Impact

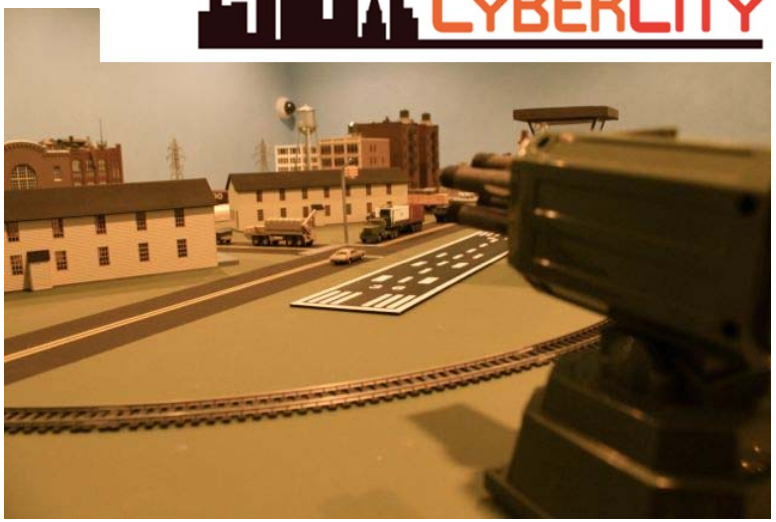
- Historically, a lot of computer security work focused on protecting sensitive information
  - PII, PHI, bank records, trade secrets, etc.
  - Even in a national security context, most discussions focused on protecting classified information against espionage and isolating networks
- But, increasingly, attackers are targeting computers and networks that control real-world equipment and devices
  - Industrial Control Systems and SCADA equipment
  - Other control systems – traffic systems, transportation systems, etc.
  - Some activity is mere mischief
  - Other attacks are a concerning sign of things to come
- Buffer overflows, shared passwords, and not-really-air-gapped networks abound

Some Noteworthy Events

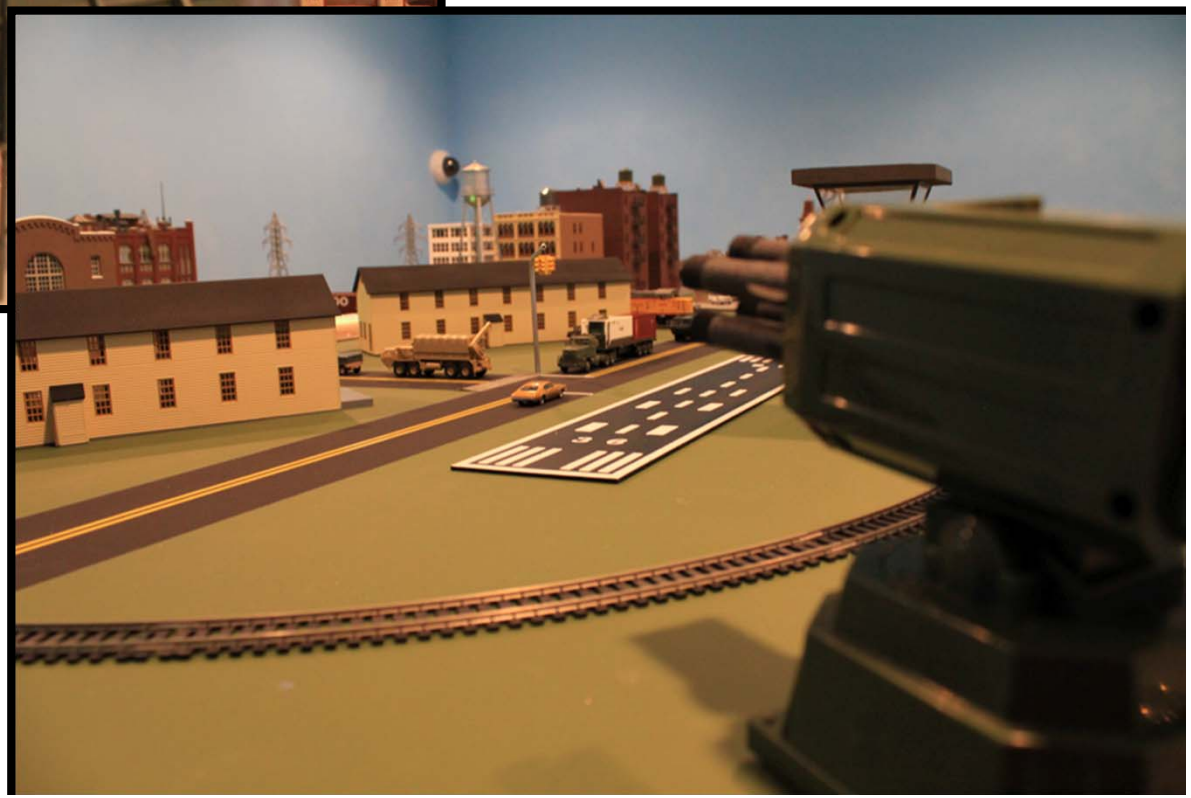
- Nov 2011: Water systems hacked in Illinois, pump disabled by repeatedly turning it off and on
- Dec 2011: TSA reports hacks against commuter trains in Pacific Northwest resulted in delays
- 2012: Hacks against smart meters used for millions of dollars of fraud
- 2012: Presentations at DefCon and elsewhere on hacking into commuter train system comms gear
- Infiltration of electric utility systems has been observed for many years
- In protecting critical information assets, our track record as an industry is a concern
- We live in an age of Wikileaks… we are rapidly moving to an age of cyber attack to cause kinetic impact

Preparing Cyber Warriors

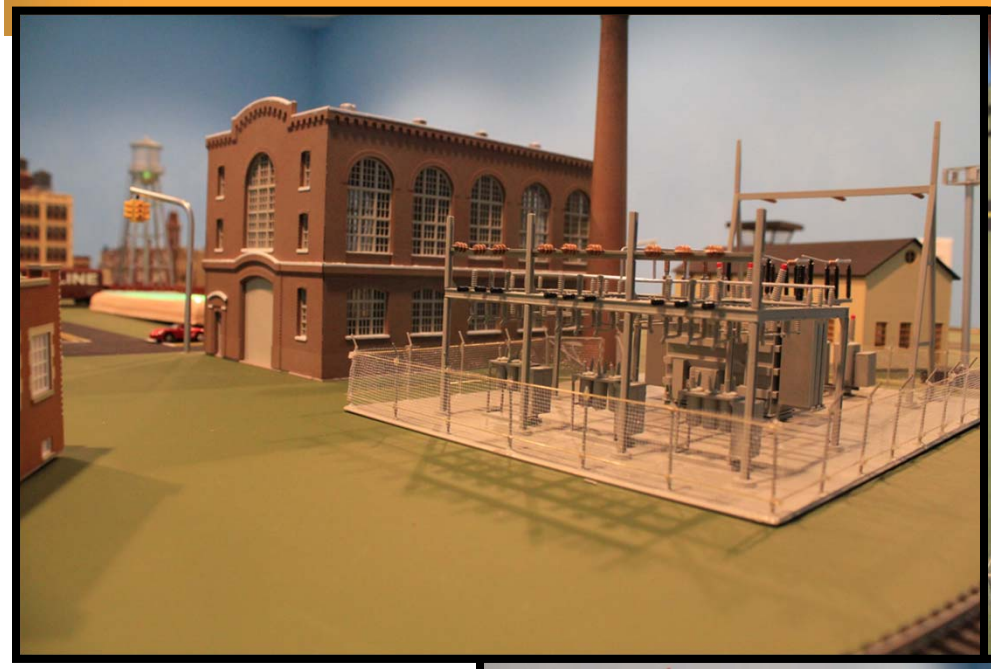
- Goal: Help cyber warriors, their leadership, military planners, and defenders understand that cyber action can have kinetic effect, and that they can master this technology
- NetWars CyberCity was built to achieve this goal
  - A miniature city, 6′ X 8′, with a variety of kinetic assets
    - SCADA-controlled power grid, traffic system, water reservoir, train system, rocket launcher, etc.
    - ISP, hospital, bank, coffee shop, etc.
  - Cyber warriors (.mil, .gov, .com) are challenged to complete missions
  - Real-time streaming video to visualize kinetic impacts



CyberCity Commercial & Military Quadrants



CyberCity Industrial Quadrant



CyberCity's Power Grid

- Currently focused on distribution
  - We will model generation in the near future
- Each quadrant of CyberCity has its own PLC (Programmable Logic Controller)
  - Allen-Bradley, GE, Siemens, and possibly others
  - Controlling residential and industrial lighting, street lighting, and railway switch junctions
- Wonderware HMI running on Win7 and WinXP for management
- Various Operator Interface Terminals (OITs)
- Protocols: Modbus/TCP, DNP3, Profinet, Ethernet/IP
- We carry wireless across highly attenuated wires and within small-scale Faraday cages
  - For power grid components and coffee shop free Wifi

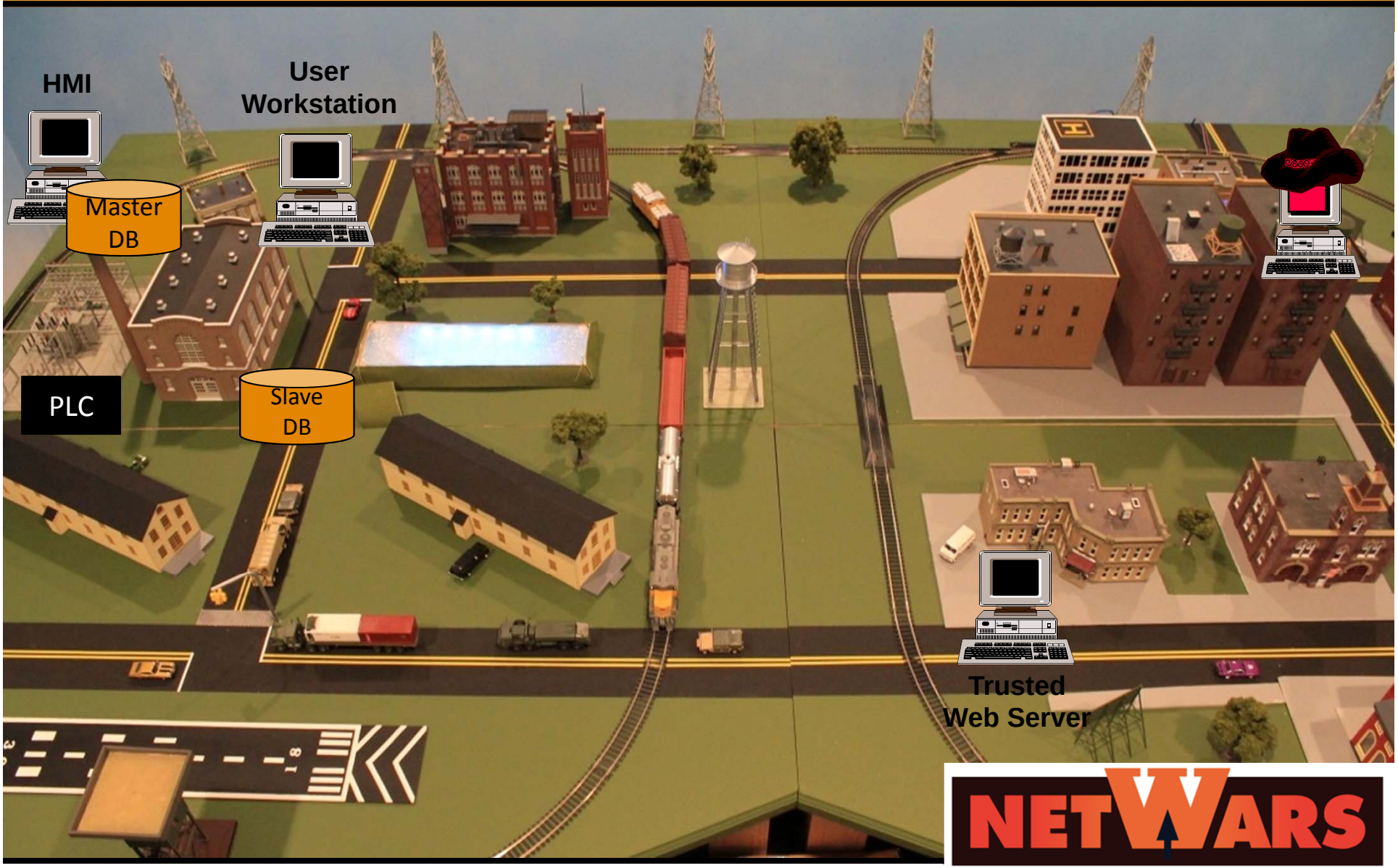
Thought Leaders

- 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

Case Study: Visualizing Real-World Attacks

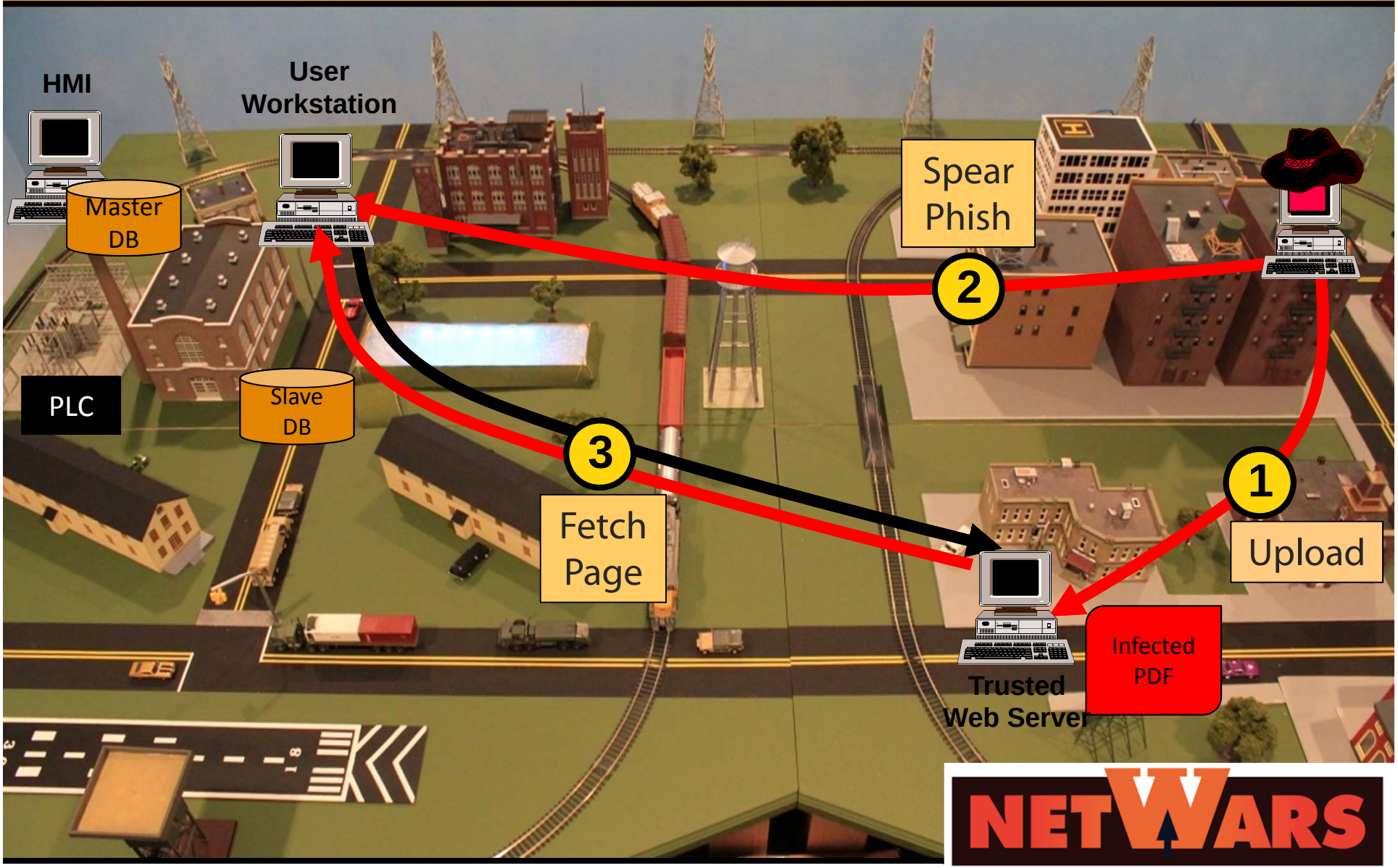
Let's walk through a real-world case study of an actual power grid attack.

Case Study: Power Grid Attack



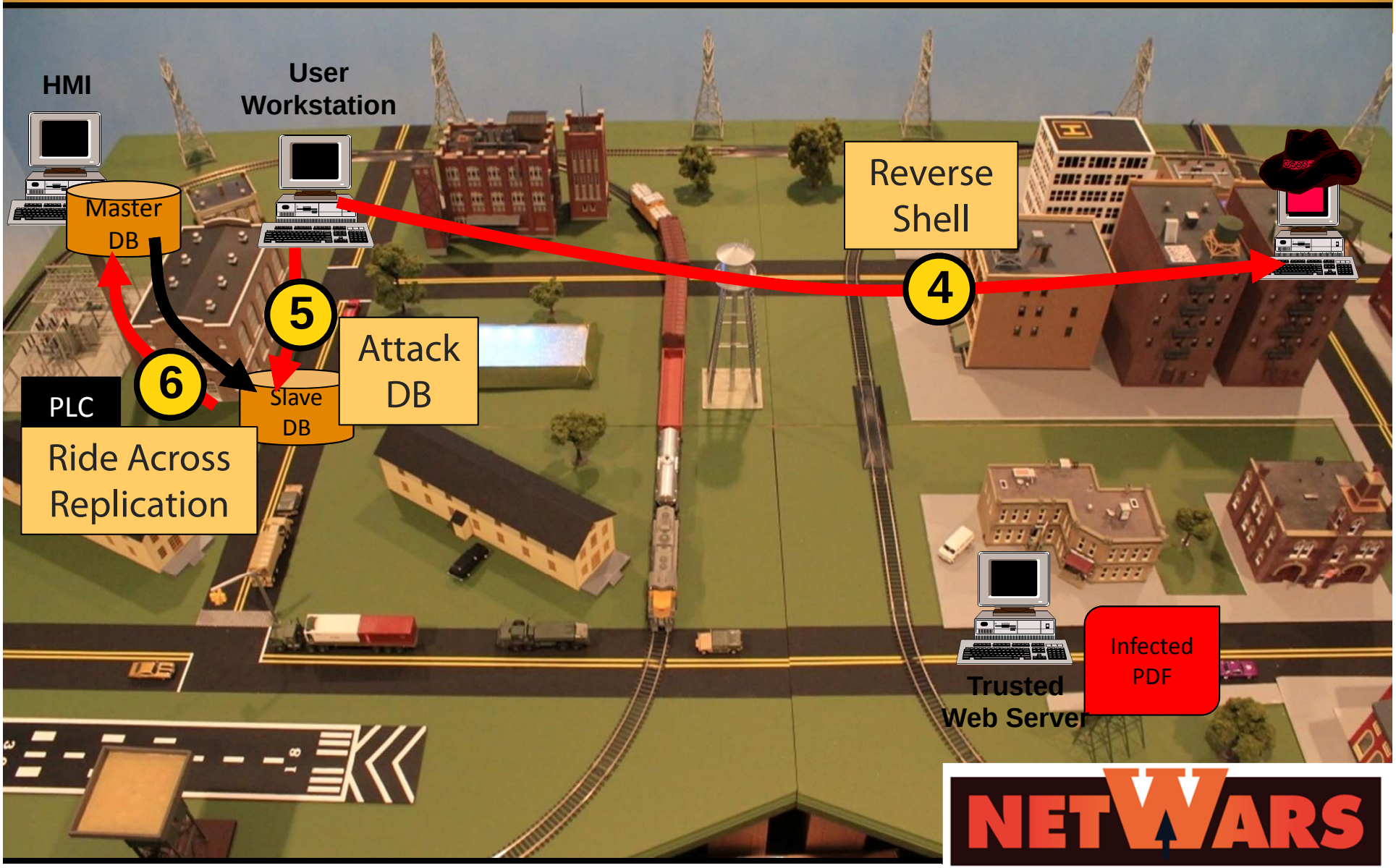
NETWARS CYBERCITY

Case Study: Power Grid Attack Steps 1-3



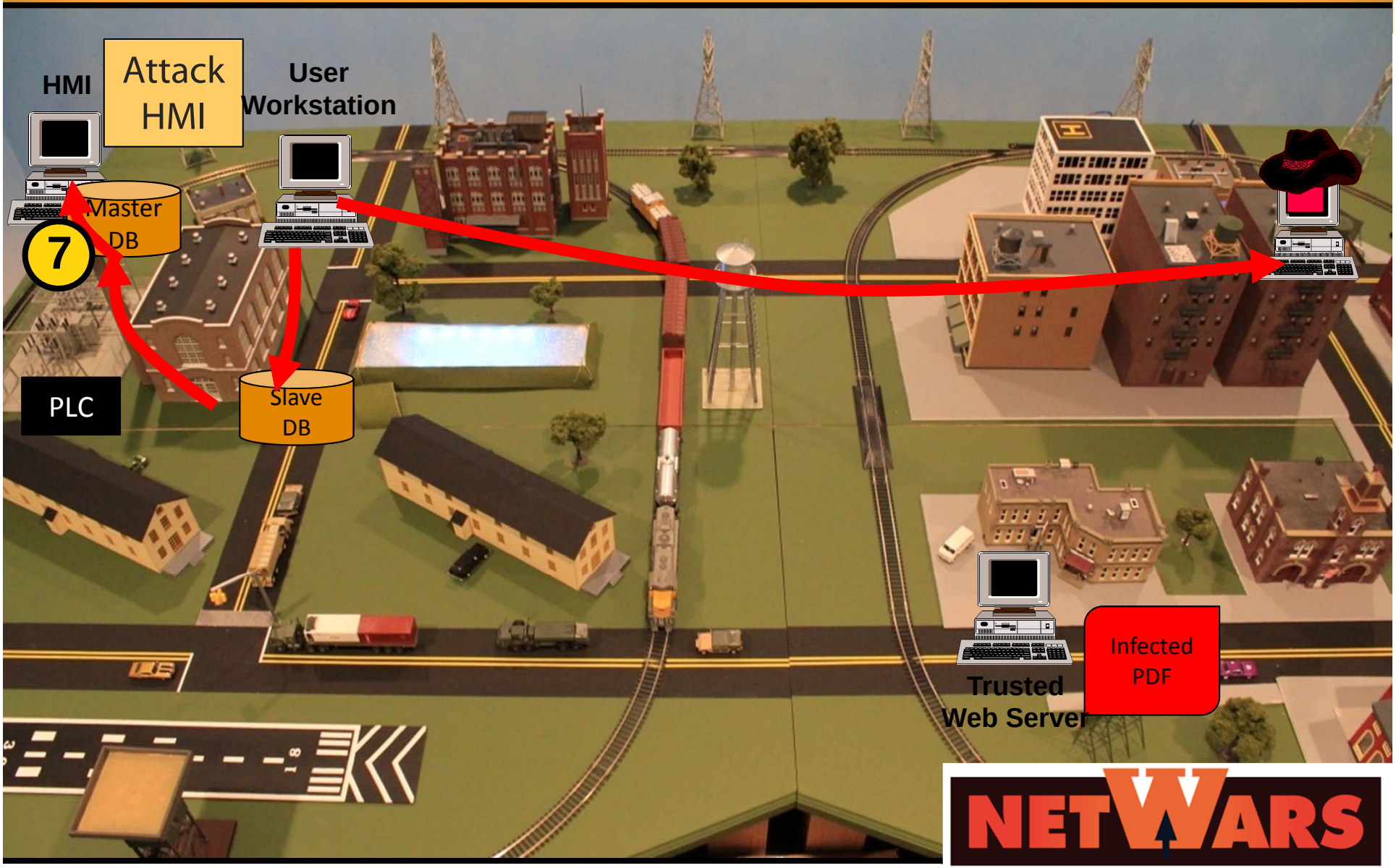
NETWARS CYBERCITY

Case Study: Power Grid Attack Steps 4-6



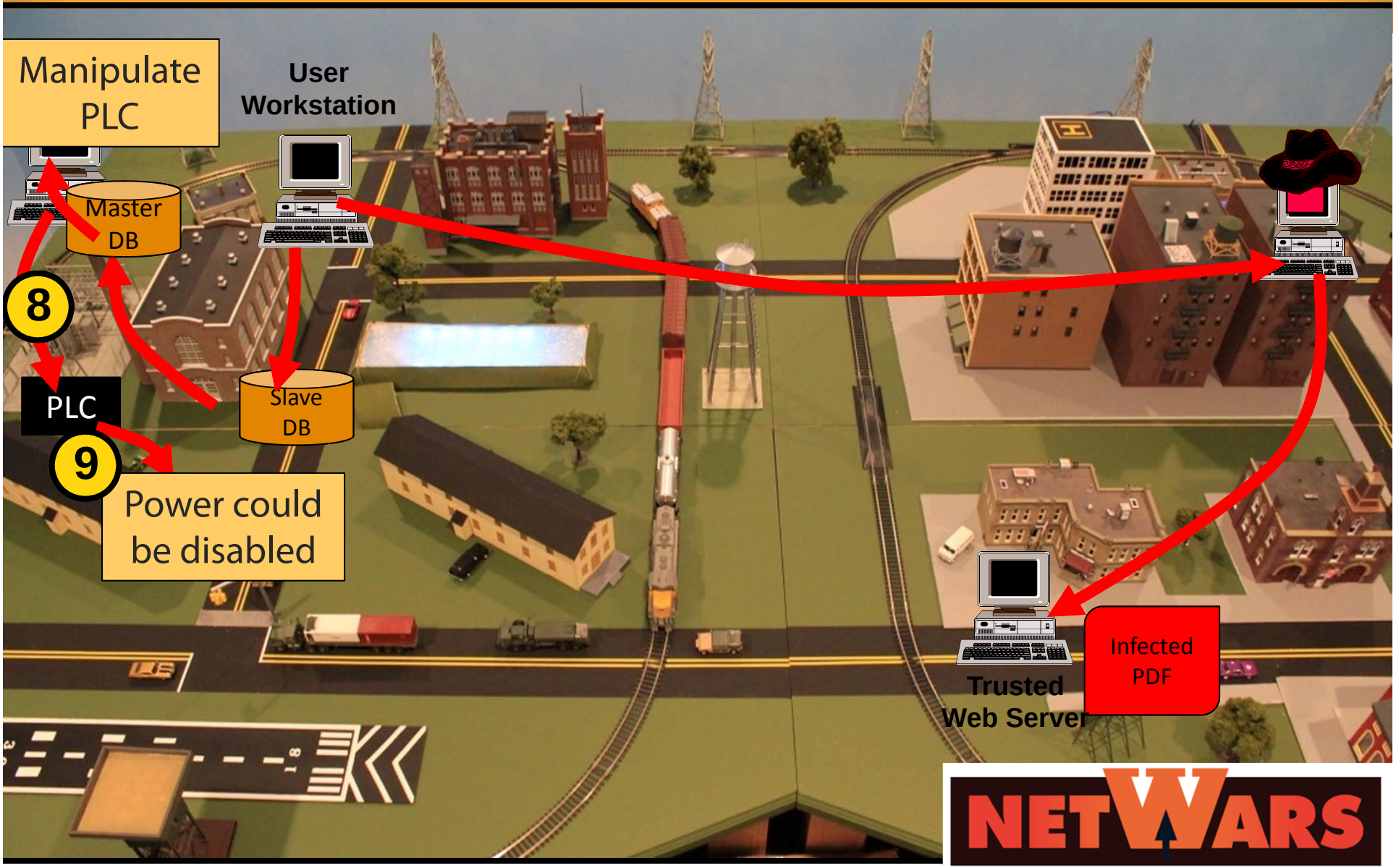
NETWARS CYBERCITY

Case Study: Power Grid Attack Steps 7



NETWARS CYBERCITY

Case Study: Power Grid Attack Step 8-9



NETWARS CYBERCITY

An Interlude:
Alan Paller
Director of Research at the SANS Institute

Security in knowledge

Surprising data affects cyber careers

- **Four Controls stop targeted attacks**
  - CEOs really like people who can prove what needs to be done first to solve recognized, important problems.
  - No cyber problem is better recognized by senior executives than targeted attacks
  - There is hard evidence from multiple sources that 4 controls stop these attacks.
  - A 10 organization pilot is proving how effective with benchmarking
  - Get ahead of this opportunity for a career changer
  - Email apaller@sans.org "Top 4" for (1) controls, (2) how to implement them, (3) dashboard powerpoint, and (4) free testing tool sources.

Johannes Ullrich – Director of the SANS Internet Storm Center

Security in knowledge

ISC – How bad is it for the rest of us?

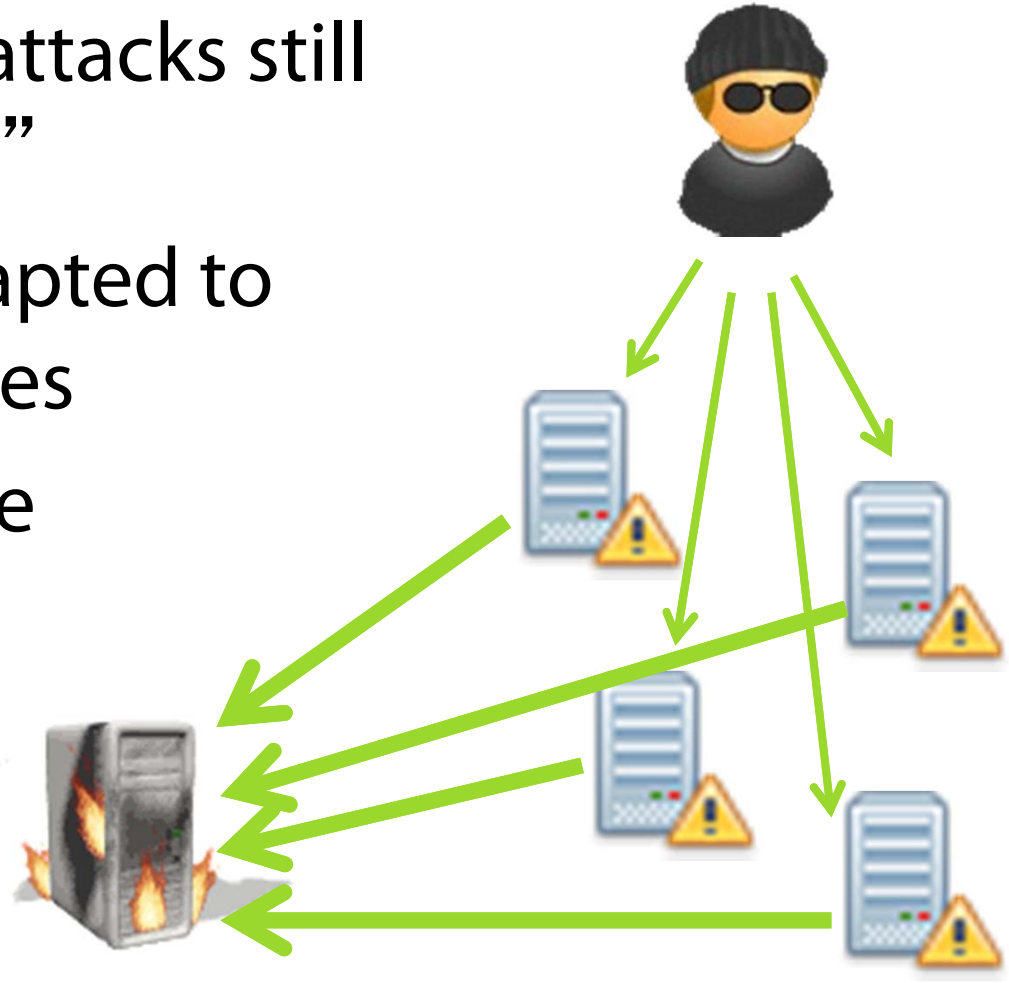
- News items tend to focus on high profile attacks
- Easy to forget that everybody is under attack, not just national/large assets
- Even if you are not direct under attack, you may be a tool in the plot to attack larger targets
- Attacks don't always require huge resources

Large DDoS Attacks

- Pretty much every large bank was a target in the last 12 months. Most several times.

How (and why) do they work

- Reflective DNS attacks still major “weapon”
- Tactics have adapted to counter measures
- Attacks are more intelligent and deadly



How Things Changes

- Defense

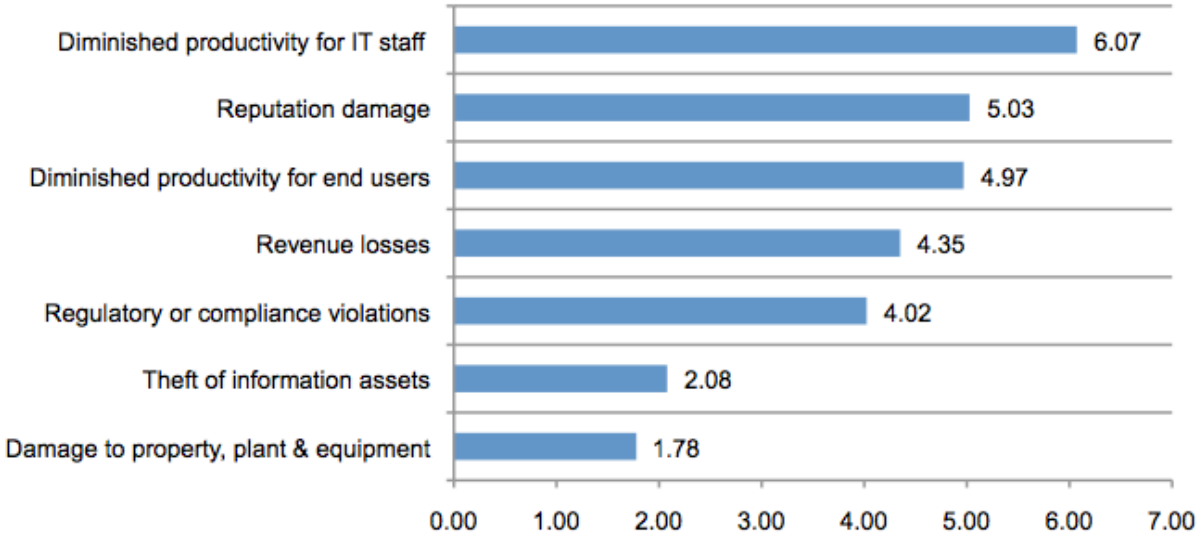
- Block DNS responses from servers that don't need to see them
- Only answer queries for which server is authoritative for
- Limit access to recursive name servers to internal users

- Offense

- Attacker uses queries for which server is authoritative
- Attacker compromises servers with substantial bandwidth
- Use of "ANY" queries
- Use of EDN0

Result

- Attacks reach 40+ gigabits/second
- Attacker only needs a 2,000+ servers
- Targets have to invest substantial resources to defend



Source: Ponemon Inst.

Password Breach / Hashing is Dead

- Old times: hash and salt your passwords, and you are good
- These days:
  - Use the right hash (hash? Bcrypt? SHAx? …)
  - Use salt correctly..

  And your passwords are still brute-forcable

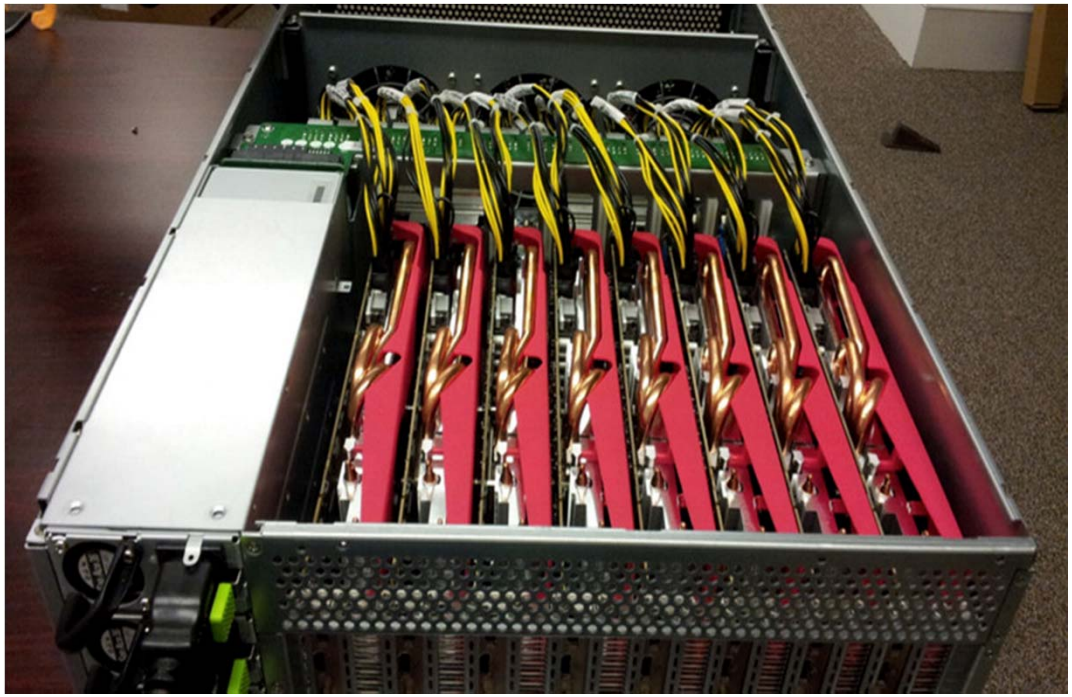
Your password is as secure as the least secure site you use it with!

Attackers have power!

25 GPUs
"affordable"
Dedicated hash
Cracker

63 G/s SHA1
180 G/s MD5
348 G/s NTLM

95% of leaked
LinkedIn Hashes
Cracked.



http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds/

Current Hardware vs Old Thinking

Algorithm	Iterations	Software	Hardware	Guesses Per Second
SHA-1	1	John the Ripper 1.7.9-jumbo6	Intel Core i7 990X	98,000,000
SHA-1	1	oclHashcat plus-0.09	4x AMD Radeon HD6690	15,500,000,000
sha512crypt	5,000	John the Ripper 1.7.9-jumbo6	Intel Core i7 990X	1,800
sha512crypt	5,000	John the Ripper 1.7.9-jumbo6	ATI Radeon HD5870	2,592
sha512crypt	5,000	John the Ripper 1.7.9-jumbo6	Nvidia GTX580	11,405
bcrypt	32	John the Ripper 1.7.9-jumbo6	Intel Core i7 990X	4,960
bcrypt	32	John the Ripper 1.7.9-jumbo6	ATI Radeon HD5870	1,745

http://securitynirvana.blogspot.com/2012/06/final-word-on-linkedin-leak.html

Solutions?

- User education: Use a different password, that you can't remember for every single site/software/company you interact with
- Oh… and please don't write it down!
- Developer education:

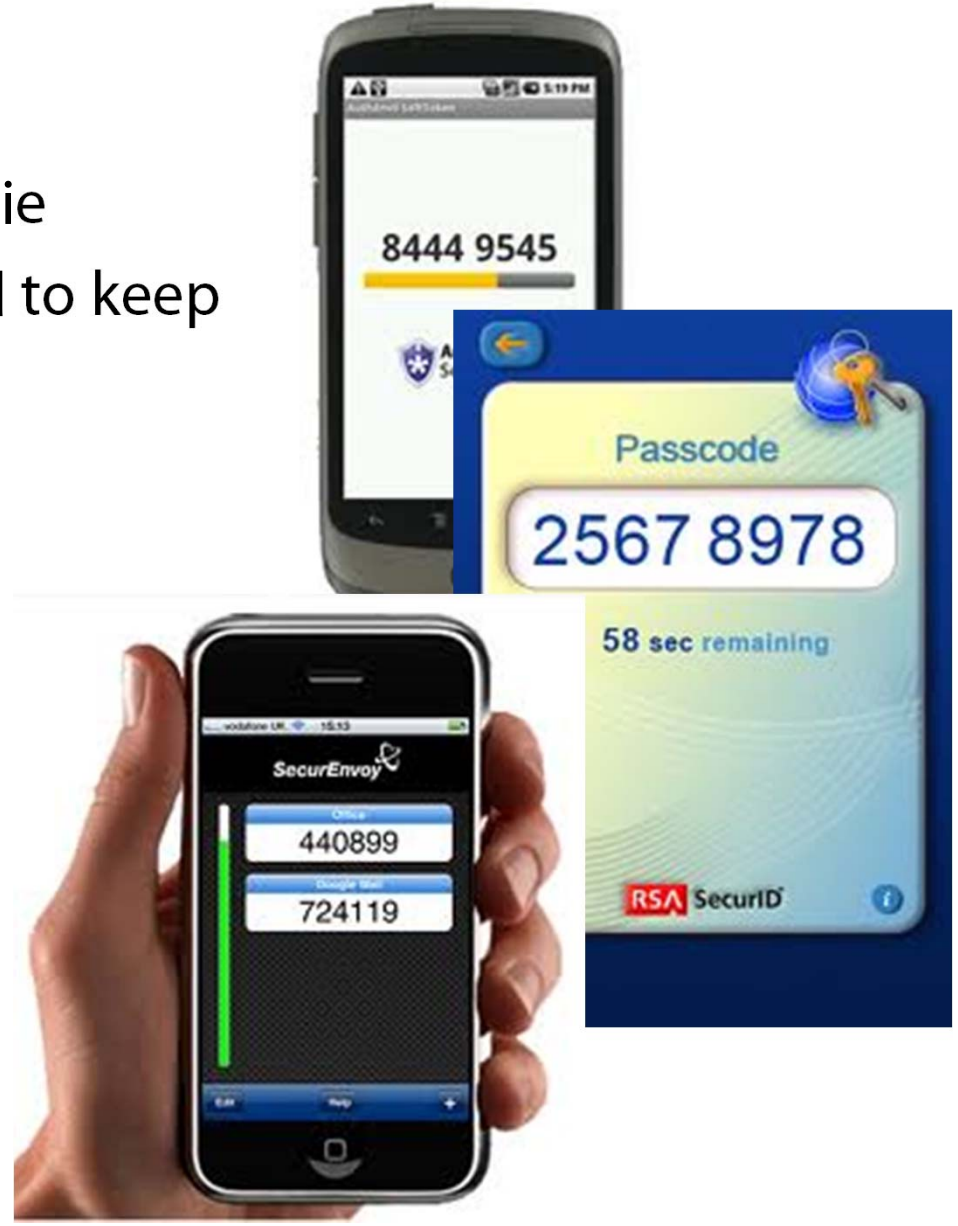
  Hashes are supposed to be efficient (SHAx).

  Password hashing is supposed to be slow

  Of course: Avoid losing your password hashes!

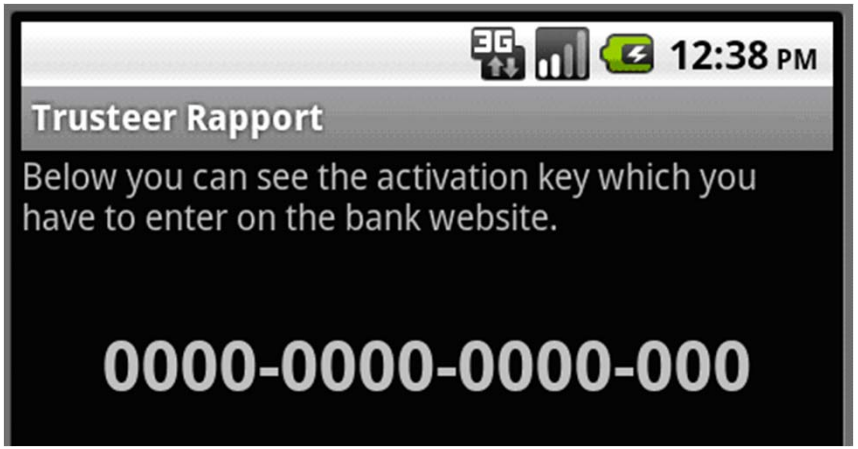
What's next?

- Passwords are dead
- Pass phrases are about to die
- Developers can't be trusted to keep our passwords secure!
- Two factor authentication is expensive
- **But everybody has a smartphone!**



Token Stealing Android Malware

- Zitmo/Eurograbber: brought to you by the same people that gave you Zeus.
- Defeats SMS based tokens
- Available even for Blackberry



Trusteer.com

Your questions and your ideas for the most dangerous new attacks???

Security in knowledge