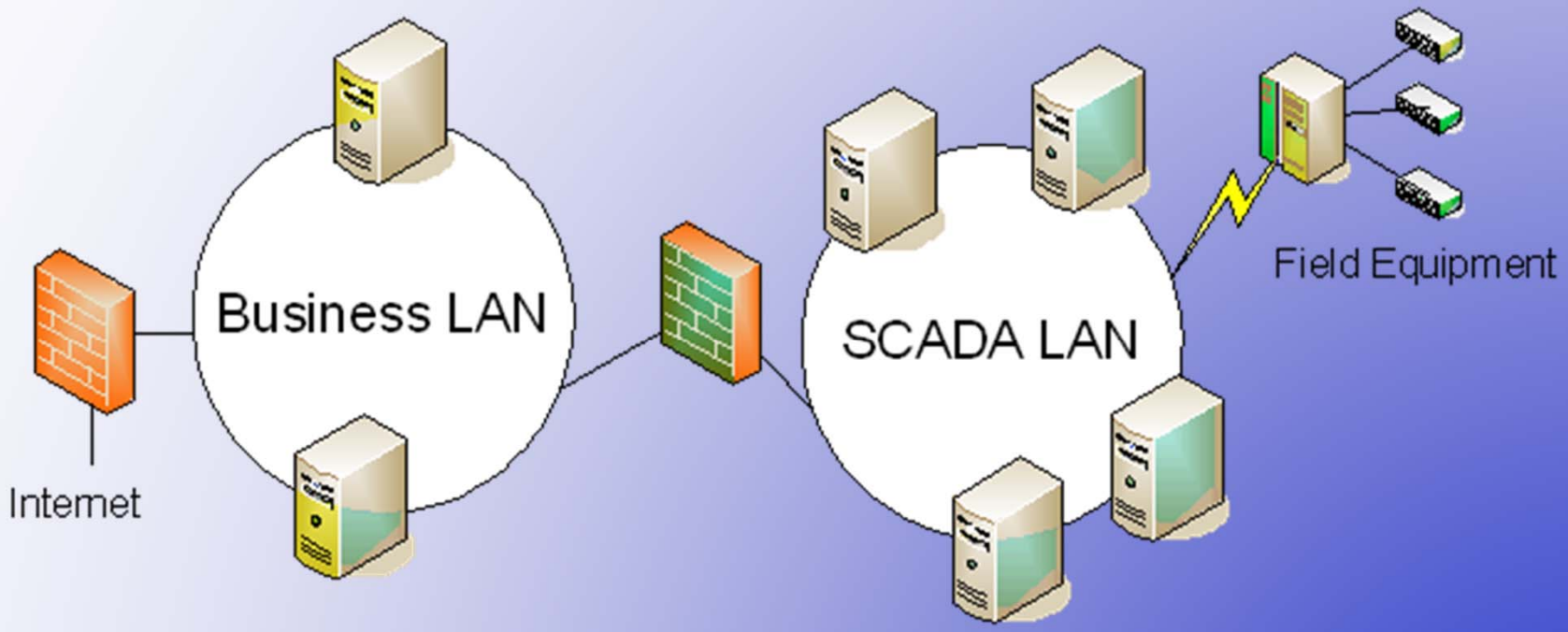
ASW 2011

Cyberspace Defense of Critical Infrastructure

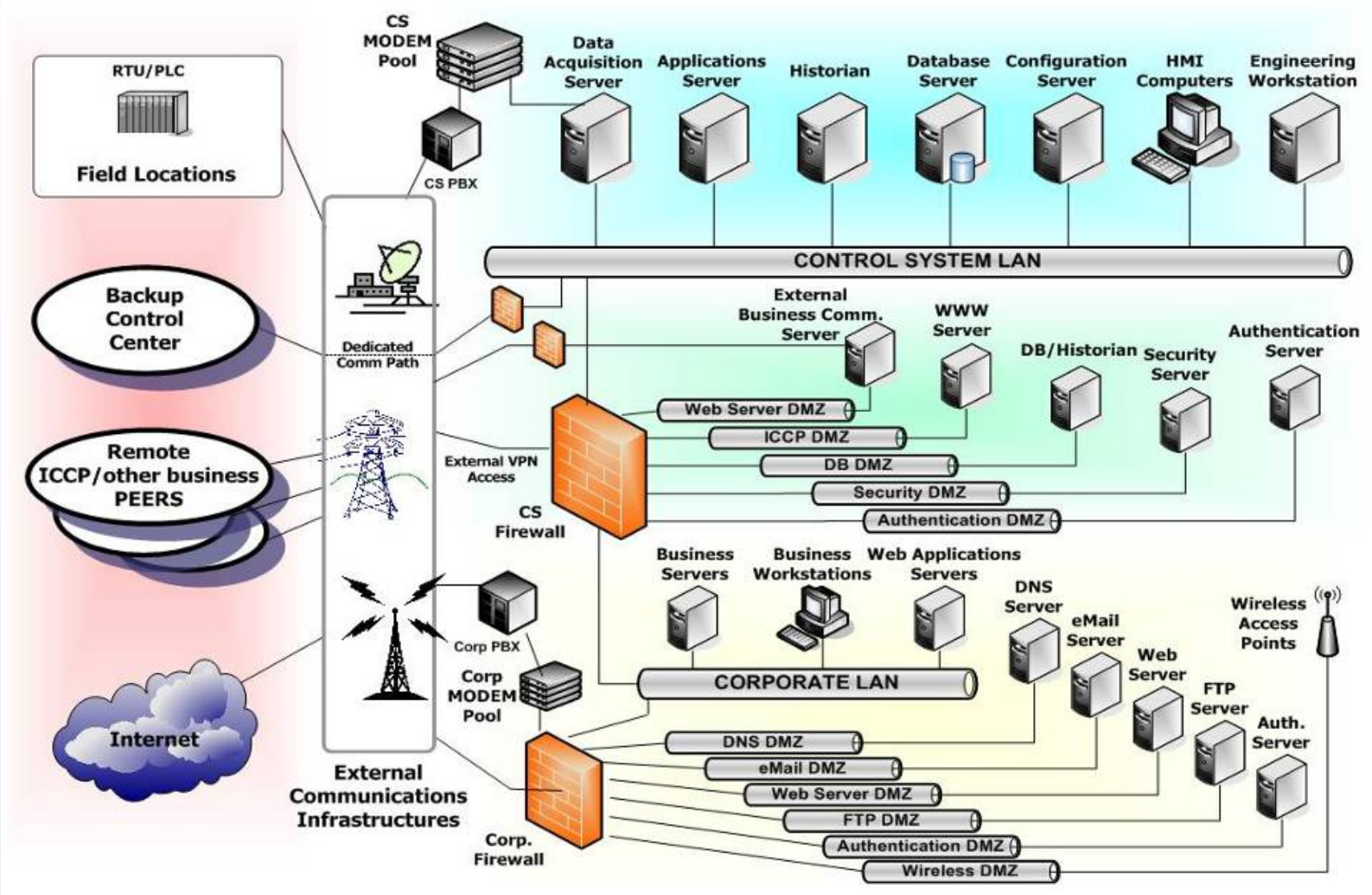
Rob Hoffman
Cyber Security Program Manager
INL

www.inl.gov

Conceptual Control System Layout



Realistic view



Regulation based Security

- "I may only have one outsourced firewall and one outsourced IDS, but I'm compliant"
- "Security standards have been excessively expensive"
- They haven't changed the playing field much
  - Good companies still have good security
  - Bad companies still have bad security
- Functional posture is actually based upon a realistic understanding of the threat, quality of technical team and availability of resources.

Attackers are finally here

- We've been waiting for years for the SCADA hackers to declare themselves
- We now have direct evidence of attackers on a control network that knew what they had hacked into
- We now have direct evidence of attackers interacting with a controller using its native control protocol
- We also have our first cases of nation state level malware directed at process control systems

Aurora - 2007

The Landscape is Changing

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands..."

"…We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities."

"We do not know who executed these attacks or why, but all involved intrusions through the Internet."

Central Intelligence Agency, 2008

Idaho National Laboratory

Black Hat Training February 2008

SCADA Defense: Protecting Critical Infrastructure

Black Hat
BRIEFINGS AND TRAINING

IOActive

Register Now

Overview:

The This course is designed to provide process control professionals with a fundamental understanding of the steps needed to effectively defend their critical infrastructure assets. Defending infrastructure controls systems (SCADA, PCS, DCS, and ICS) has never been more important, nor more in the public eye. This course is designed as an introduction for owners and managers of critical infrastructure on the tools and methods being employed by modern attackers. Besides reviewing the methods and tools, participants will have active classroom exercises focused on defending systems against simulated attacks. These hands-on exercises include scenarios where the attendees will perform analysis, and participate in the defense of a live process and both live and simulated attackers. This uniquely designed atmosphere includes pathways of attack and architectural flaws that the attendees have to identify, diagnose, and protect. Students gain hands-on experience using available tools.

Adversary Capabilities

Black Hat DC 2008

www.ioactive.com

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Classes of Physical Damage

- Inertial Attacks
- Exclusion Attacks
- Resonance Attacks
- Wear Attacks
- Surge Attacks
- Latent Abilities

Adversary Interest

Full Disclosure Mail List January 2008

INSECURE.ORG

Nmap Security Scanner
•Intro
•Ref Guide
•Install Guide
•Download
•Changelog
•Docs
Security Lists
•Nmap Hackers
•Nmap Dev
•Bugtraq
•Full Disclosure
•Pen Test
•Basics
•More
Security Tools
•Pass crackers
•Sniffers
•Vuln Scanners
•Web scanners
•Wireless
•Exploitation
•Packet crafters
•More

Online PLC Training
Train for PLCs at your own pace in the comfort of your own home!
www.online-tech-training.com/gb/2/

Full Disclosure: scada/plc gear

scada/plc gear

- *This message:* [Message body] [More options]
- *Related messages:* [Next message] [Previous message] [Next in thread] [Replies]

From: gmaggro <gmaggro_at_rogers.com>
Date: Sat, 05 Jan 2008 14:01:23 -0500

OK, having done some digging a decent little chunk of industrial automation gear has started coming my way. 1 of 6 pieces. All totaled, roughly under $1000. Small standalone stuff for now, the shipping on populated PLC chassis like SLC-500 stuff is problematic.

If people have specific technical questions, want a script run against a piece of gear or a custom protocol capture done I will entertain such requests. I am also willing to open the cases and pick up the soldering iron, attempt rom/firmware dumps, etc.

Are there any particular tests or tools someone would like me to work into my routine right from the start?

Hardware piece #1 is a Kohler Power Systems modbus/ethernet converter, pn= GM40165.

So far, nmap (4.52) has been detecting the modbus running on port 502/tcp as asa-appl-proto. There is not a great deal of information out there about this protocol. The email contact associated with the port in

Adversary Capabilities

Re: How to BoostUp Tomcat's Performance

Posted by: niceware niceware on August 12, 2007 in response to Message #224661

We provide cracked softwares, these software are all in english language and absolutely full cracked.
The list is not full, any more need, please mail me: judydan@hotmail.com

Amtec Tecplot 10.0
Bernina Artista 4
COADE CAESAR 4.50
COADE PVELITE2005
COADE TANK2.50
RSI.CAMCAD.Pro.v4.5
RSI.Exchange.v6.0.38
RSI.IDL5.5
RSLogix 5 v620
RSLogix.5000.v12.01()
RSoft.LinkSIM.v3.4a
RTI.SCOPETOOLS.V4.0C.CP1.FOR.VXWORK
RX.AutoImage.Pro.R7.5
S7.200.PC.Access.v1.0.2.26
S7.Distributed.Safety.v5.4.SP1
Saber_Z-2007.03
Sage.Payroll.v10
SAM-LEAP_CLASSIC_V6.2.4

Adversary Opportunity

Yahoo Groups February 2008

Re: Terrorists hacking power systems [was RE: Genset from AT&T site

Topic List < Prev Topic | Next Topic >

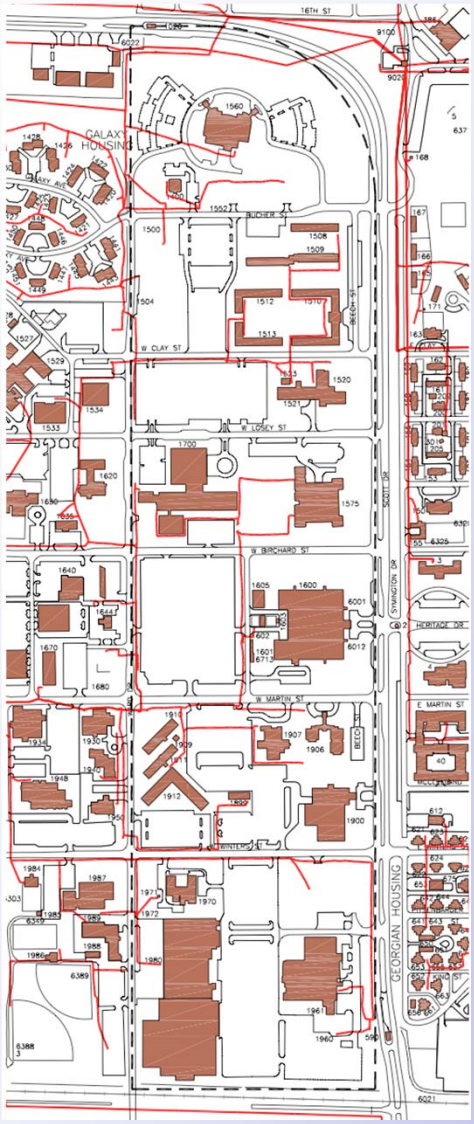
Reply | Forward < Prev Message

Sat Mar 1, 2008 6:40 pm

Show Message Info

Hello All:
I need to weigh in here. Address a couple points,
sorry this is not so much
comms related.
Somehow I missed "the" video, could someone point me
to it.
-I am a Chief Powerplant Operator at a mainstem
Columbia River dam, in the
northwest.
I have worked in hydro powerplants, and high voltage
switchyards for 27
years.

- As far as comms go, I do know our "computer
engineers" both for the
security system, and the plant control system, and
power system control
computers, can get in from home, over the public
network, and that access is
"deeper" that my access running the plant. Not sure of
the security but,
there is also a modem that can be called over a public
phone line, so the
manufacturer can get in if needed.
I feel we are lacking on security, and it would be
easy to get in if you
wanted to.
-Plant physical security is better than before 9-11,
but it is still
horrible, you can "tag in" or follow someone in
through a security gate, and
we have so
many contractors working on site, that anyone could
walk in or out, and no
one would notice, how could we?



Building 1900, receive electrical service from Substation #3 (4,160 volts). Facilities north of West Birchard Street with the exception of Buildings 1700 and 1575, receive electrical service from Substation #6 (4,160 volts). Building 1600 receives electrical service from Substation #5 (4,160 volts). The three buildings listed as exceptions, Buildings 1575, 1700, and 1900, as well as Building 1600, are directly connected to the base 34KV system via a series of pad-mounted switchgear. The first switchgear is located inside the Substation #3 enclosure. Additionally, these buildings are connected to the 34KV system through large transformers rated as follows: • Building 1575 – 4,750 kVA • Building 1600 – 3,750 kVA • Building 1700 – 3, 000 kVA • Building 1900 – 3,750 kVA

AFB is no longer serviced by a central heating/cooling plant. All but eight facilities have been switched to natural gas for heat. Two chiller plants service a total of 10 buildings: Building 1523 services five buildings (Buildings 1509, 1510, 1511, 1512, and 1521) and Building 1899 services five buildings (1906, 1907, 1910, 1911, and 1912). Building 1700 has its own chiller plant. For additional information regarding base-wide utility infrastructure, refer to the #### AFB General Plan.

MAJOR COMMAND ADMINISTRATION AREA DEVELOPMENT PLAN

A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents.

The 14-year-old modified a TV remote control so that it could be used to change track points, The Telegraph reports. Local police said the youngster trespassed in tram depots to gather information needed to build the device. The teenager told police that he modified track setting for a prank.

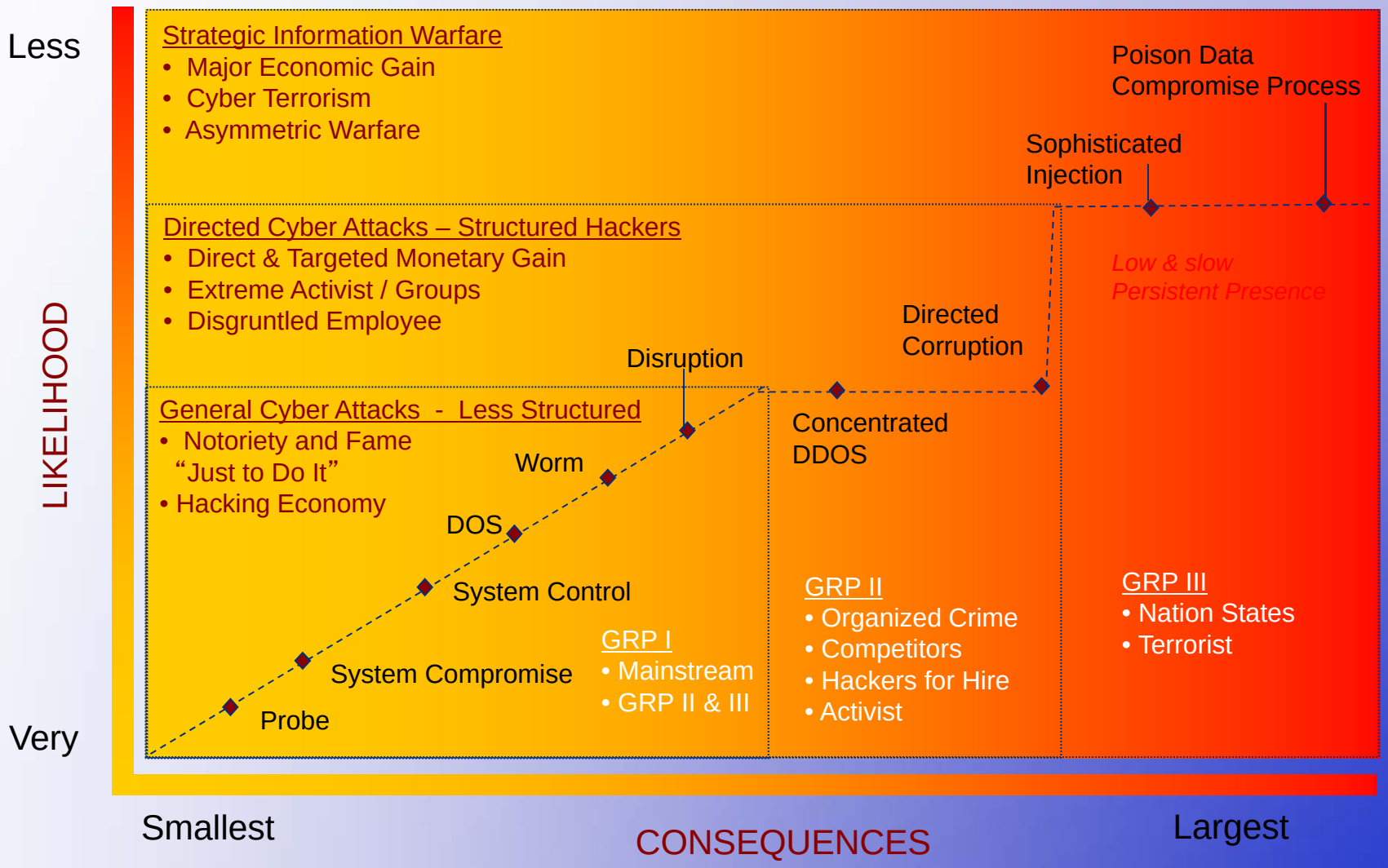
The Register, Jan 11 2008

Wayne D. Says:
January 24th, 2008

"Heh, you would be surprised how lax security is around trains even in the US. BNSF (Burlington Northern/Santa Fe) trains have a really simple wireless system that is not secured very well. They mostly count on no one understand SCADA systems. Also, some railroads transmit unique DTMF tones to switches over their radios. Not to hard to hack when you use their frequency and get a list of tones from a manual."

http://hackedgadgets.com/…

CI Cyber Threats



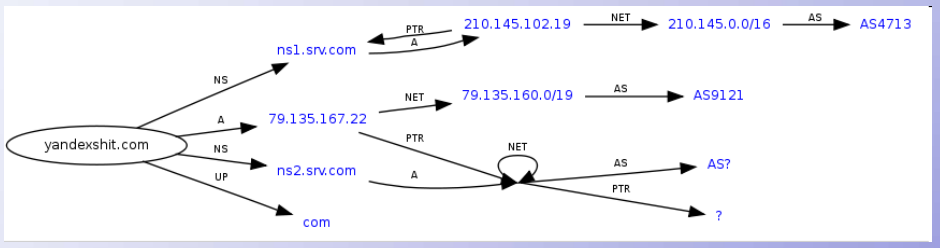
The Operational Environment – 2010-2015

- *CI CS worldwide will:*
  - Display greater presence
  - Be subject to increased unprotected exposure
- *Threat actors will have access to:*
  - More technical anti-CS Capability
  - Expanded Opportunity
- *National defense and CI protection will be hampered by:*
  - Time-late indications & warning
  - Degraded identification of threat actors
  - CI CS servers used as "cyber sanctuaries"

Capability
+
Intent
+
Opportunity

= Threat

Russo-Georgian Conflict
Did it change the environment?



- *Beyond the media hype*
  - Malicious cyber activity, primarily DDoS attacks, preceded & coincided with military activity;
  - "Neutral" servers were captured and "impressed" into combat as "botnets"; and
  - Real-time forensics were stymied
- *Implications*
  - These tactics will be refined and blended;
  - No country's flag of cyber neutrality will be respected;
  - U.S. CI CS servers will be at risk during "any" conflict; and
  - Forensics will be time-late in supporting CI protection
  - Collateral Damage is a very real liability

Emerging Threats

PRC Information Warfare Militia

民兵网络战分队

一、建立网络监测、监控、管理系统，确保网络正常运转。
二、加强网络战的研究和演练，不断提高网络攻击手段。
三、平时广泛获取对方网络信息、建立对方网络信息数据库。
四、战时攻击敌方网络系统、抗击敌方网络攻击。
五、完成上级赋予的其他任务。

Information Warfare Militia Duties

1 - Establish network monitoring systems, conduct monitoring, analyze normal network operations.
2 - Increase research and network warfare training, and continuously improve network attacks.
3 - During peacetime, develop broad access to network information and establish network information database.
4 – During wartime attack enemy networks, resist enemy network attacks.
5 – Conduct other tasks assigned by superiors.

Espionage

Night Dragon

夜龙

Chinese hackers working regular business hours shifts stole sensitive intellectual property from energy companies for as long as four years using relatively unsophisticated intrusion methods in an operation dubbed "Night Dragon," according to a report from security vendor McAfee.

ICS-NA

Stuxnet

Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment. While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.

Control Systems targeted malware

- **Stuxnet worm hit industrial systems**
- "the worm eats away at a very specific kind of industrial control system: a configuration of the Siemens-manufactured Supervisory Control and Data Acquisition (SCADA) system that commands the centrifuges enriching uranium for Iran's nuclear program, the key step for an Iranian bomb", Wired Jan 16, 2011 With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era?

Iran's president, Mahmoud Ahmadinejad, confirmed on Monday night that a computer worm (Stuxnet), affected centrifuges in the country's uranium enrichment programme.

Telegraph – Nov, 29th 2010

INL milestones in critical infrastructure security

2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010

National SCADA Test Bed
DOE

- INL focuses Cyber Security Test bed on Critical Infrastructure SCADA/PCS
- INL demonstrates 3 phase attack against Critical Infrastructure process
- First vendor, ABB enters research relationship
- International research
- Exploit based research used to prove the concept

Control Systems Security Program
DHS

- Multi Sector focus
- Asset owners enter into collaborative research
- IC community engages
- Aggressor based training developed

Aurora Test
Physical Consequence of Cyber Attack

- Utilize remote cyber attack against a 20,000lb Diesel Generator
- Total destruction of unit.

ICS-CERT
DHS

- Conducting vulnerability and malware analysis
- Providing actionable intelligence
- Conduct incident response forensics
- Coordinate vendor, asset owner & CERT vulnerability response.

SCADA Vulnerability Research Center

- Cyber Assessment
- Term Analysis
- Advanced Training
- Modeling and Simulation

Protecting the Systems Controlling Our Infrastructure

- *Control Systems Capabilities*
  - Supervisory Control and Data Acquisition (SCADA)/CS Vulnerability Testing
  - Asset owner Vulnerability Assessments
  - Analysis of vulnerabilities
- *Primary Facilities & Resources*
  - Critical Infrastructure Test Range
    - SCADA Test Bed
    - Power Grid Test Bed
    - Mock Chemical Mixing Facility
    - Wireless Test Bed
- *Full Scale testing with operational infrastructure*

Access/Working Relationships With Global Vendors

Objectives

- Create secure CS environments that improve the security posture of our nation's critical infrastructure.

Capabilities

- Fully functional SCADA systems and Energy Management Systems (EMS)
- Fully functional Distributed Control Systems (DCS)
- Safety systems and protective components
- Real world configurations and consequence testing
- Ability to generate CS data traffic
- Vendor and asset owner partnerships
  - Large SCADA/EMS systems
  - On-site assessments

Aggressive engagement

Partnerships are key to success – in the face of a multi-faceted, largely non-attributable threat, cooperation is essential to survival.

- On behalf of our existing customers, INL coordinates efforts among federal, state, local and tribal governments
- Works with owner/operators, vendors and security researchers
- Collaborates with international CERTs and private sector ISACs

Recommended Resources

- 21 Steps to improve Cyber Security of SCADA Networks
  - http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
- NIST SP 800.82 Guide to Industrial Control Systems (ICS) Security
  - http://csrc.nist.gov/publications/PubsSPs.html
- Catalog of Control Systems Security: Recommendations for Standards Developers
  - http://www.us-cert.gov/control_systems/index.html
- DHS, Industrial Control Systems Cyber Emergency Response Team, (ICS-CERT)
  - http://www.us-cert.gov/control_systems/ics-cert
- Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies
  - http://www.us-cert.gov/control_systems/index.html

Additional Information

- Rob.hoffman@inl.gov
- id2hofrw@doe.ic.gov
- (208) 526-8599

Idaho National Laboratory

Thank - you

www.inl.gov

Idaho National Laboratory