Control Systems Cyber Security for Managers and Operators

September 13, 2007

Idaho National Laboratory

Disclaimer

- **References made herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, any agency thereof, or any company affiliated with the Idaho National Laboratory.**

- **Use the described security tools and techniques at "***your own risk***" – i.e. carefully evaluate any tool prior to using it in a production SCADA Network.**

- **The demonstrations and exploits used in the workshop are NOT SCADA vendor specific. The exploits take advantage of TCP/IP network and Operating system vulnerabilities. At no time is the actual PLC or RTU exploited.**

Workshop Agenda

- **Introductions**
- **Background**
- **Understanding the Risk**
- **Attack Trends and Attacker Profile**
- **Understanding Exposure**
- **Experiences from Field Visits**
- **Anatomy of an Attack**
- **Energy System Exploitation (DEMO)**
- **Demo Exploits**
- **Mitigations**
- **Firewalls and Intrusion Detection**
- **Conclusions**
- **NERC Mitigation Activities**
- **Q & A**

Introductions

The Idaho National Laboratory

A DOE National Laboratory located in Idaho

- ***Facilities located in Idaho Falls and on the 890 square mile reservation located 40 miles away***
- ***Work force of 3,300 people ~ 7,000 total employees with all contractors***
- ***Historically focused on nuclear reactor research***
  - ***Operated by Battelle***

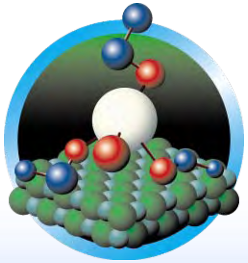
Idaho National Laboratory

The INL R&D

Mission execution is guided by five laboratory divisions

Nuclear Energy

National Security



Science and Technology

SCADA/PCS Test Bed

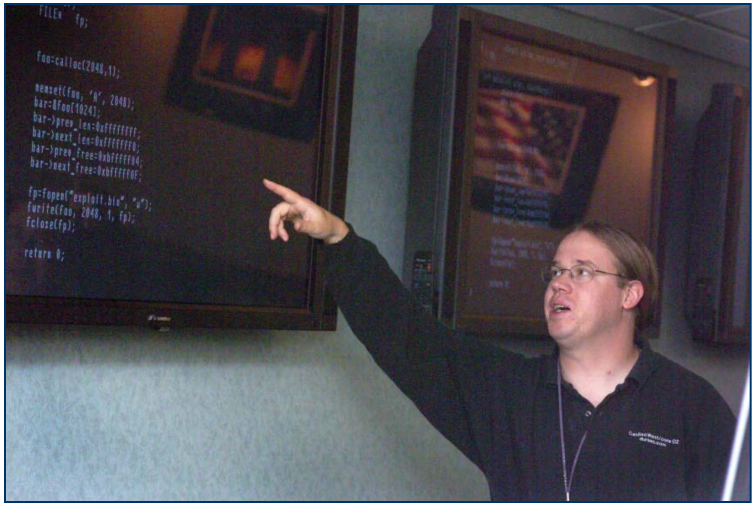
Control Systems

- *Multiple Vendor participation*
- *Fully functional SCADA/EMS systems*
- *Fully functional DCS and PCS systems*
- *Inter-systems (ICCP) communication capability*
- *Real world configuration capability*
- *Remote testing capability*

Cyber Security Test Bed

An integral part of the SCADA/ Process Control Test Bed

- ***Supports control system security***
- ***Industry assessments***
- ***State of the art knowledge***



Next Generation Wireless Test Bed

Operational since April 2003

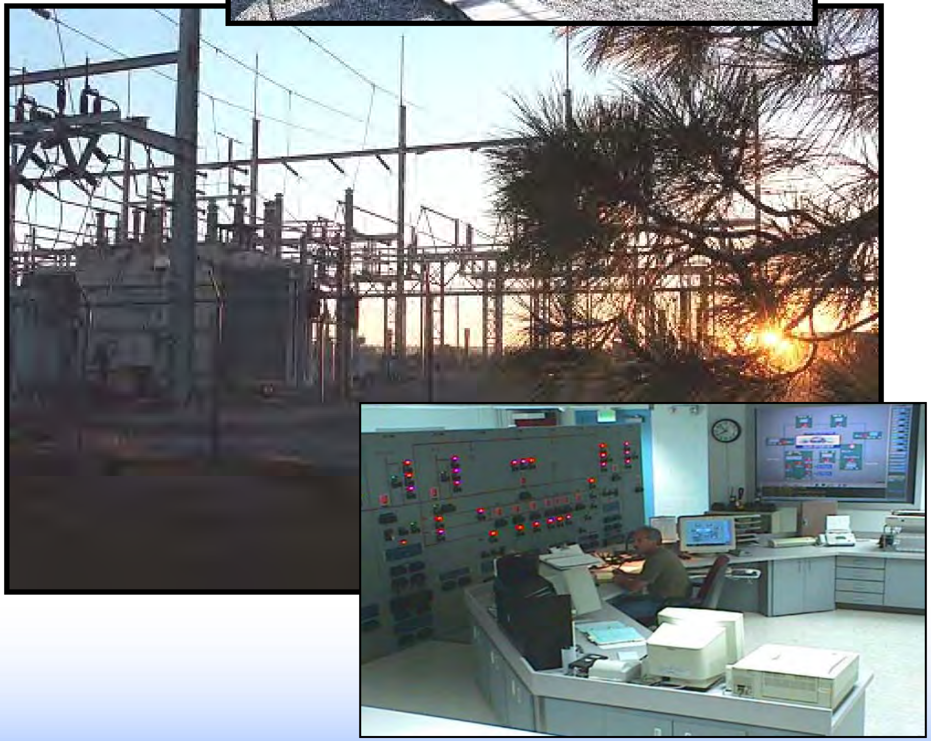
- ***America's only "city sized" wireless test facility***
- ***9 Cell tower system operational; potential to expand***
- ***Testing next generation (3G/4G) wireless communication, wireless LANs and Land Mobile Radio systems***
- ***Access to commercial and government spectrums as NTIA experimental test station***
- ***Physically secure, interference free environment (Radio Free Idaho)***
- ***Has supported IED jammer testing for USMC/Navy EOD***

Idaho National Laboratory

Power Grid Test Bed

Various power grid test beds available:

- ***Secure power distribution system***
  - ***61 mi dual fed, 138kV power loop***
  - ***7 substations***
  - ***3 commercial feeds***
- ***Real-time grid monitoring and control through centralized SCADA operations center***
- ***Ability to isolate portions of grid for specialized testing***
- ***Protection & Restoration***
- ***Research***



Idaho National Laboratory

DOE OE Mission

To establish a National capability to support industry and government in addressing control system cyber security and vulnerabilities in the energy sector

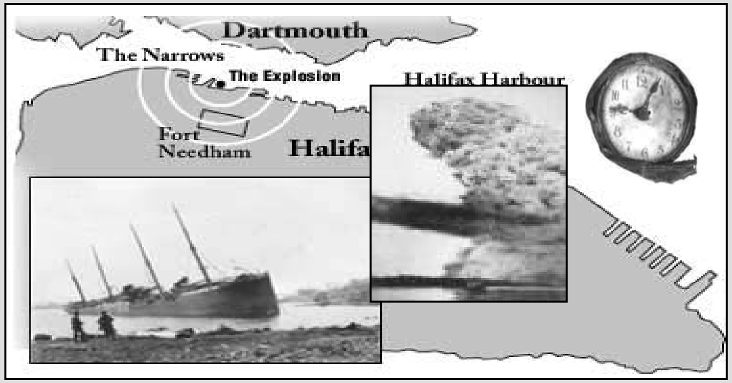
Control Systems Security Program

Create a national-level capability to coordinate between government and industry to reduce vulnerabilities and respond to the threats associated with the control systems that operate our national critical infrastructure.

Reduce Cyber Risk to Critical Infrastructure Control Systems

Understanding the Risk

These Images Demonstrate A Common Theme



Halifax Explosion on Dec 6th

Pearl Harbor on Dec 7th

The World Trade Center's South Tower begins to collapse. Estimates were that each jet was carrying approximately 60,000 pounds of jet fuel and traveling at 300 miles per hour when they crashed into the Towers

Rescue helicopter responded to attack near Washington, DC on September 11, 2001, after hijacked American Airlines Flight 77 crashed into the Pentagon, killing 189 persons, including all aboard the aircraft.

WTC & Pentagon on September 11th

…An inability to see what was possible

Idaho National Laboratory

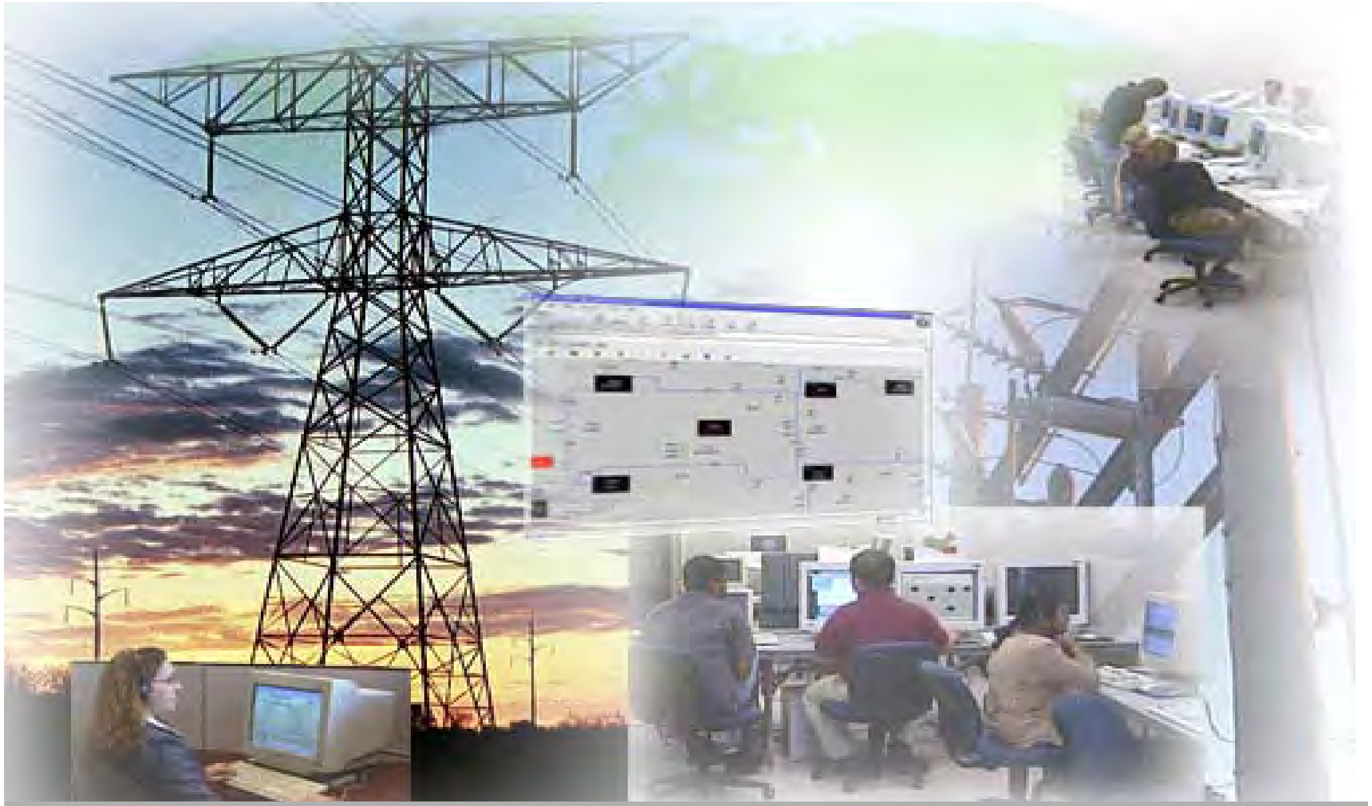
The Risk Equation

Risk = Threat x Vulnerability x Consequence

- **Threat:** *Any person, circumstance, or event with the potential to cause loss or damage*
- **Vulnerability:** *Any weakness that can be exploited by an adversary or through accident*
- **Consequence:** *The amount of loss or damage that can be expected from a successful attack*

> **Cyber infrastructure** includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.
>
> **NIPP 1.7.1**

Risk is Elevated in Converged & Interconnected Systems



Technology has blurred the line between the physical machine and the electronic machine driving our infrastructure.

Idaho National Laboratory

Nine Core Operational Processes

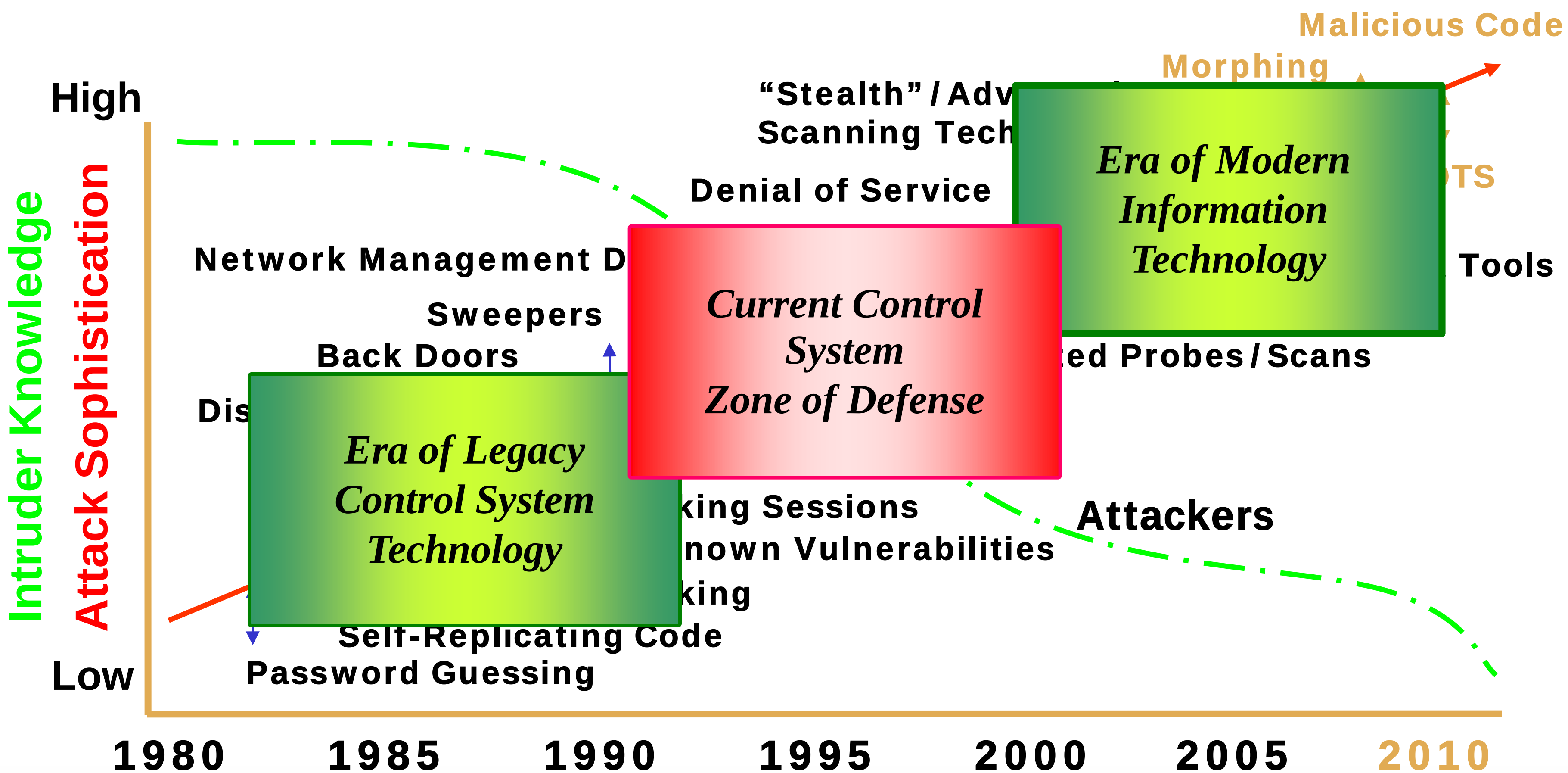
- Monitoring and Investigative Processes
  - Monitoring & Logging
  - Forensics & Investigations
  - Threat Analysis & Assessment
- Risk and Vulnerability Management Processes
  - Risk Management
  - Vulnerability Management
  - Secure Development Life Cycle
- Response and Continuity Processes
  - Business Continuity Planning
  - Crisis Management
  - Incident Response

*A Program approach used at AEP

Attack Trends
and the
Attacker Profile

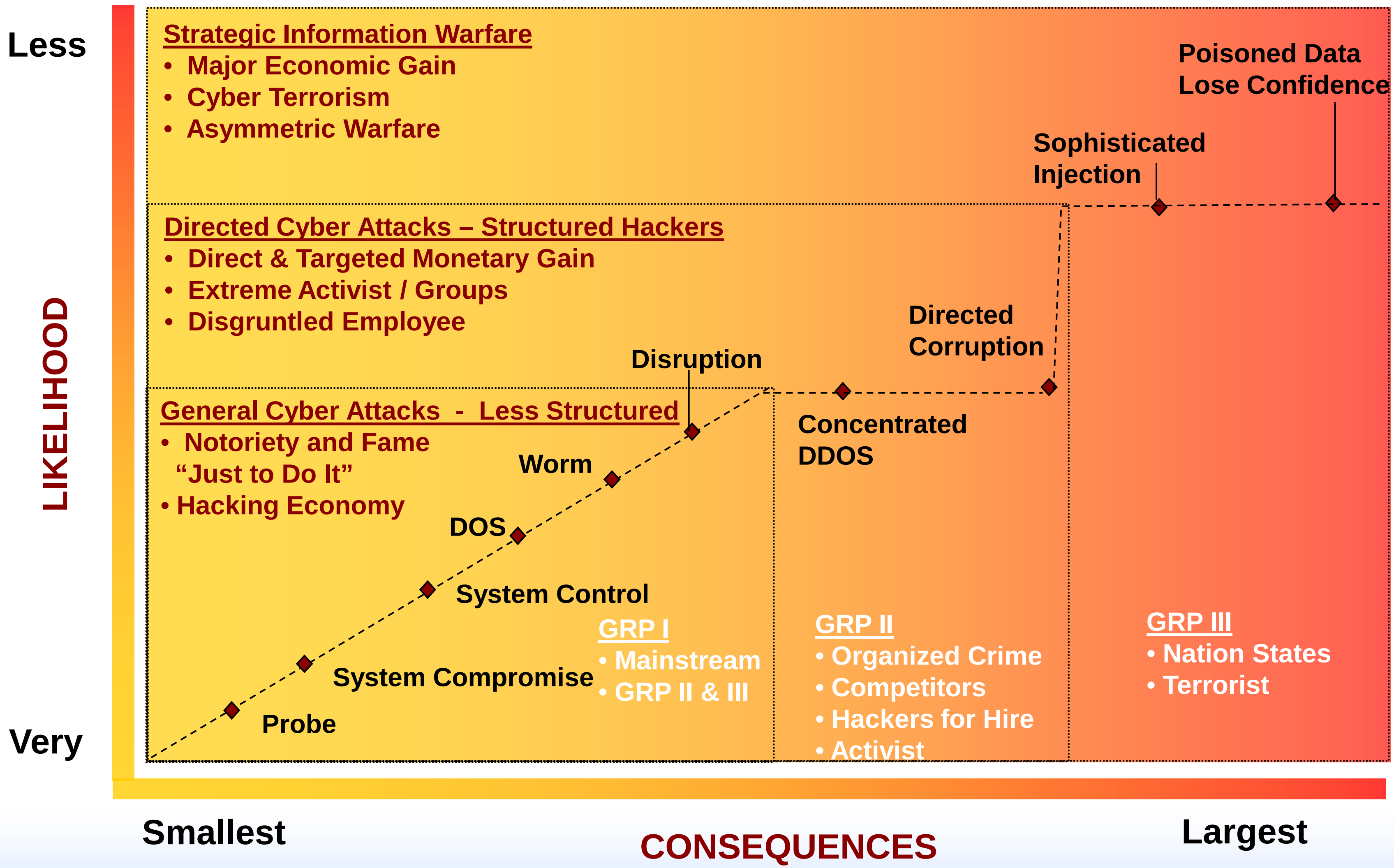
Threat Trends

- Threats More Complex as Attackers Proliferate



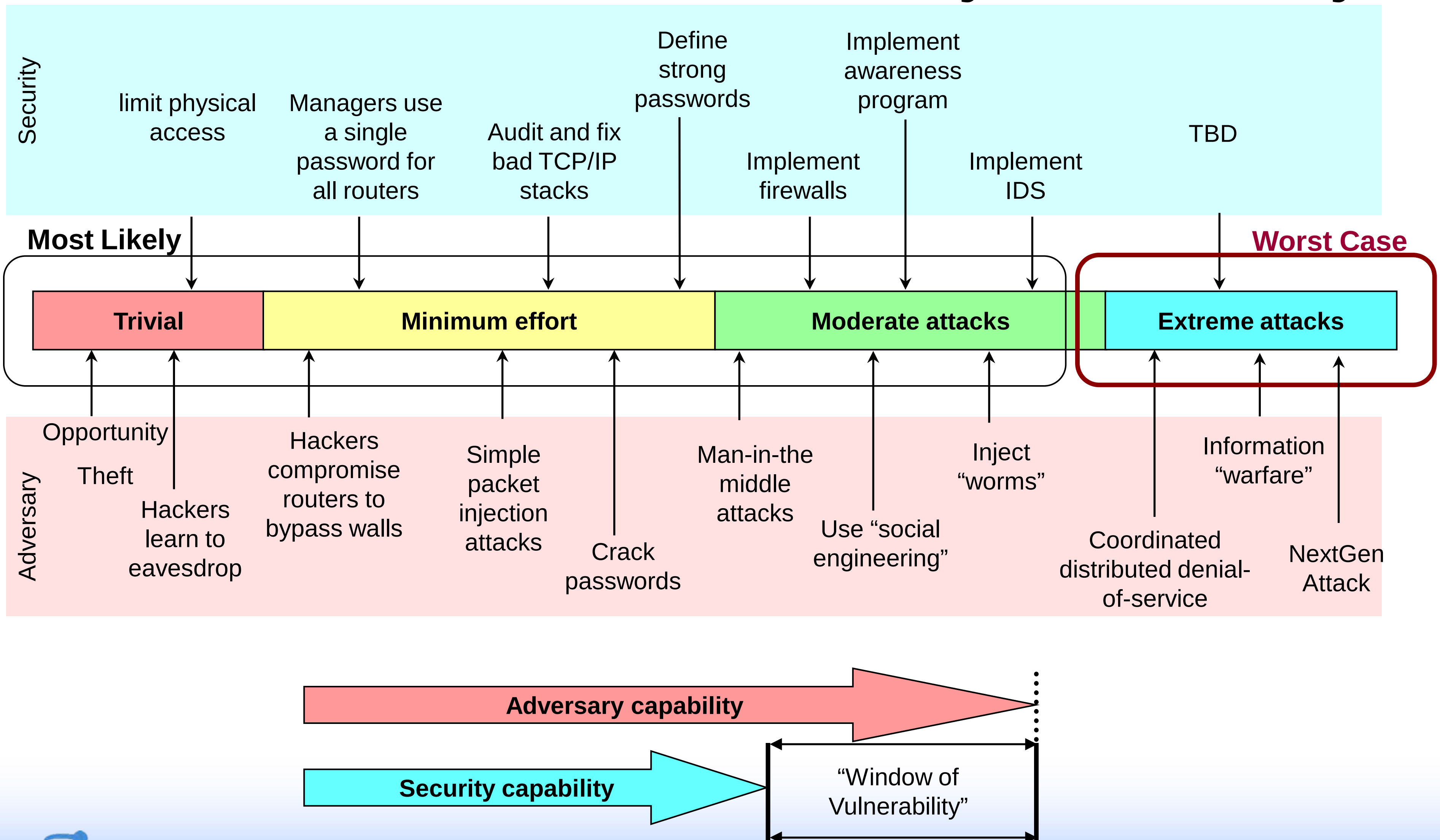
Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

Cyber Threats: The Flattening of the Line



Idaho National Laboratory

The electronic arms race of cyber security



Control System Security IS a Concern

From the control system manufacturers' side, SCADA and automation devices need to undergo security robustness design and testing prior to deployment in the field. SCADA & control protocols should also be improved to include security features. Currently most devices appear to be highly vulnerable to even minor attacks and have no authentication/authorization mechanisms to prevent rogue control.

Failure to adapt to the changing threats and vulnerabilities will leave the controls world exposed to increasing cyber incidents. The result could easily be loss of reputation, environmental impacts, production and financial loss and even human injury.

Insidious threat to control systems InTech January 01, 2005; Eric Byres and Justin Lowe

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress

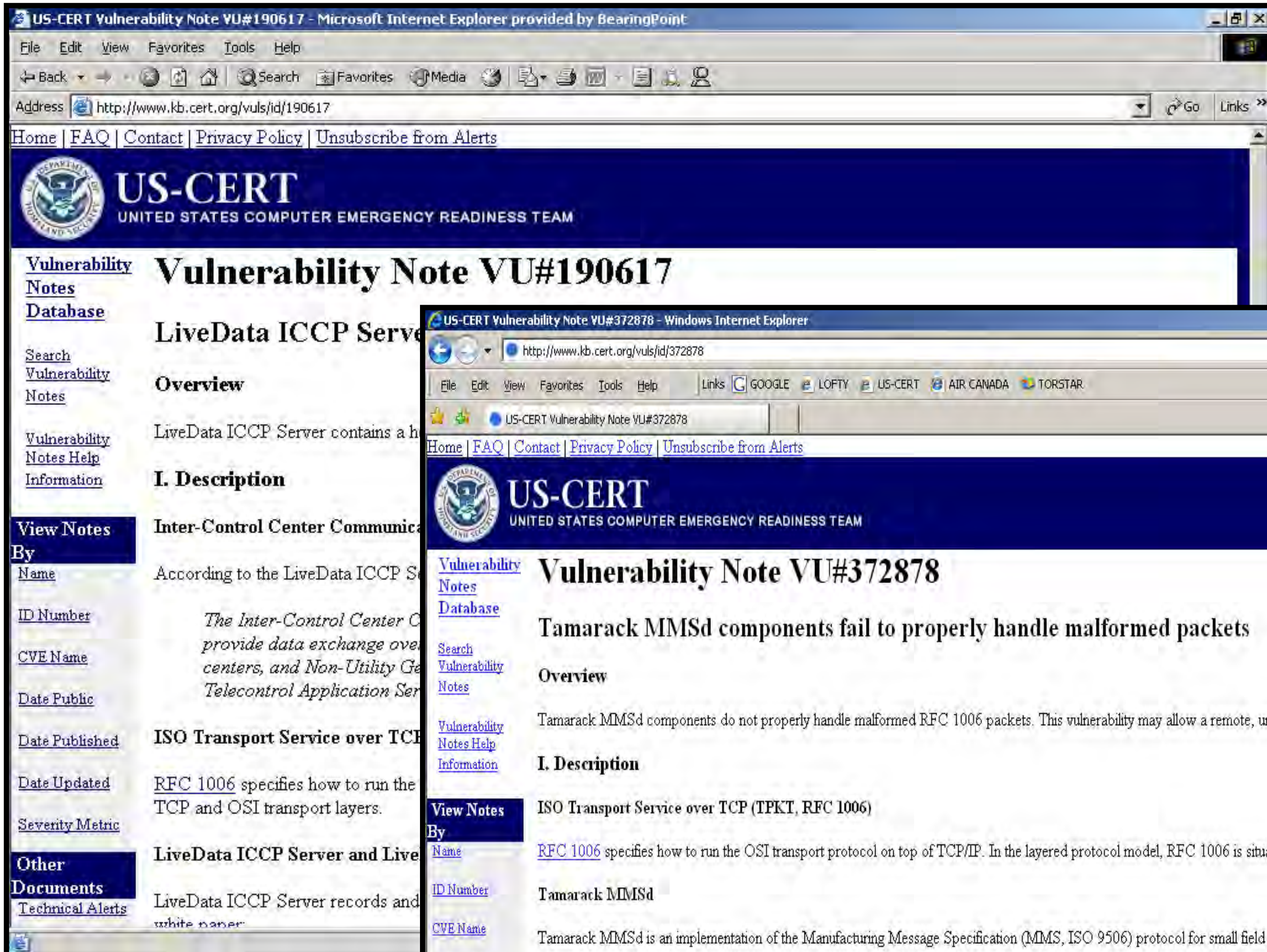
October 17, 2003

For Release on Delivery
Expected at 1:00 p.m. EDT
Wednesday, October 1, 2003

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Securing Control Systems

Idaho National Laboratory



US-CERT Vulnerability Note VU#190617 - Microsoft Internet Explorer provided by BearingPoint

Address http://www.kb.cert.org/vuls/id/190617

Home | FAQ | Contact | Privacy Policy | Unsubscribe from Alerts

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By
Name
ID Number
CVE Name
Date Public
Date Published
Date Updated
Severity Metric

Other Documents
Technical Alerts

Vulnerability Note VU#190617

LiveData ICCP Serve

Overview

LiveData ICCP Server contains a h

I. Description

Inter-Control Center Communica

According to the LiveData ICCP S

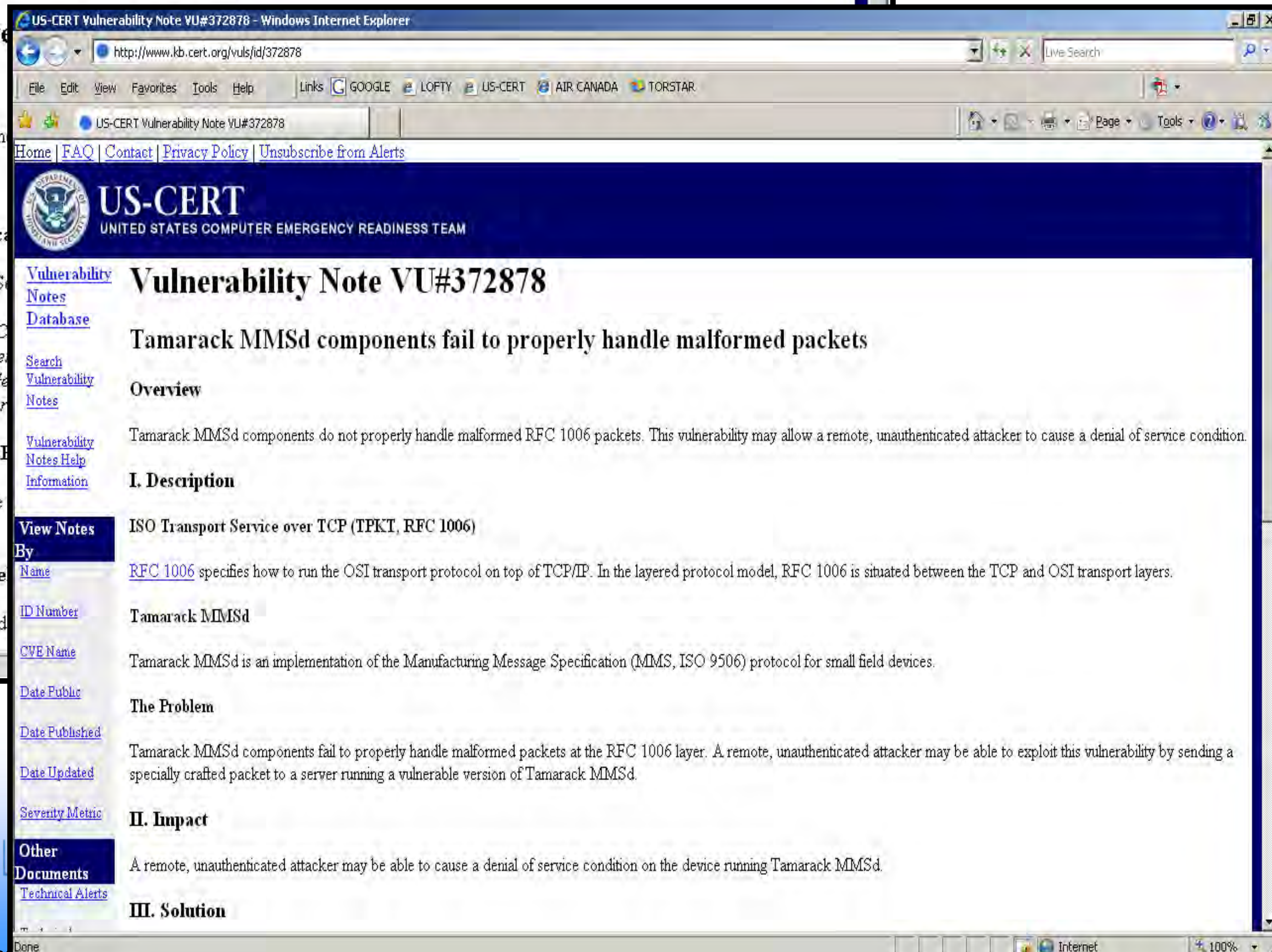
The Inter-Control Center C
provide data exchange ove
centers, and Non-Utility Ge
Telecontrol Application Ser

ISO Transport Service over TCI

RFC 1006 specifies how to run the
TCP and OSI transport layers.

LiveData ICCP Server and Live

LiveData ICCP Server records and
white paper



US-CERT Vulnerability Note VU#372878 - Windows Internet Explorer

http://www.kb.cert.org/vuls/id/372878

Home | FAQ | Contact | Privacy Policy | Unsubscribe from Alerts

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By
Name
ID Number
CVE Name
Date Public
Date Published
Date Updated
Severity Metric

Other Documents
Technical Alerts

Vulnerability Note VU#372878

Tamarack MMSd components fail to properly handle malformed packets

Overview

Tamarack MMSd components do not properly handle malformed RFC 1006 packets. This vulnerability may allow a remote, unauthenticated attacker to cause a denial of service condition.

I. Description

ISO Transport Service over TCP (TPKT, RFC 1006)

RFC 1006 specifies how to run the OSI transport protocol on top of TCP/IP. In the layered protocol model, RFC 1006 is situated between the TCP and OSI transport layers.

Tamarack MMSd

Tamarack MMSd is an implementation of the Manufacturing Message Specification (MMS, ISO 9506) protocol for small field devices.

The Problem

Tamarack MMSd components fail to properly handle malformed packets at the RFC 1006 layer. A remote, unauthenticated attacker may be able to exploit this vulnerability by sending a specially crafted packet to a server running a vulnerable version of Tamarack MMSd.

II. Impact

A remote, unauthenticated attacker may be able to cause a denial of service condition on the device running Tamarack MMSd.

III. Solution

Davis – Besse "SQL Slammer"

NRC NEWS

U.S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs Telephone: 301/415-8200
Washington, DC 20555-001 E-mail: opa@nrc.gov
Web Site: http://www.nrc.gov/OPA

No. 03-108 September 2, 2003

NRC ISSUES INFORMATION NOTICE ON POTENTIAL OF NUCLEAR POWER PLANT NETWORK TO WORM INFECTION

The Nuclear Regulatory Commission staff has issued an Information Notice to alert nuclear power plant operators to a potential vulnerability of their computer network server to infection by the Microsoft SQL Server worm.

The vulnerability was demonstrated by a January event at the shutdown Davis-Besse nuclear power plant. The worm infection increased data traffic in the site's network, resulting in the plant's Safety Parameter Display System and plant process computer being unavailable for several hours. Neither of those systems, however, affects the safe operation of a nuclear plant. NRC regulations require safety-related systems to be isolated or have send-only communication with other systems. Public health and safety were never impacted during the incident.

Idaho National Laboratory

Harrisburg, PA water facility

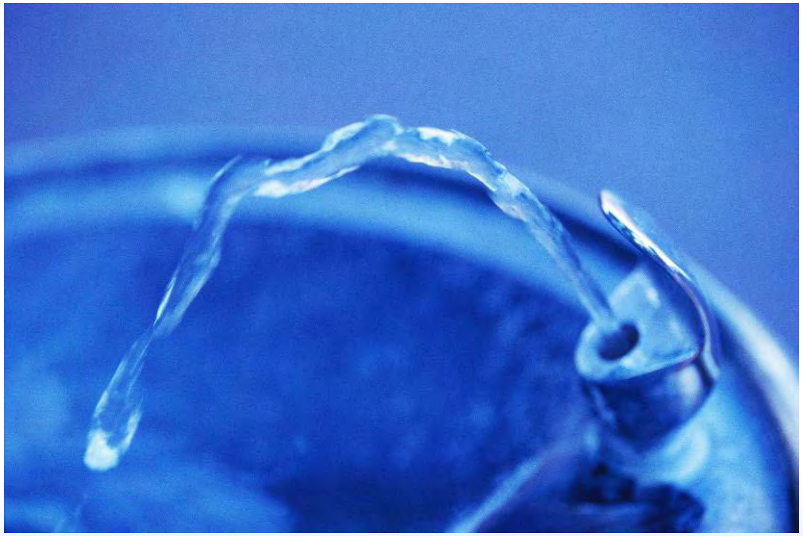
Water Tech ONLINE www.watertechonline.com

Legal Briefs - 11/1/2006 1:46:48 PM

PA water plant tapped by computer hackers

HARRISBURG, PA – The FBI is investigating a security breach in which hackers gained access to the computer system at a Harrisburg drinking water treatment plant, according to a November 1 report on InfoWorld.

The breach, which was discovered earlier this month, occurred after a laptop used by a plant employee was accessed by hackers via the Internet and used to install a computer virus and "spyware" on the plant's computer system, the article noted.



Idaho National Laboratory

Insider Threat

2 deny hacking into L.A.'s traffic light system

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

By Sharon Bernstein and Andrew Blankstein, Times Staff Writers - January 9, 2007

Back in August, the union representing the city's traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

City officials took the threat seriously.

Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.

But officials now allege that two engineers, Kartik Patel and Gabriel Murillo, figured out how to hack in anyway. With a few clicks on a laptop computer, the pair — one a renowned traffic engineer profiled in the national media, the other a computer whiz who helped build the system — allegedly tied up traffic at four intersections for several days.

Los Angeles Times

Idaho National Laboratory

DoD Penetration Testing Video

Statistics… Revisited

- **Industrial Security Incident Database**
  - 83 Confirmed Incidents

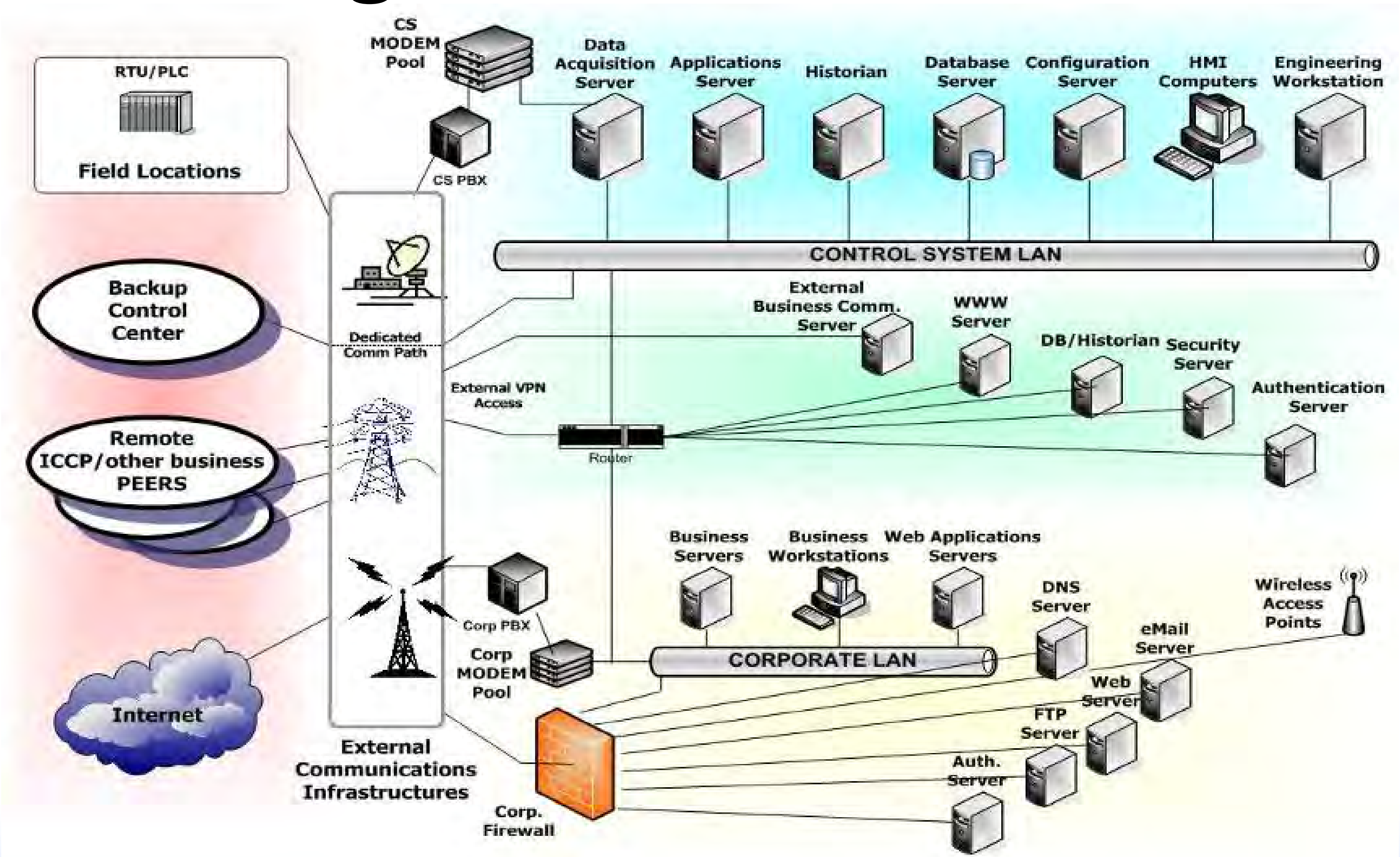
- **The video claims that for every reported incident, you have 400 that remain undiscovered / unreported (83 * 400 = 33200)**

- **Other knowledgeable sources claim this ratio is more like 100 that remain undiscovered / unreported (83 * 100 = 8300)**

- **Any way you slice it, and even if we are off by an order of magnitude, there are a LARGE number of control system related security incidents occurring**

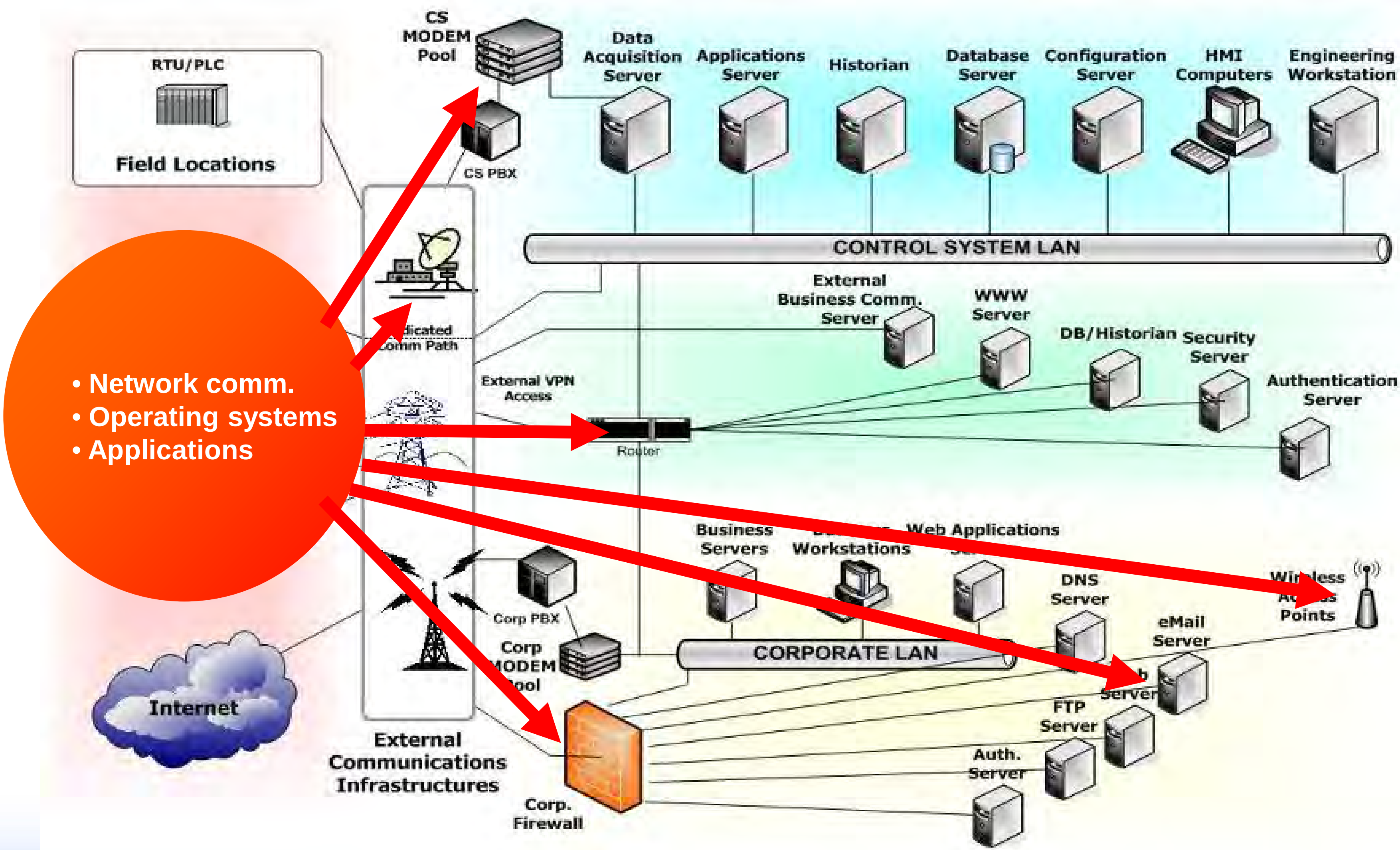
Understanding Exposure

Looking at the Network



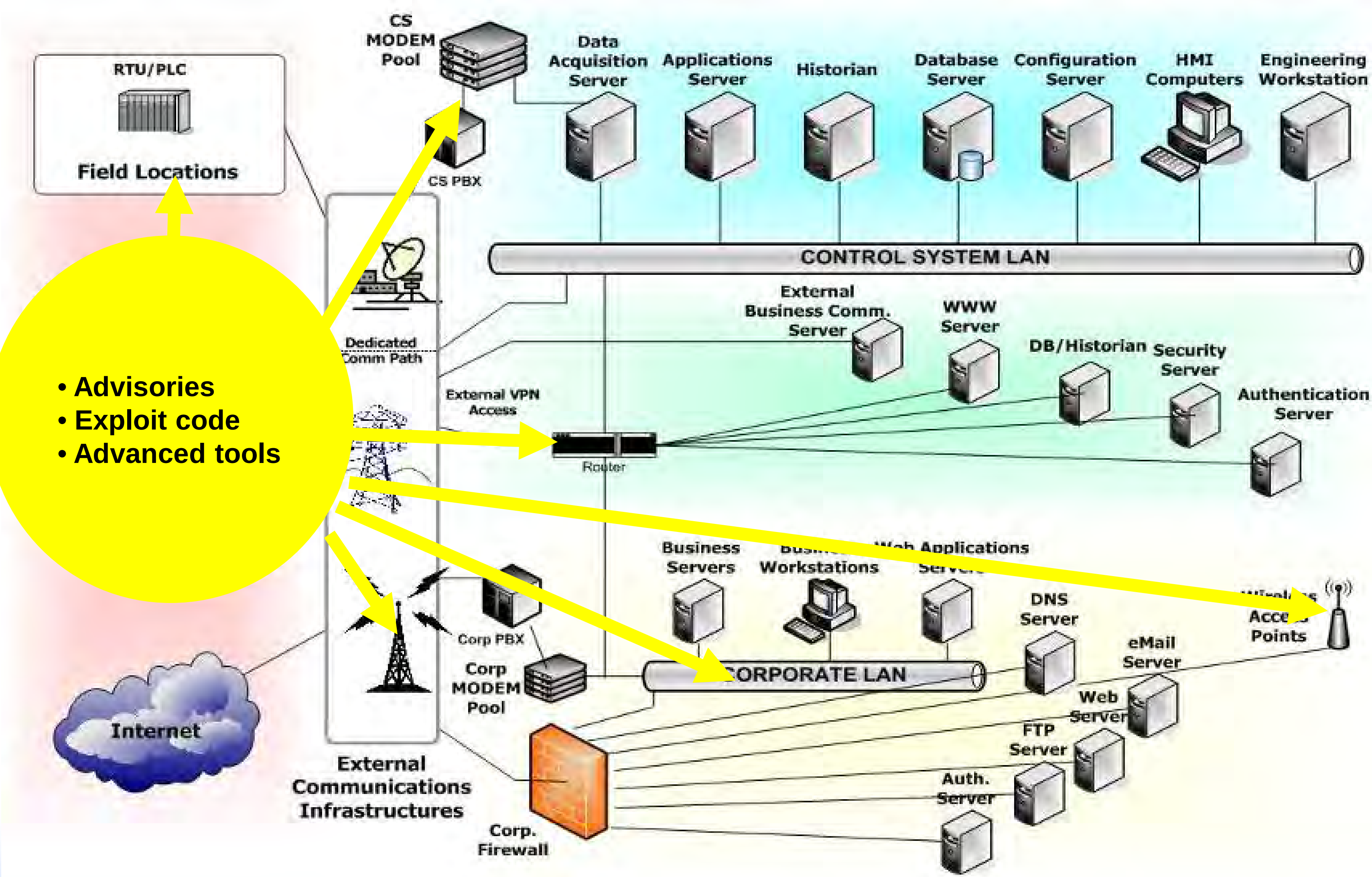
Idaho National Laboratory

Identify Vulnerable Components



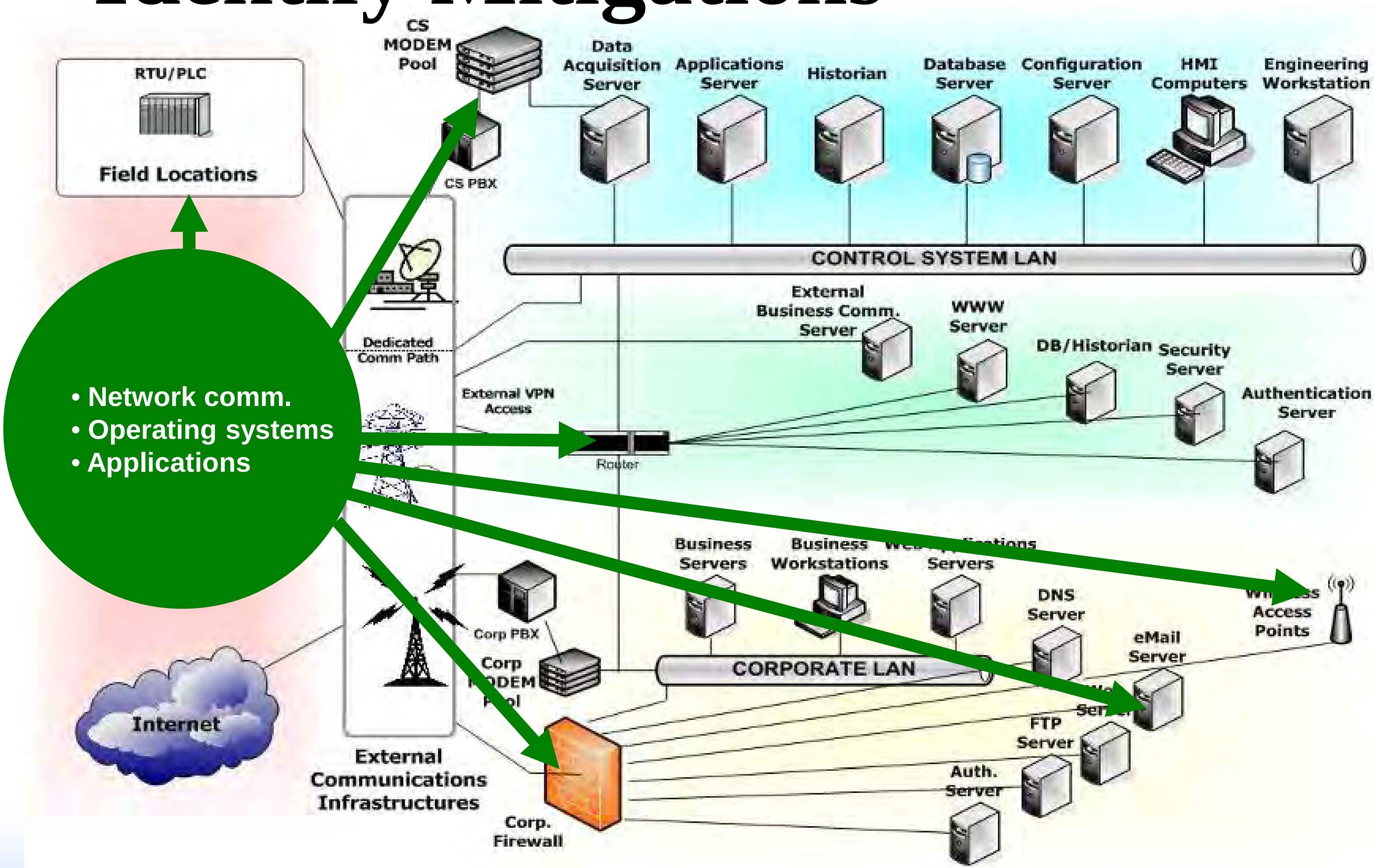
Idaho National Laboratory

Identify Threat Vectors

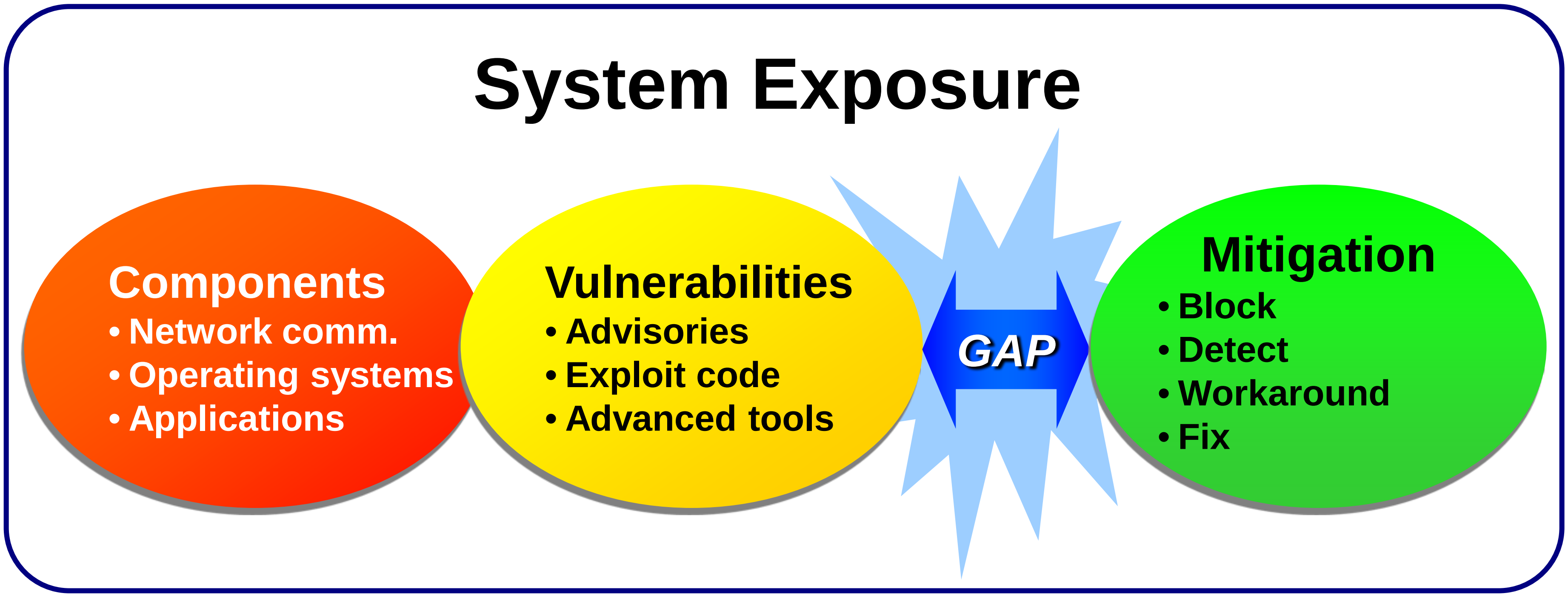


Idaho National Laboratory

Identify Mitigations



Exposure


System Exposure
Components
• Network comm.
• Operating systems
• Applications
Vulnerabilities
• Advisories
• Exploit code
• Advanced tools
GAP
Mitigation
• Block
• Detect
• Workaround
• Fix

Experiences from Field Visits

Evolution of IT Security vs. Control System Security

TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus& Mobile Code Countermeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-5 years	Up to 20 years
Outsourcing	Common/widely used	Rarely used
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24 x 7 x 365 x forever
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

General Findings

- Vendor default accounts and passwords
- Guest accounts still available
- Control system use of enterprise services (DNS, NTP, etc.)
- Inadequate security level agreements:
  - with peer site(s)
  - with vendor(s)

General Findings

- Dynamic ARP tables with no ARP monitoring
- Unused software still on systems
- Unused services still active
- Writeable shares between hosts
- Direct VPN from off site allowed to control systems

General Findings:
Switches and Routers

- Delivered wide open and remains unchanged
- Limited on-site expertise to address security
- In most cases, DEFAULTS are NOT shown in configuration lists
- Port security rarely used to secure domains

General Findings: Firewalls

- Rules
  - not commented
  - Generic or Simplified rules
  - Old/temporary rules not removed
  - Many without ownership or justification
- Logging not turned on
- In some cases, firewall is subverted by direct connection
- Same firewall rule set used on control domain and corporate domain

General Findings:
IDS – Intrusion *Detection* System (passive)

- Fairly new to control system environments (SCADA, DCS and PLC signatures are being developed)
- Deployed at corporate level in many cases
- Little or no budget or support for staffing and training
- Can not analyze encrypted traffic

Idaho National Laboratory

General Findings:
IPS – Intrusion *Prevention* System (active)

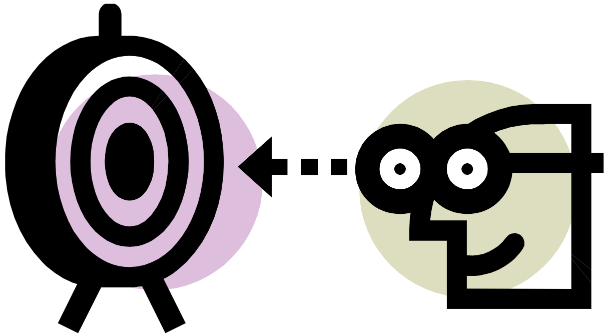
- Fairly new to industry (in general)
- Not fully understood in many applications
- Difficult to deploy at any level
- Little or no budget or support for staffing and training
- Caution if deploying inside critical real-time system networks
  - Packet scrubbing
  - False positives

Anatomy of an Attack

Typical Attack Steps

- Target Identification / Selection
- Reconnaissance
- System Access
- Keeping Access
- Covering the Tracks

Target Identification / Selection

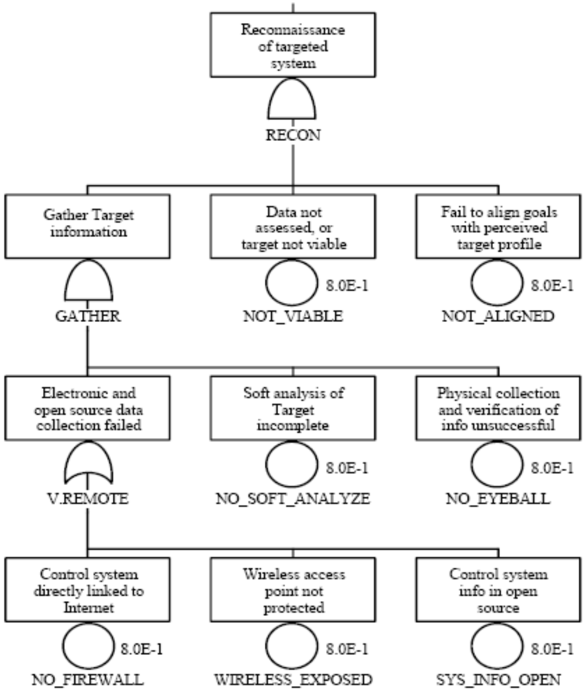


- Dependent on the attacker
- How ‘accessible’ is your company?
  - Internet, media, etc. presence
- How much information is available through your vendor?
- Is your company/utility desirable as a target?
- How do your defenses compare to your neighbors?

Idaho National Laboratory

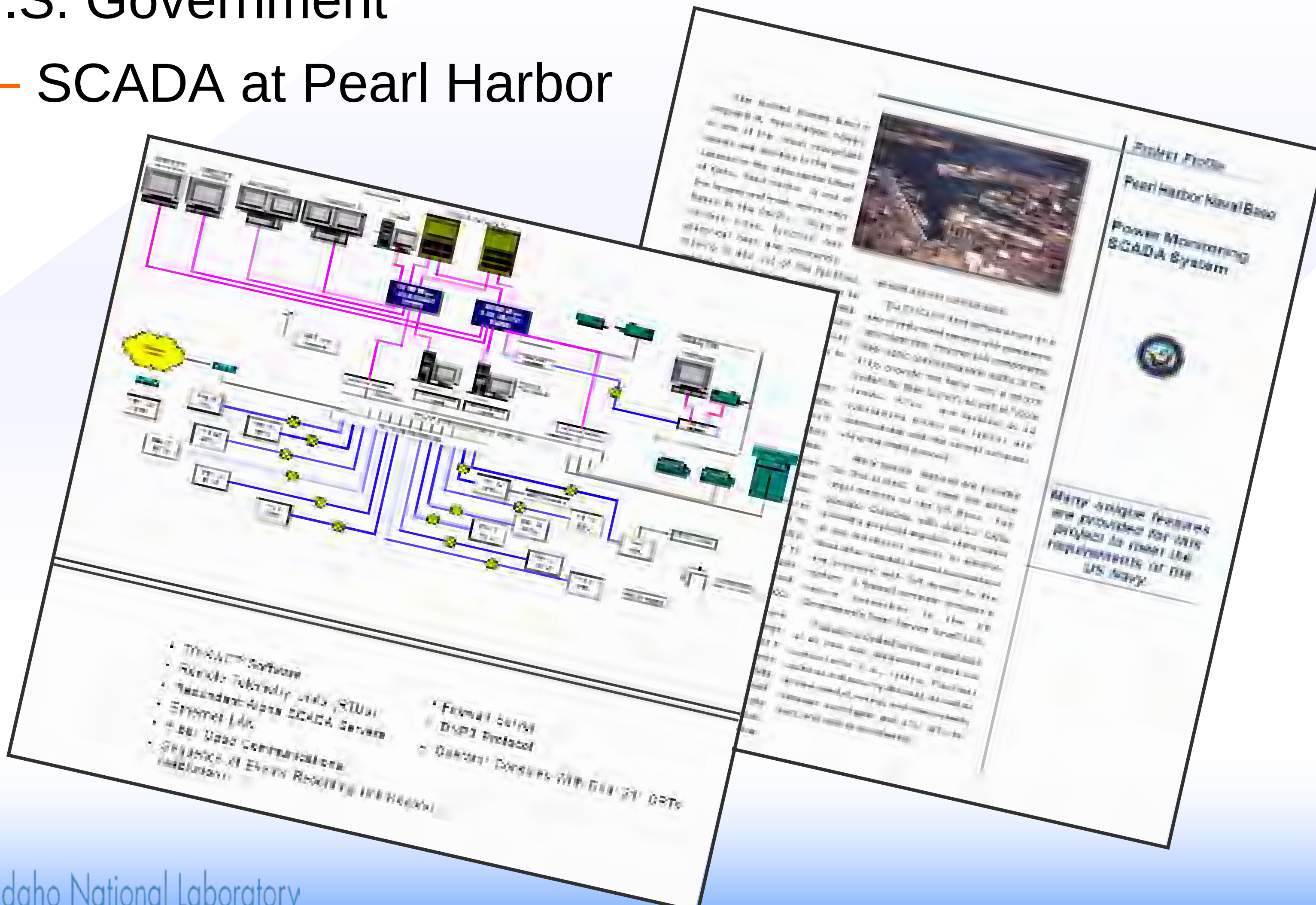
Reconnaissance

- Mapping the target assets and resources
- Open Source Intelligence
  - External Web Site
  - Google (Internet) Searches
  - DNS Lookups
- Dumpster Diving
- Social Engineering
- War Dialing / War Driving
- Scanning
  - Asset/service discovery, network connectivity
- Insider Threat



Reconnaissance Example

- U.S. Government
  - SCADA at Pearl Harbor



Social Engineering Video

eBay item 3090141797 (Ends Apr-13-04 11:16:47 PDT) - HAKO PLC HMI SCADA Touch screen + software - Microsoft Internet Explorer p

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=50423&item=3090141797&rd=1&ssPageName=WDVW Go Links

Click on a picture to enlarge

00239

FREE Counters and Services from Andale

Shipping and payment details

Shipping and handling: **GBP 15.50** (within United Kingdom)
Buyer pays for all shipping costs

Shipping insurance: GBP 4.00 (Optional)

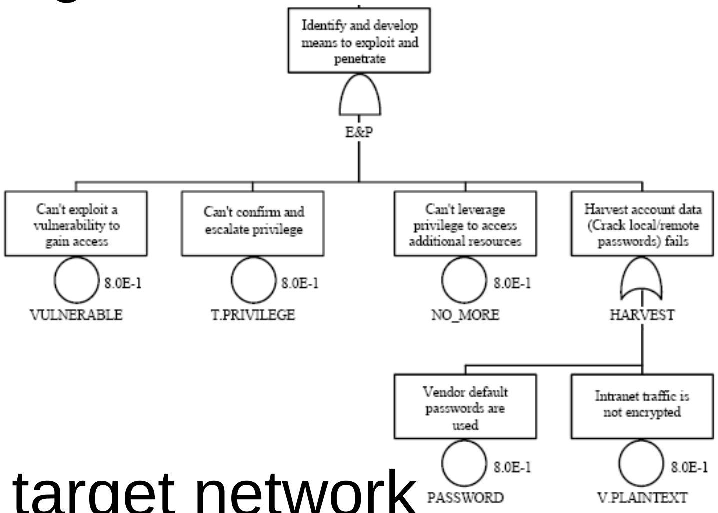
Will ship worldwide.

Seller's payment instructions & return policy:
Please make sure you put the auction # , & your name and address with all payments . Please NOTE Failing to give the details above will slow the dispatch of your goods ?? . Pay Via cheque Note cheques take up to 10 working days to fully clear . Postal Orders . Cash (via recorded delivery only) and @ senders risk . Payments via PAYPAL is exepted but must include the 20p + 5% surcharge as paypal fees are just costing to much

Done Internet

System Access (Exploit/Penetrate)

- Use attack vectors discovered in reconnaissance phase
- Develop attack schemas leveraging weaknesses
  - Viruses and Worms
  - Email
  - Hostile Web Pages
  - Direct Attacks



- Repeat reconnaissance once on target network
  - Map internal assets
  - Map peer connections

Keeping Access

- Depending on goals, attacker may/may not care
- Escalation of privileges
- Account creation
  - Becoming a trusted user
- Password cracking
- Backdoors / Trojan Horses
- Rootkits

Covering the Tracks

- Physical damage
- Hiding files
- Log file modification / deletion
- Covert channels (loki, ncovert)
- Hiding activity
  - Altering operators view at HMI

Idaho National Laboratory

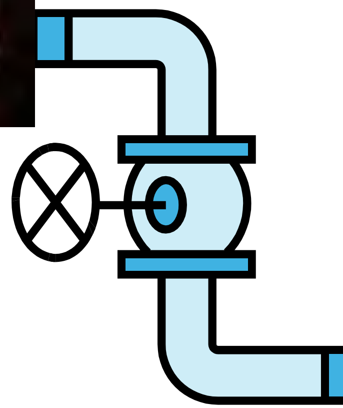
Video Demonstration

Recent Accidents

- Three accidents during 2005 resemble the Chem-Spill demonstration in the video.
  - Taum Sauk (Missouri)
  - Buncefield (UK)
  - BP Refinery (Texas)
- Faulty information and improper response to control system displays

Taum Sauk Failure 12/14/05

Taum Sauk – Pumped Storage



- Control indicated incorrect level
- Pumping continued
- Dam overflowed
- Dam washed out

Buncefield Petroleum Tank Explosion 12/11/2005

- A fuel-level gauge stuck
- Records showed an "anomaly" in the gauging system
- Pumping continued
- Tank overflowed
- Secondary safety system failed

Idaho National Laboratory

Texas City, 3/23/05

- Gauge-in-error assumed correct
- Accurate-gauge assumed wrong
- 15 dead, 170 injured, economic losses in excess of $1.5 billion

(Chemical Safety Board)

Photo by Dwight C. Andrews

Idaho National Laboratory

Impact of Database Attacks

NATIONAL TRANSPORTATION SAFETY BOARD
Public Meeting of October 8, 2002
(Information subject to editing)
Report of Pipeline Accident
Pipeline Rupture and Release of Gasoline, Olympic Pipeline Company
Bellingham, Washington
June 10, 1999
NTSB/PAR/02-02

EXECUTIVE SUMMARY

About 3:28 p.m., Pacific daylight time, on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek. Two 10-year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham's water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least $45 million.

Idaho National Laboratory

Impact of Database Attacks (cont)

5. If the supervisory control and data acquisition (SCADA) system computers had remained responsive to the commands of the Olympic controllers, the controller operating the accident pipeline probably would have been able to initiate actions that would have prevented the pressure increase that ruptured the pipeline.

6. The degraded SCADA performance experienced by the pipeline controllers on the day of the accident likely resulted from the database development work that was done on the SCADA system.

7. Had the SCADA database revisions that were performed shortly before the accident been performed and thoroughly tested on an off-line system instead of the primary on-line SCADA system, errors resulting from those revisions may have been identified and repaired before they could affect the operation of the pipeline.

8. Olympic did not adequately manage the development, implementation, and protection of its SCADA system.

Impact of Database Attacks (cont)

photo by David Willoughby copyright *Bellingham Herald*

copyright 1999 nwcitizen.com

Idaho National Laboratory

Mitigations

Firewalls and Intrusion Detection

Some History

- Like the Internet, the firewall has its roots in the military
- Designed to ensure secure collaboration between trusted environments
- Commercial products emerge early 1990's
- Two types of firewalls
  - OS-specific shields
  - Hardened kernel stand-alone
- Next generation designs encapsulate intrusion detection, intrusion prevention, heuristic analysis, use-models

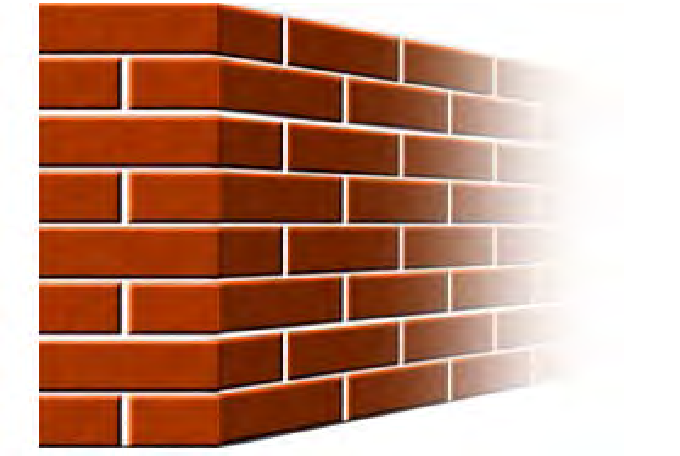
How does this impact migration from proprietary communications to standards-based protocols?

Firewall Functions

- **Protect the inside from the outside**
- **Protect the outside from the inside**
- **Enforce security policy**
- **Track network activity**

Firewall Rules

- **Actions to be taken: accept, drop, reject**
- **Locked down firewall rules or router ACLs (Access Control List)**
  - **IP/port security**
  - **Only allow necessary traffic into control network**
- **Monitoring firewalls: logs, Intrusion Detection System**
- **Use 'whitelist' connections**

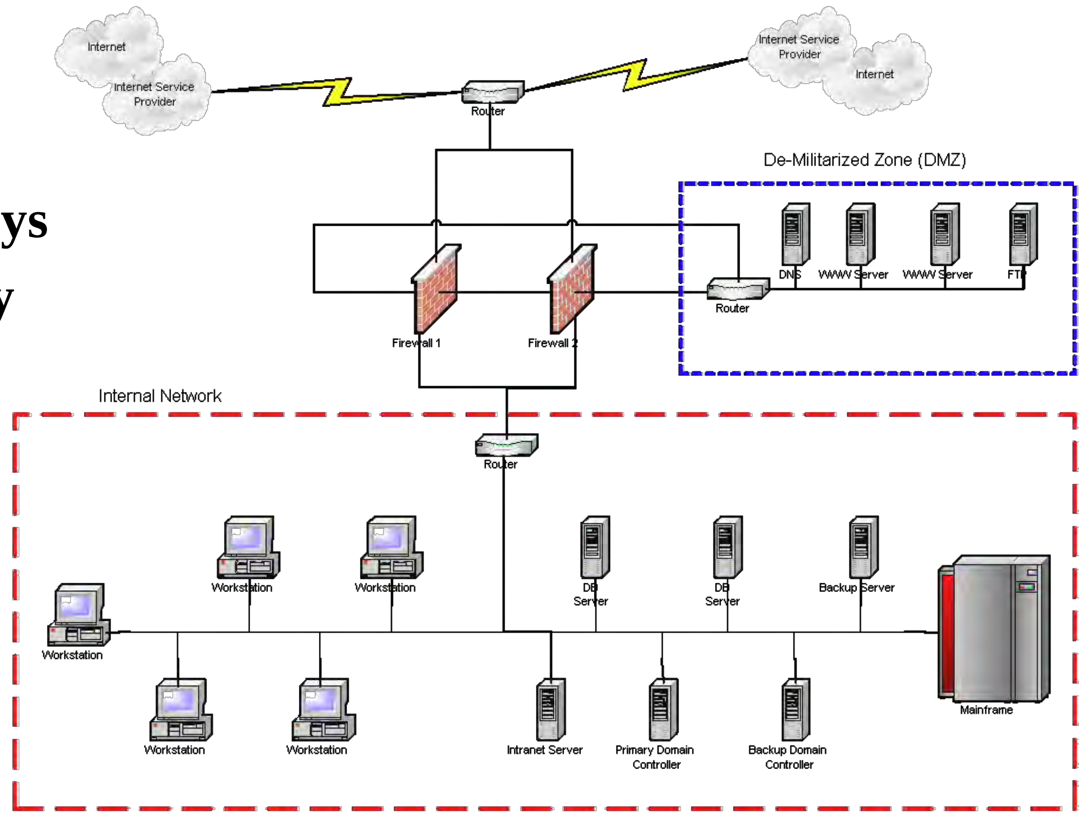


Key Firewall ‘components’

- **Deployed with the golden rule**
  - *That which is not explicitly allowed is denied*
- **Deployed with domain separation**
- **Monitor system events**
- **Protected audit trails that have been created**
- **User authentication before any action**
- **Self-test capability**
- **Supports a ‘trusted path’ to users and a 'trusted channel’ to other IT devices**

Firewall Diversity

- **Types vs. Classes**
  - **Packet filter**
  - **Circuit Level Gateways**
  - **Proxy Level Gateway**
  - **Stateful Inspection**
- **Hybrid Solutions**
  - **Multiple firewall/firewall**
  - **Cross vendor**
  - **Layer2/3 switching**
  - **Virtual Private Network**



Firewall and Defense-in-Depth

- **Traditional model used in open systems connectivity (n-tier architectures)**
  - **Network–Host–Application**
- **Segregation of the security zones provided by firewalls**
  - **Support security policy**
  - **Supports corporate policy**
  - **Supports best practices**
- **Rule-base may be more important than location of firewall**

Promotes the data sharing between trusted domains

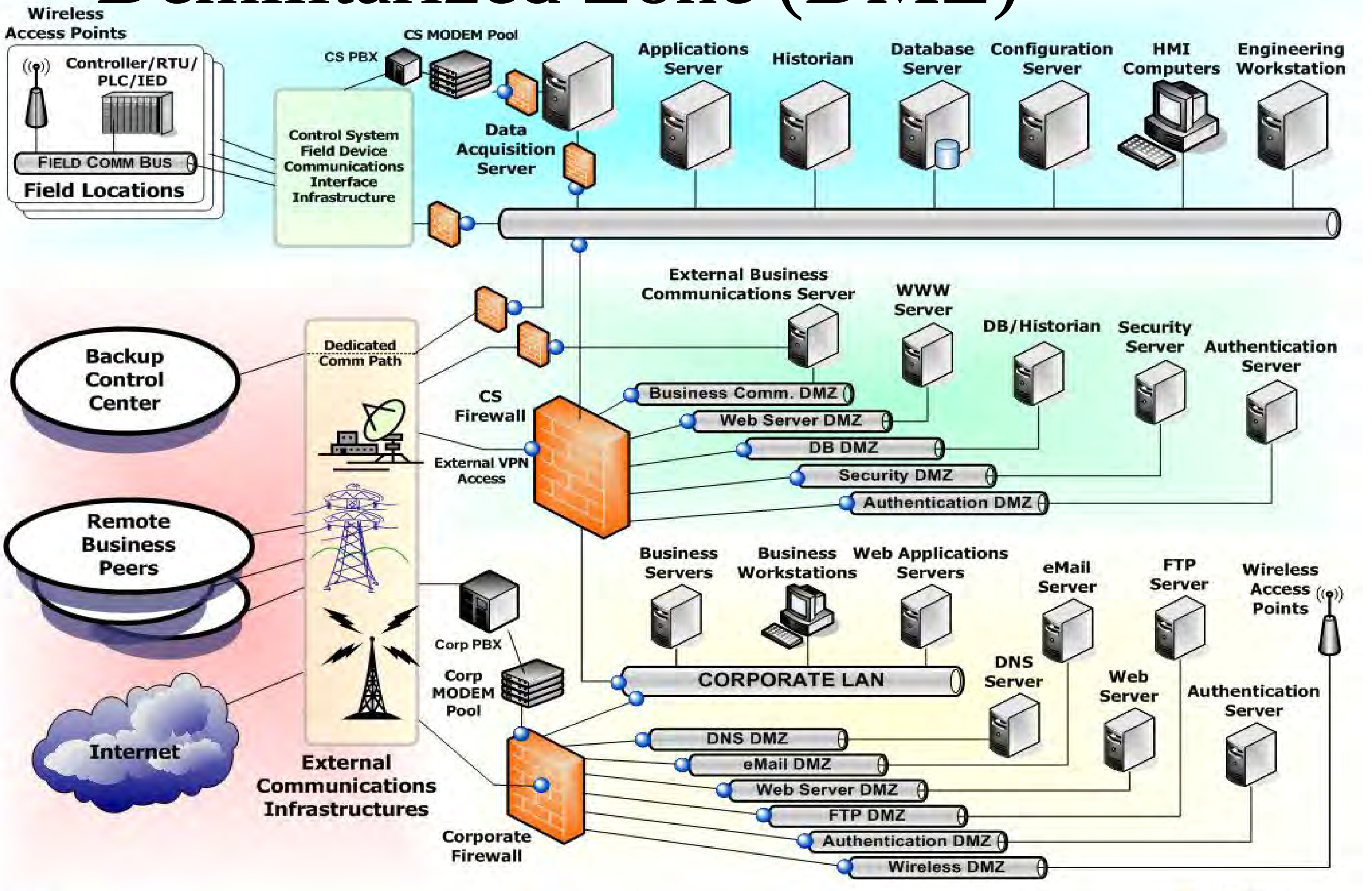
Idaho National Laboratory

Traditional Firewall Centric Defensive Problems

- **Denial of Service**
  - **Request overload**
  - **Reassembly attacks**
  - **Connection flooding**
  - **Key generation attacks**
- **Fragmentation**
  - **Perimeter bypass**
- **Covert Channels**
- **Session Hijacking**
- **Bounce Attacks (where firewall has inherent servers)**
- **Token-based *'race'* attacks**

Idaho National Laboratory

Demilitarized Zone (DMZ)



INL Idaho National Laboratory

Firewall Conclusions

- **Still no accepted standard (OS blanket / hard kernel)**
- **Trade-off of speed/throughput vs. security vs. cost**
  - **How does risk factor into the decision?**
- **Erroneously deployed as lynch-pin of architecture**
- **Out of the box modifications lead to:**
  - **Transformation of firewall into router**
  - **Firewall becomes a simple proxy gateway**
  - **Broken on-stack DNS (Domain Naming System)**
    - **Divulge internal naming structure**
- **Firewall often introduces massive architecture rebuilds**

Firewall Conclusions

- **Firewalls are complex devices that need a lot of careful design, configuration, and management if they are to be effective**
- **Firewalls are one line of defense, not our only line of defense**
- **There is an emerging focus on firewall for the Process Control Network/SCADA domains**

Basic IDS (with anti-Malware) Categories

- **Network Intrusion Detection Systems (NIDS)**
- **Host-Based Intrusion Detection Systems (HIDS)**
- **Intrusion Prevention Systems (IPS)**
- **Anti-Virus/BOT Scanners (AVS)**

Idaho National Laboratory

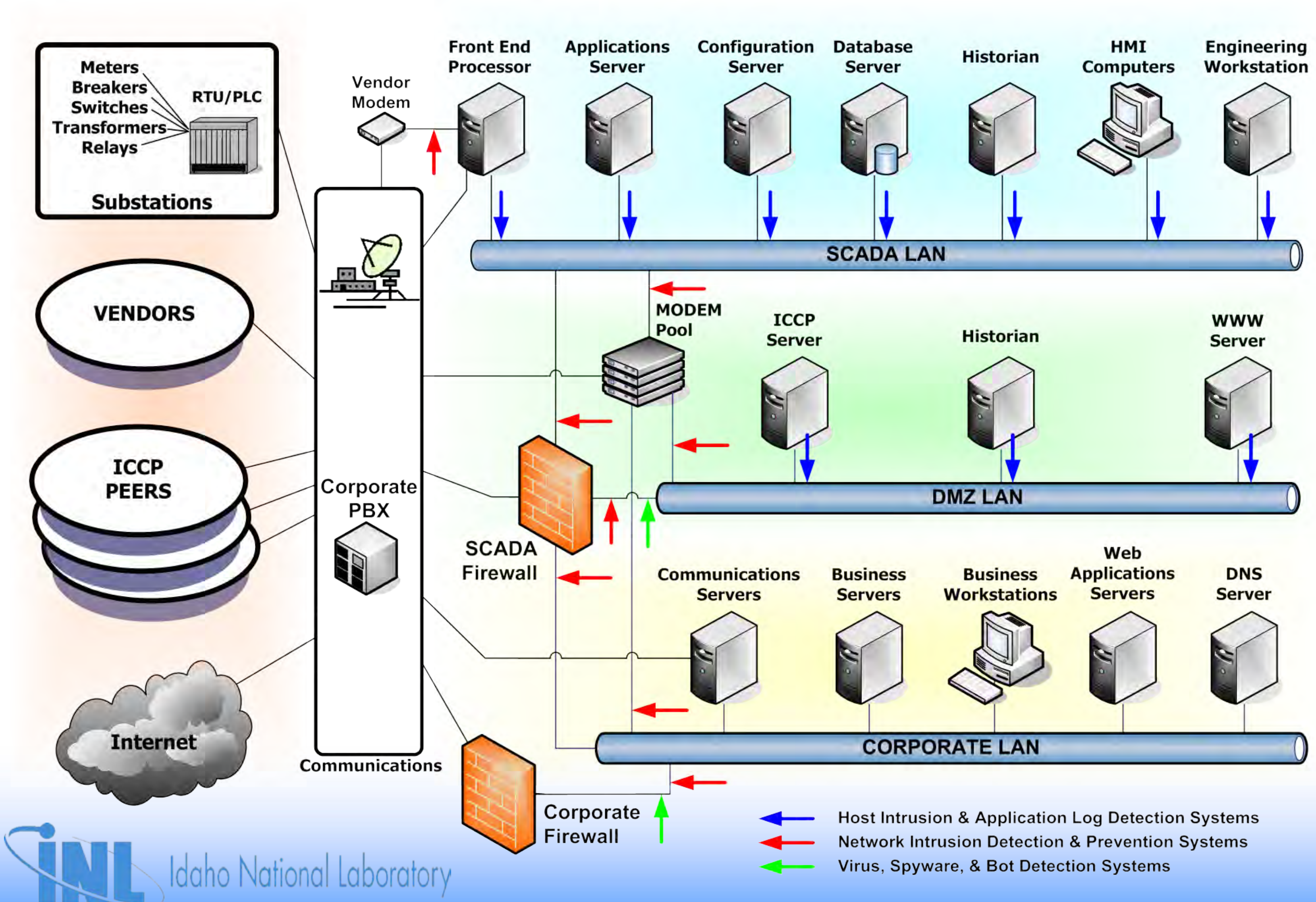
IDS Functions

- **Are your firewalls doing their job?**
- **Are your company policies being followed?**
- **Are servers affected by malicious traffic?**
- **Are there mis-configured systems?** (Data leakage)

Rule Sets

- **Actions taken: notification, alerting**
- **Writing rules**
- **Data collection**
- **Monitoring Intrusion Detection System**

IDS Placement Overview



Adding Control System Intelligence

- **Funded Homeland Security Advanced Research Projects Agency (HSARPA)**
  - **Snort IDS rules for SCADA Protocols**
    - **Phase 1 – Modbus TCP, DNP3, OPC**
  - **Data Dictionary for SCADA Application Logs**
    - **Phase 1 – 19 Events**
  - **Invited proposal for Phase II Research Contract**

Current CS-specific IDS signature total about 70

PCS Snort IDS Rule Examples

- **Denial of service**
  - **Force reboot**
  - **Force listen-only mode**
- **Unauthorized clients**
- **Reconnaissance**
- **Buffer overflow attacks**

IDS Rule Example – write(unauth)

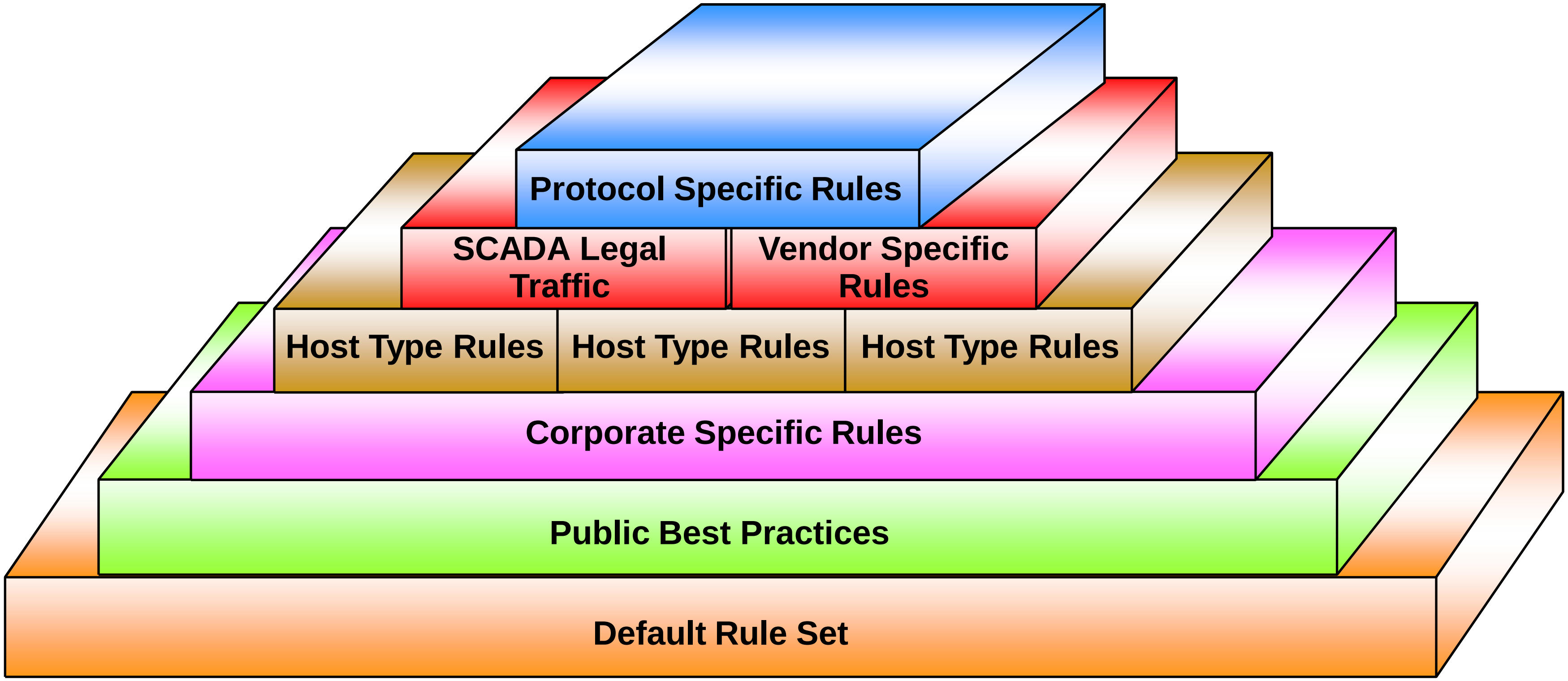
SIGNATURE ID	
Message	**Modbus TCP - Unauthorized Write Request to a PLC**
Rule	**alert tcp !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (flow:from_client,established; content:"|00 00|"; offset:2; depth:2; pcre:"/[\S\s]{3}(\x05|\x06|\x0F|\x10|\x15|\x16)/iAR"; msg:"Modbus TCP – Unauthorized Write Request to a PLC"; reference:scada,1111007.htm; classtype:bad-unknown; sid:1111007; rev:1; priority:1;)**
Summary	**An unauthorized Modbus client attempts to write information to a PLC or other field device.**
Impact	**System integrity. Denial of service.**
Information	**Modbus TCP is a protocol commonly used in SCADA and DCS networks for process control. The Modbus protocol does not provide authentication of the source of a command. Most SCADA/DCS networks have a limited number of HMI or other control devices that should read information from a PLC. An adversary may attempt to corrupt a PLC or set in a state to negatively affect the process being controlled.**
Affected Systems	**PLC's and other field devices that contain Modbus TCP servers.**

Idaho National Laboratory

Rule Strategy

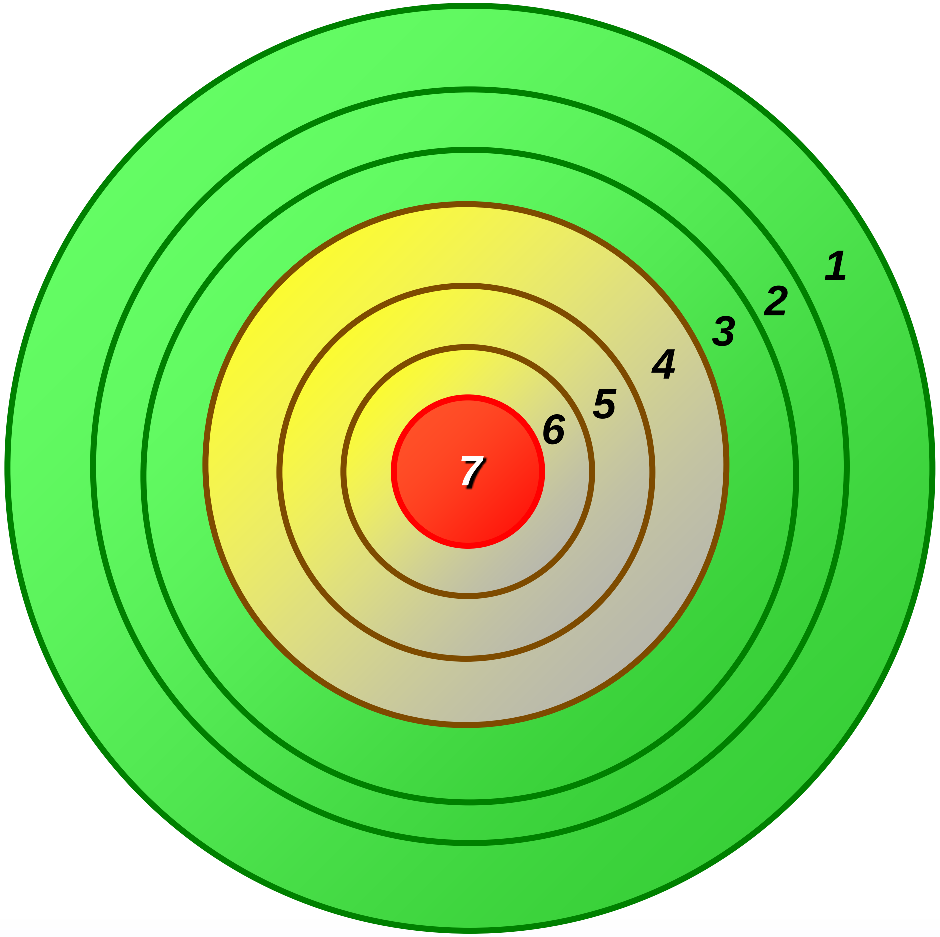
- **Level I**
  - **External Border and Corporate Systems**
- **Level II**
  - **Internal to the Firewall – Outgoing Traffic**
- **Level III**
  - **Modem Pool and DMZ – Back Door**
- **Level IV**
  - **Campus Sensors and Special Systems**

Rule Strategy (Cont’d)



Rule Set Should Build Upon Existing Rules

Defense in-Depth Security



1 Perimeter Controls –
Internet and Corporate Perimeter

2 Access Control,
People, Policies

Cyber Control

3 Network Architecture Components

4 Operating Systems

5 Host Security

6 Application Security

7 Core Operational Services

Idaho National Laboratory

Defense in Depth - Example

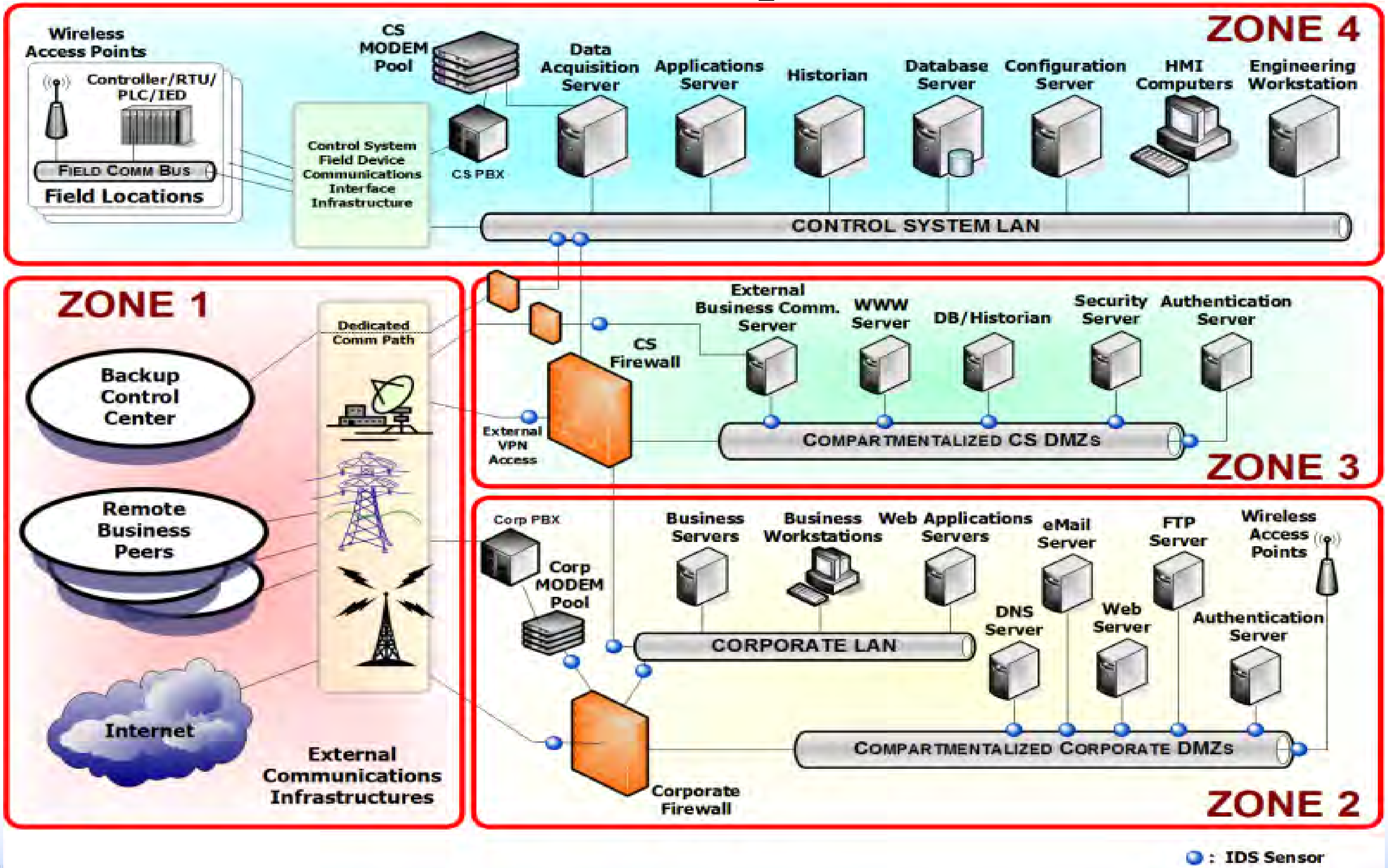
Component - A TL60 safe is rated to withstand a 60 minute attack by someone with proper tools, knowledge, etc

Vulnerability - We know it will take 60 minutes for someone to break into the safe

Mitigation - Schedule the guard to make 30 minute rounds of the area in order to mitigate the known vulnerability

Idaho National Laboratory

Zones in Control Systems



Idaho National Laboratory

Why vulnerability testing?

- Provides you with information on weaknesses
- Can detail what patches are needed
- Detects software not authorized by security plan
- Locate systems with auto-answer modems
- Provide a list of hosts and their operating system

Security Vulnerability Testing

A security vulnerability scanner is software which will audit a given network of hosts and determine whether someone (or something – like a worm) may break into the hosts, or misuse them in some way.

- **Nmap (http://www.insecure.org) - Nmap uses raw IP packets in novel ways to determine what hosts are on a network, what operating systems and versions they a using.**
- **Nessus (http://www.Nessus.org) – Checks systems and applications for known vulnerabilities.**
- **CIS benchmark kits (http://www.cisecurity.org) – A set of security configuration benchmarks used to audit a host for security settings.**
- **Many others available**

Vulnerability Testing - Warning

- Only tests vulnerabilities they know
- May need more than one tool for complete test
- Only good for that moment in time
- Most corporations have rules against unauthorized use of these tools
- Should NOT be used on production networks

Idaho National Laboratory

Training – A MUST!!!

- Your Hardware Vendors
- SANS http://www.sans.org
- Foundstone http://www.foundstone.com
- NIST http://csrc.nist.gov/ATE

Resources

- **SANS.org Resources**

  http://www.sans.org/resources

- **Idaho National Laboratory**

  http://www.inl.gov/scada

- **Securitywizardry.com**

  http://www.securitywizardry.com

- **US-CERT**

  http://www.us-cert.gov/control_systems

Wrapping Up

Common Sense for Control Systems

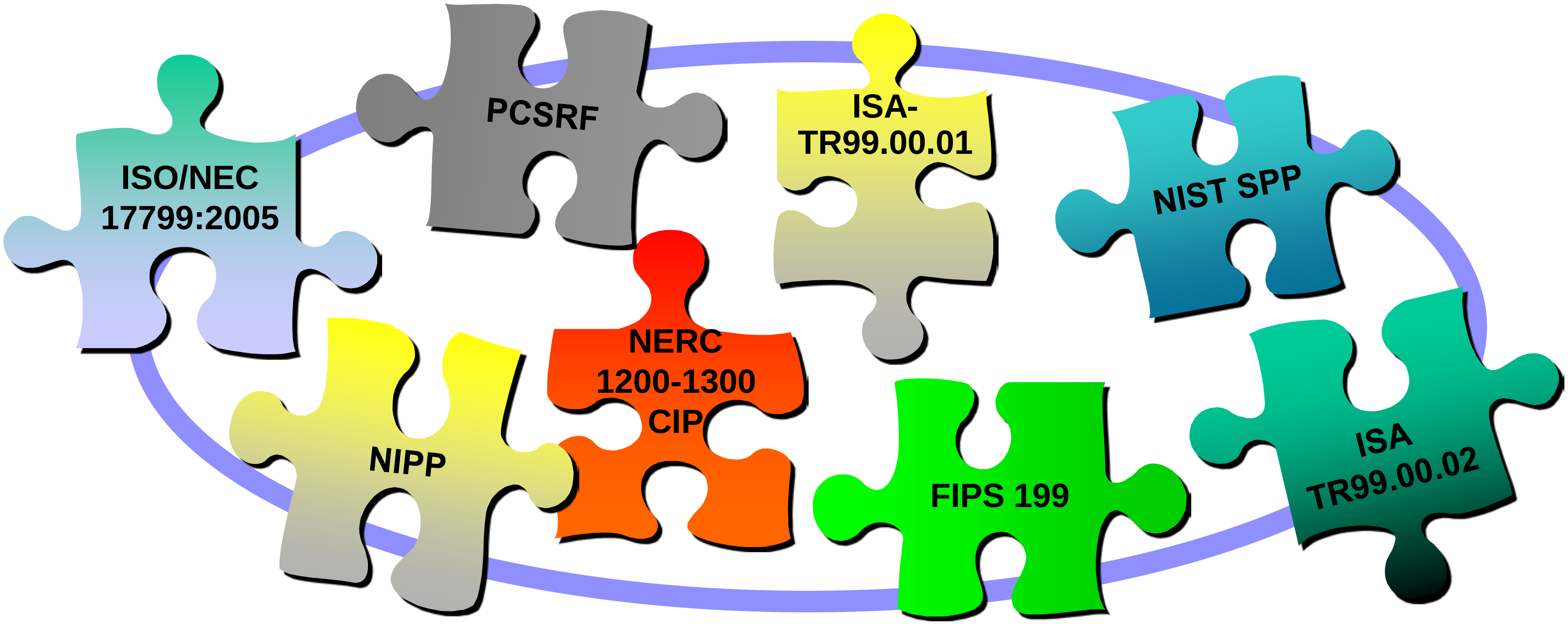
- **ICCP Capability links should only move ICCP traffic**
- **Secure critical clear text traffic**
- **Use host tables instead of Domain Naming System**
- **Reconsider Internet Control Message Protocol on the Control System local area network (LAN)**
- **Update default parameters**
- **Remove unused services (disable ports)**
- **Restrict outbound traffic from Control LAN**
- **Use separate (secure) log servers for logging**
  - **Aggregate to a central (secure) location**
- **Dedicated policies for wireless and remote access (Virtual Cluster Number, etc.)**

Incidents and Forensics

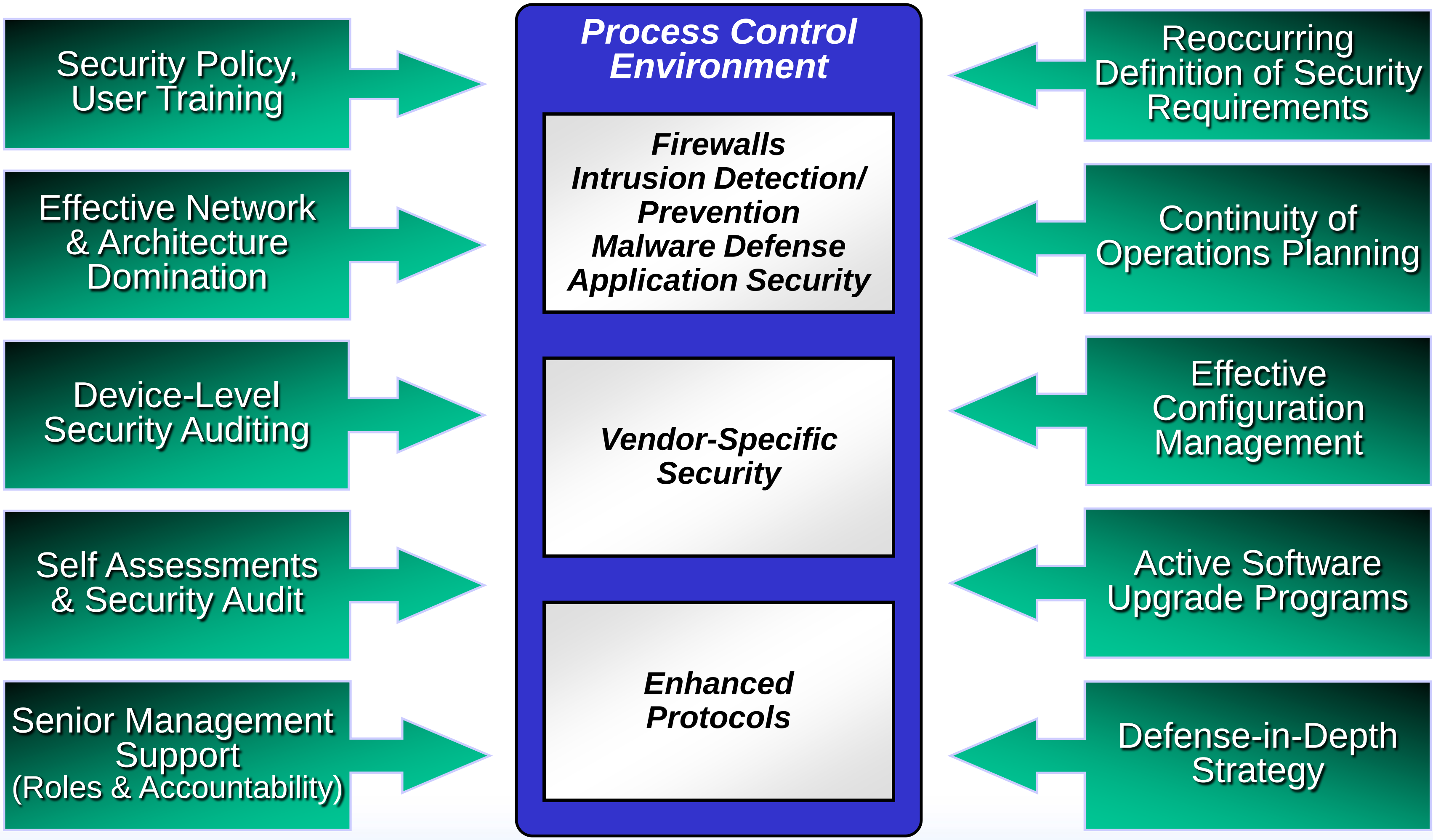
- **Connection attempts on traditional Control System ports (including 6000)**
- **Review RIP v1 traffic (no authentication)**
- **ARP (Address Resolution Protocol) table corruption**
- **Excessive log files, Excessive log file sizes**
- **Log file tampering (checksums, etc.)**
- **IDS logs with aftermarket modules (i.e., MODbus scanning)**
- **Replayed HMI (Human Machine Interface) traffic (repeated timestamps)**
- **Control System LAN DNS (Domain Naming System) poisoning**
- **Excessive P2P (Peer to Peer) connections**
- **rlogin/rsh at inappropriate time of day**

Effective Guidance – How to Start?

There is an entire suite of effective policy guidance available!



Cyber Security Foundations



Idaho National Laboratory

US-CERT Control Systems Security Program

- **Dedicated function of US-CERT for supporting security of Control Systems**
  - Supported by Idaho National Laboratory
  - Facilitate the US-CERT capability to coordinate control systems incident management and
  - Assess vulnerabilities and risks associated with control systems
  - Enhance control systems security awareness through training and outreach initiatives
  - Provide strategic recommendations for control systems security research and development needs
- **CS^{2}SAT Assessment Toolkit**
- **Recommended Practices program**
- **Procurement Language (Draft v1.5)**

http://www.us-cert.gov/control_systems

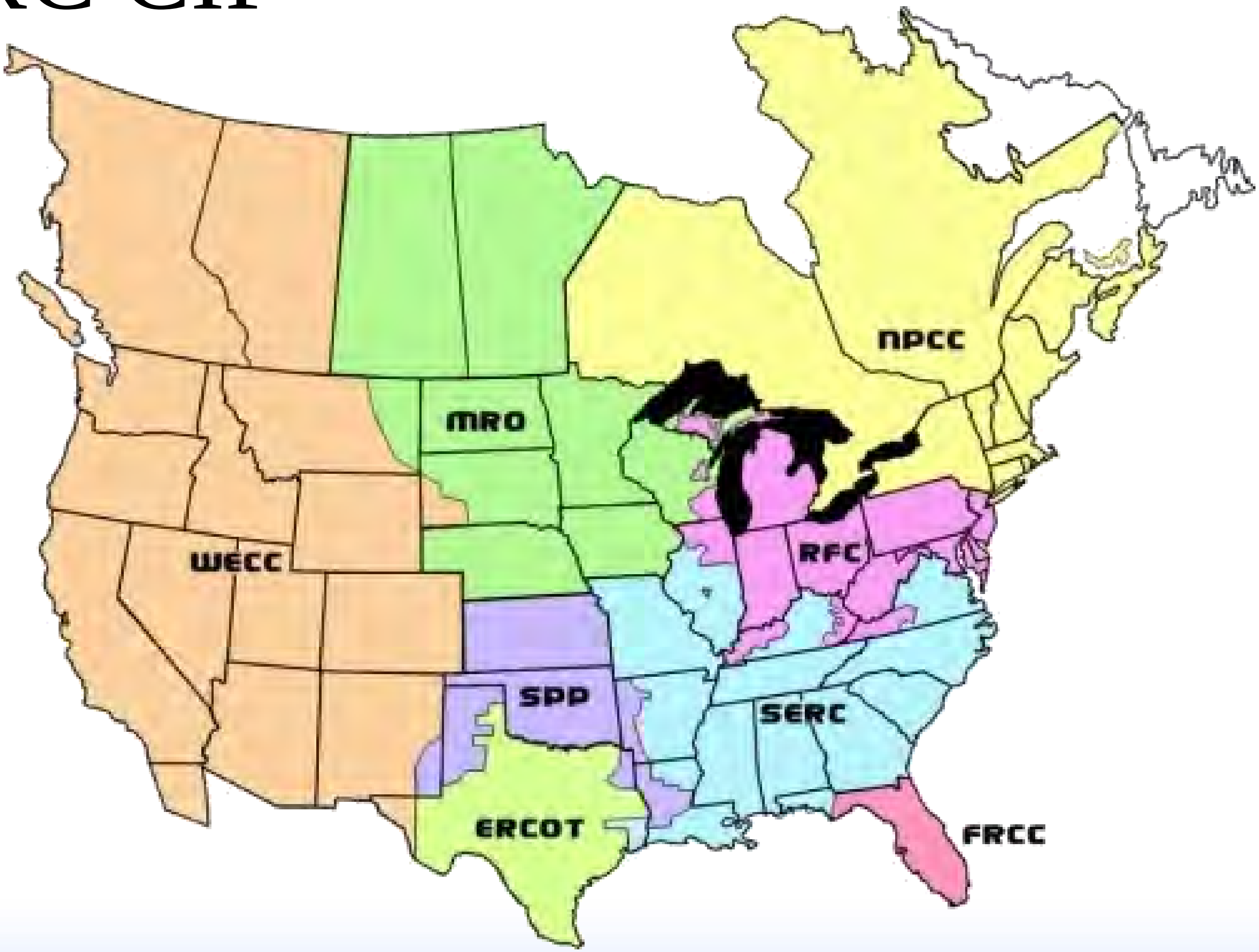
Idaho National Laboratory

Layered Security Model

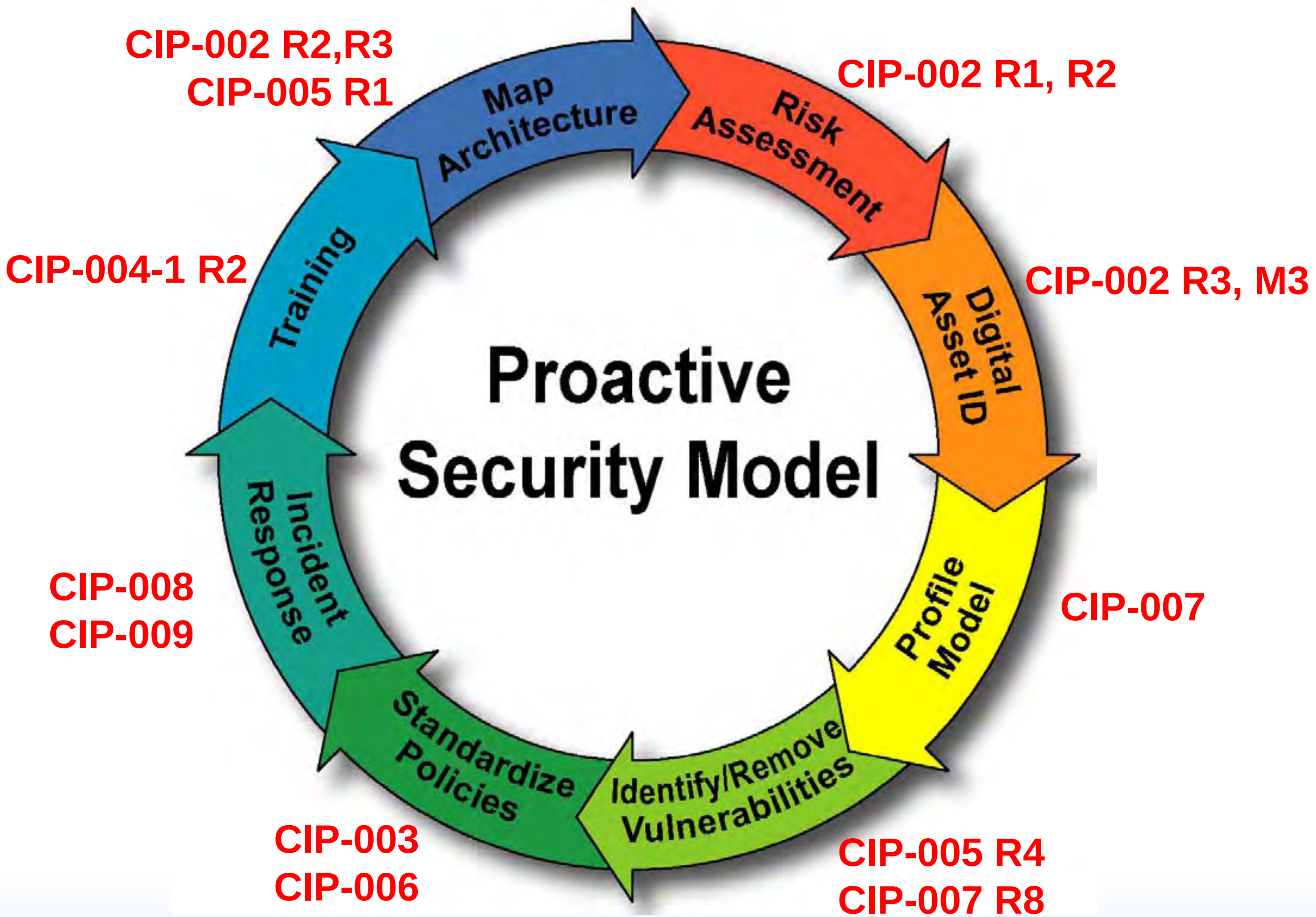
Idaho National Laboratory

NERC Mitigation Activities

NERC CIP



Security is a Never Ending Process



Idaho National Laboratory

Idaho National Laboratory

2005 “Top 10” Vulnerabilities

Identified by the NERC Control System Security Working Group (CSSWG)

NERC Top 10 Vulnerabilities - 2005

1. Policies, procedures & culture governing control system security are inadequate and lead to lack of executive management buy in. In addition, personnel routinely ignore or lack training in policies and procedures to protect the control systems.
2. Poorly designed control system networks that fail to employ sufficient defense-in-depth mechanisms.
3. Remote access to the control system through means which do not provide identity control.
4. Prescribed system administration mechanisms are not part of control system implementation.
5. Use of wireless communication

These are not in any order of importance

NERC Top 10 Vulnerabilities - 2005

6. Lack of a dedicated communications channel for command and control in applications such as Internet based SCADA, and inappropriate use of control system network bandwidth for non control purposes.
7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity. Non existent forensic and audit methods.
8. Installation of inappropriate applications on critical systems.
9. Software used in control systems is not adequately scrutinized, and newer systems include extraneous vulnerable software.
10. Control systems data sent in clear text.

Idaho National Laboratory

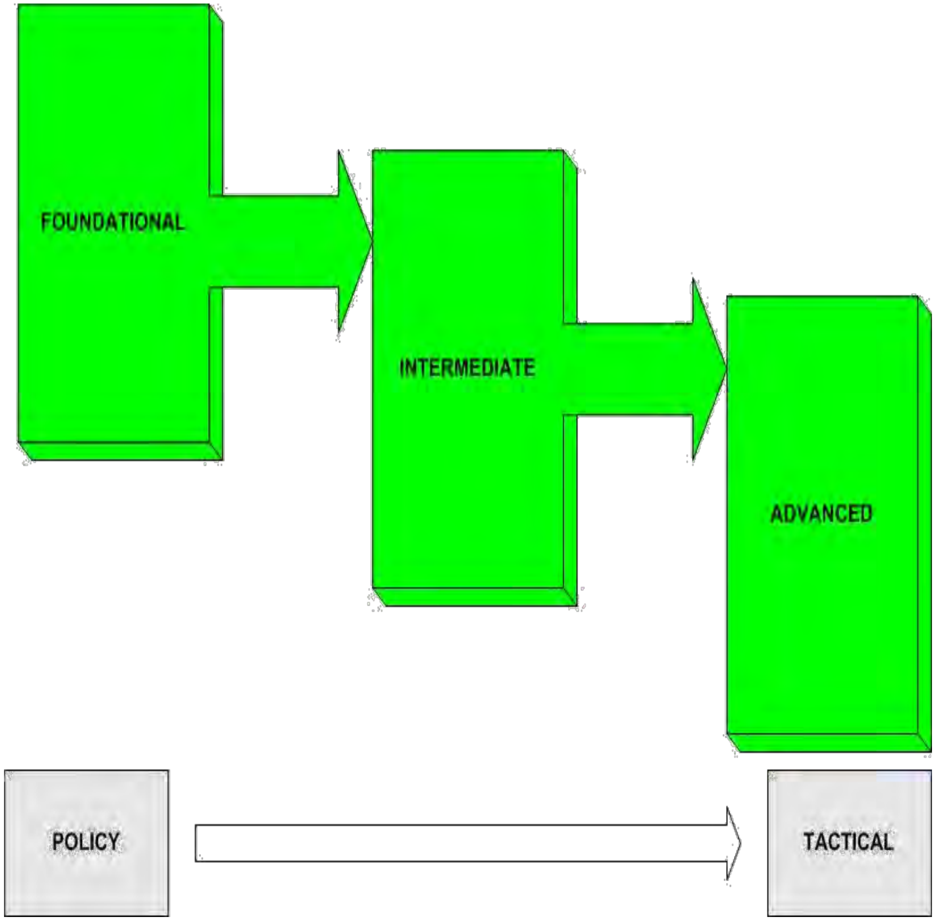
These are not in any order of importance

Preface

- The following mitigation strategies may be applicable to some electricity sector organizations and not applicable to others.
- Each organization must determine the <u>risk</u> it can accept and the practices it deems appropriate to mitigate vulnerabilities.
- If an organization can not apply some of the technology suggested here, then other strategies should be applied to mitigate the associated vulnerability.

Three (3) levels of mitigation

- ***Foundational***
  - Policy driven functions that are programmatic and leverage traditional non-IT activities
- ***Intermediate***
  - Initial tactical programs that provide for the implementation of management direction using IT-based activities
- ***Advanced***
  - Granular IT security activities that are supportive of foundational and intermediate goals, and may require expertise for deployment of specific technologies



Vulnerability 1 Mitigations

Inadequate policies and procedures governing control system security

- *Foundational*
  - Implement policies and procedures governing control system security. (ref: NERC CIP Standards)
- *Intermediate*
  - Share industry best practices in security policy structure and topics.
  - Enforce policies and procedures governing control system security.
- *Advanced*
  - Adopt a process for continuous improvement for implementation and enforcement of policies and procedures governing control system security.

Security Policy

- Corner stone of your network security!
- Empowered by technology
- Enforceable with management oversight
- Users need to know the whys
- Reviewed annually or sooner
- Recursive testing to validate policy

Policy Components

- Organizational Security
- Asset Classification
  - Documentation
  - Communications
- Personnel Security
- Physical Security
  - Doors, locks, guards, CATV
- Communications Management
- Access Control
  - LDAP, MS AD
- Systems Development
  - Applications
  - After-market technology
- Business Continuity
  - COOP
  - Resiliency
  - Business Continuity
- Compliance
  - SOX
  - NERC

Vulnerability 2 Mitigations

Poorly designed Control System Networks

- *Foundational*
  - Implement electronic perimeters. Disconnect all unnecessary network connections. (ref: Control System - Business Network Electronic Connectivity Guideline)
- *Intermediate*
  - Implement concentric electronic perimeters. Use autonomous networks with minimal shared resources between control system and non-control system networks.
  - Training: supply company’s best practices and guidelines to new employees, vendors, integrators.
- *Advanced*
  - Implement virtual LANs, private VLANS, intrusion prevention, anomaly detection, smart switches, etc.

Vulnerability 3 Mitigations

Misconfigured operating systems and embedded devices

- *Foundational*
  - Conduct inventory. Ensure sufficient training of personnel responsible for component configuration and maintenance.
- *Intermediate*
  - Evaluate and characterize applications. Remove or disconnect unnecessary functions.
  - Patch management process: Hardware, firmware, software. Maintain full system backups and have procedures in place for rapid deployment and recovery. Maintain a working test platform and procedures for evaluation of updates prior to system deployment. (ref: Patch Management Guideline)
- *Advanced*
  - Active vulnerability scans. (Caution: recommend use of development system so that on-line control systems are not compromised during the scan.) Disable, remove, or protect unneeded or unused services/features that are vulnerable.

Vulnerability 4 Mitigations

Use of inappropriate wireless communication

- *Foundational*
  - Establish a policy on where wireless may be used in the system.
  - Implement WEP.
- *Intermediate*
  - Implement 802.1x device registration.
- *Advanced*
  - Implement WPA encryption and 802.1x device registration along with unregistered device detection.
  - Use PKI and certificate servers
  - Use non-broadcasting SSIDs
  - Utilize MAC address restrictions
  - Implement 802.11i

Vulnerability 5 Mitigations

Use of non-deterministic communication for command and control

- *Foundational*
  - Implement defense in depth architecture (e.g., multiple firewalls between control network and other networks).
- *Intermediate*
  - Implement technologies to enforce legitimate traffic.
- *Advanced*
  - Authenticate and validate control system communication.

Vulnerability 6 Mitigations

Lack of mechanisms to detect and restrict administrative or maintenance access to control system components

- *Foundational*
  - Perform background personnel checks on employees with access to sensitive systems. Ensure vendors and contractors have implemented similar procedures.
  - Establish a policy for system access including password authentication. Change all default passwords. Do not allow unsecured modems.
  - Use VPN technology when the Internet is used for sensitive communications.
  - Ref: Securing Remote Access to Electronic Control and Protection Systems Guideline

Idaho National Laboratory

Vulnerability 6 Mitigations – Cont.

Lack of mechanisms to detect and restrict administrative or maintenance access to control system components

- *Intermediate*
  - Define levels of access based on need. Assign access level and unique identifiers for each operator. Log system access at all levels. Implement network IDS to identify malicious network traffic, scan systems for weak passwords, separate networks physically.
- *Advanced*
  - Design access levels into the system restricting access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms. Use multi-factor authentication (e.g., two-factor, non-replayable credentials). Implement protocol anomaly detection technology.

Vulnerability 7 Mitigations

Lack of quick and easy tools to detect and report on anomalous or inappropriate activity

- *Foundational*
  - Install monitoring technology, e.g., Intrusion Detection System (IDS) to log all existing and potential points of entry into the system. Preserve logs for subsequent analysis.
- *Intermediate*
  - Install anomaly detection, actively monitor logs.
- *Advanced*
  - Work with vendors to develop appropriate tools to identify inappropriate control systems traffic.

Vulnerability 8 Mitigations

Dual use of critical control system low band width network paths for non-critical traffic or unauthorized traffic

- *Foundational*
  - Define critical network paths.
  - Restrict or eliminate non-critical traffic on the control network.
  - Segregate functionality onto separate networks (e.g., do not combine email with control system networks).
- *Intermediate*
  - Implement IDS to monitor traffic. Evaluate network traffic and control system point counts and polling rates. Reconfigure for optimal use of existing resources.
- *Advanced*
  - Update system technology to allow for higher bandwidth traffic. Separate critical and non-critical systems. Implement protocol anomaly and active response systems to enforce legitimate traffic.

Vulnerability 9 Mitigations

Lack of appropriate boundary checks in control systems that could lead to "buffer overflow" failures in the control system software itself

- *Foundational*
  - Actively monitor server status.
- *Intermediate*
  - Implement processes to automatically stop and restart services.
- *Advanced*
  - Enforce vendors' software development standards that incorporate secure software development techniques.

Idaho National Laboratory

Vulnerability 10 Mitigations

Lack of appropriate change management/change control on control system software and patches

- *Foundational*
  - Maintain a maintenance agreement with software vendors for update notification and distribution. Define change management process.
- *Intermediate*
  - Establish a schedule of checks for system updates for all applicable software, operating systems, and component firmware. Implement version control system and enforce change management process.
- *Advanced*
  - Utilize a dual redundant or clustered system architecture that allows for rebootable updates without requiring system downtime. Actively scan resources to ensure security patches are installed. (Caution: procedures should be developed that will ensure on-line control systems are not compromised as a result of the scan.)

THANK YOU

For more information about NSTB
www.inl.gov/scada

To contact us
Email: scadasummit@inl.gov
Phone: 866-495-7440

Idaho National Laboratory