Introduction SCADA Security for Managers and Operators

September 28, 29, 2006

Homeland Security

U.S. DEPARTMENT OF ENERGY

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
- Understanding the Risk
- Attack Trends and Attacker Profile
- Understanding Exposure
- Experiences from Field Visits
- Anatomy of an Attack
- 10 Minute Break
- Energy System Exploitation (DEMO)
- Demo Exploits and Mitigation Strategies
- Vulnerability Testing
- 10 Minute Break
- Network Components and Architecture
- Firewalls and Intrusion Detection
- 10 Minute Break
- NERC Mitigation Activities
- Interactive Exam Discussion
- 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***

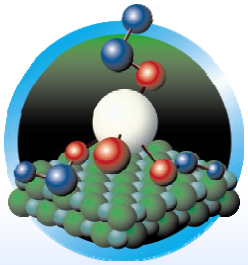
Idaho National Laboratory

The INL R&D

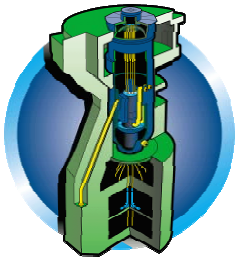
Mission execution is guided by five laboratory divisions

Nuclear Energy

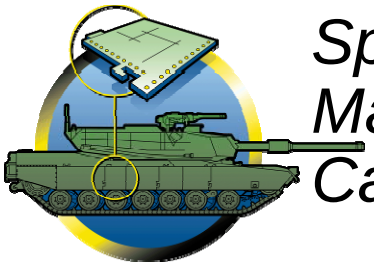
National Security



Science and Technology



Advanced Test Reactor



Specific Manufacturing Capability

Idaho National Laboratory

SCADA 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*

Idaho National Laboratory

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

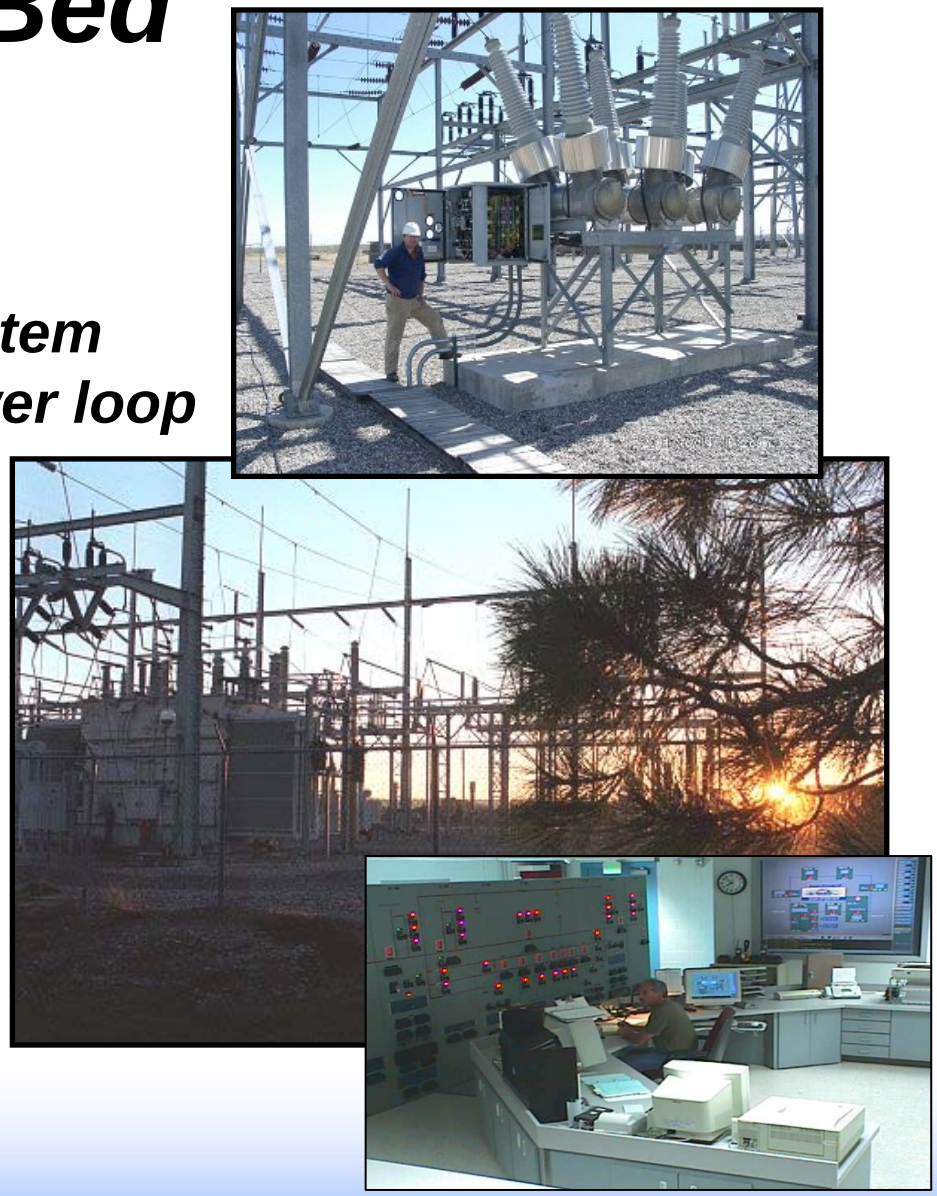
- America's only "city sized" wireless test facility
- 3 Cell tower system operational; potential to expand
- Testing next generation (3G/4G) wireless communication, wireless LANs and Land Mobile Radio systems
- Access to commercial and government spectrums as NTIA experimental test station
- Physically secure, interference free environment
- 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

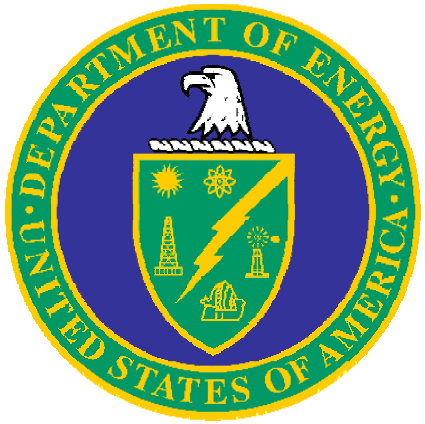
INL Critical Infrastructure Security Programs

National SCADA Test Bed

Control Systems Security Program

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



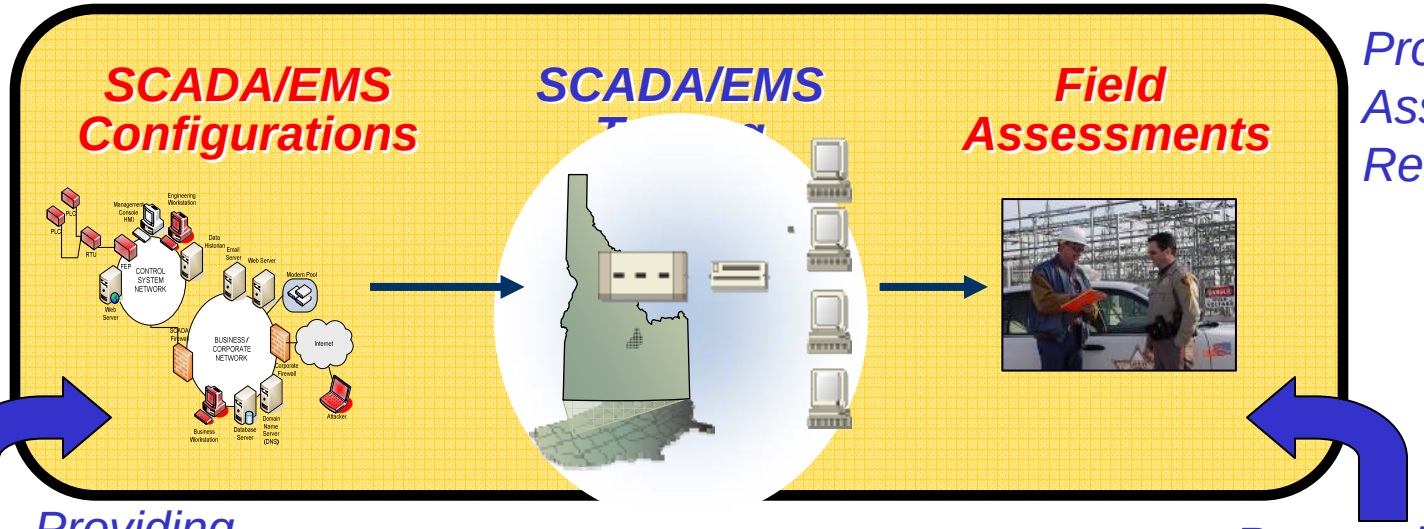
DHS Primary Objective

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.

All sectors involved in control systems.
Multiple National Laboratories.

Working Together to Deliver & Operate Secure Systems

National SCADA Test Bed



Providing Test Results

Providing Assessment Results

Providing figurations ning

Requesting Field Assessments

Requesting Security Testing

Vendor

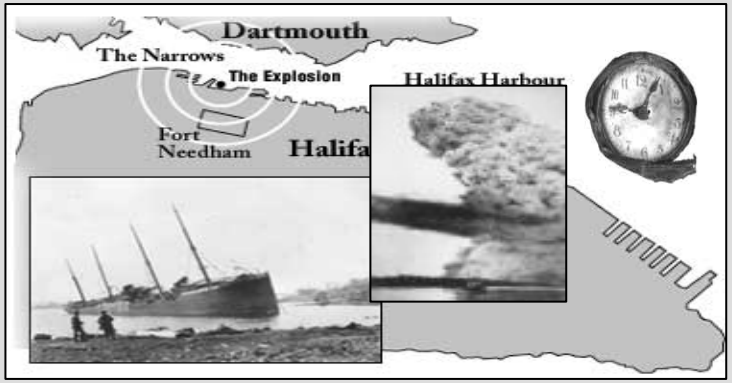
Providing Updated Systems and Testing Results

Asset Owners

Idaho National Laboratory

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

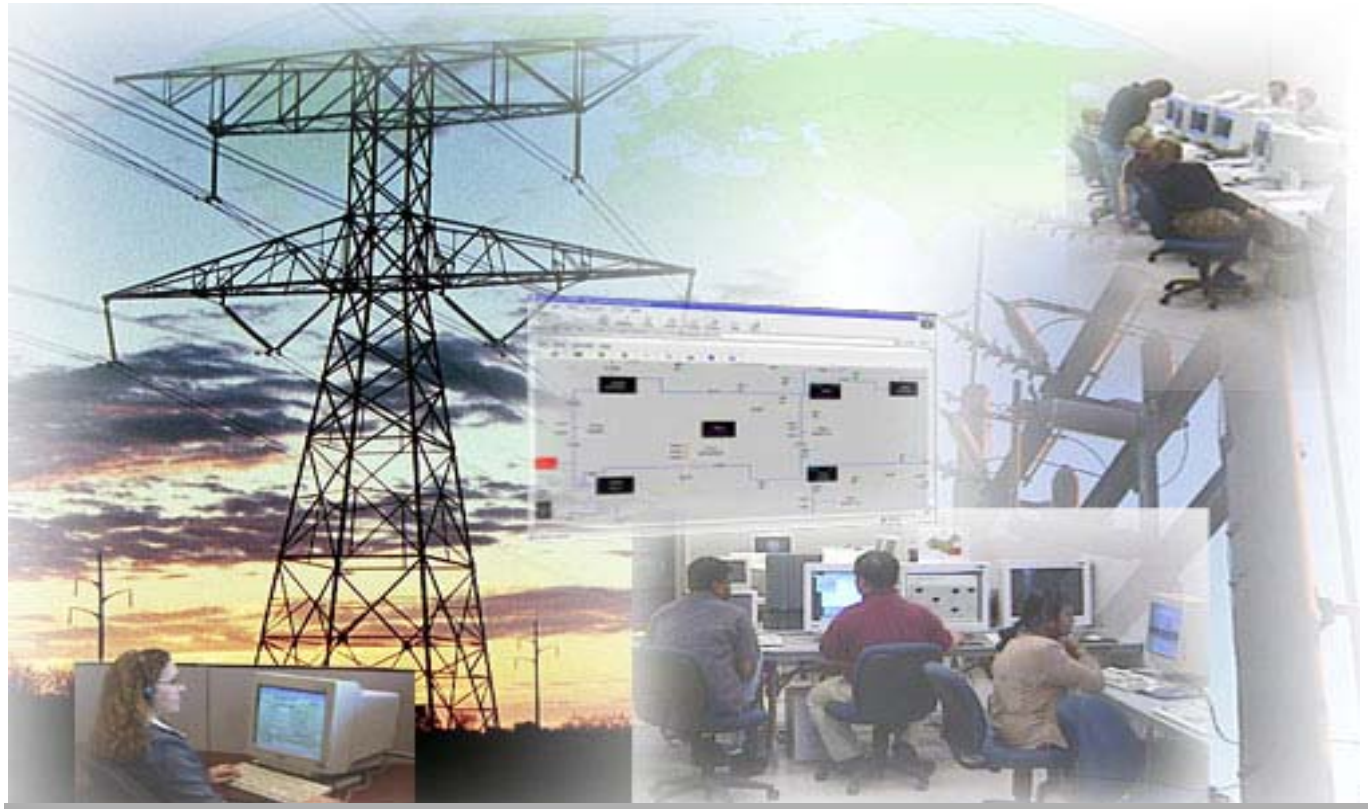
Idaho National Laboratory

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.*

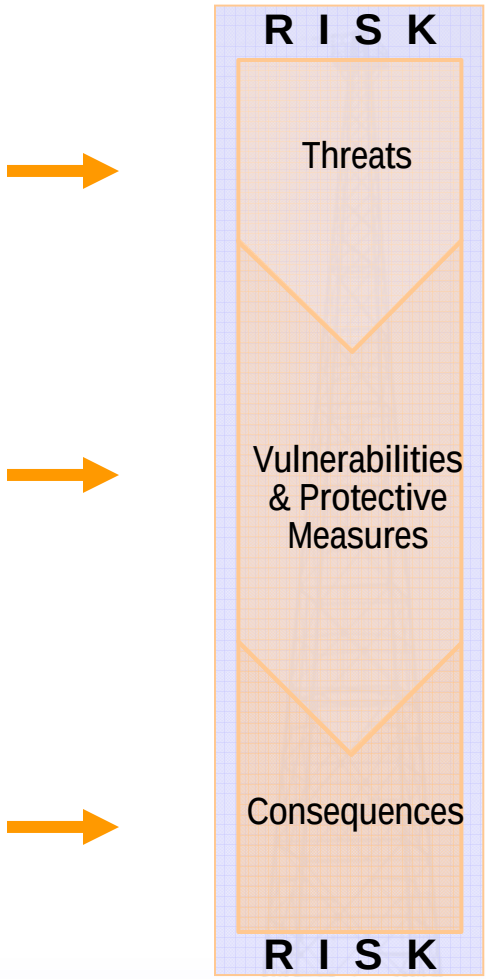
Risk is Elevated in Converged & Interconnected Systems



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

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

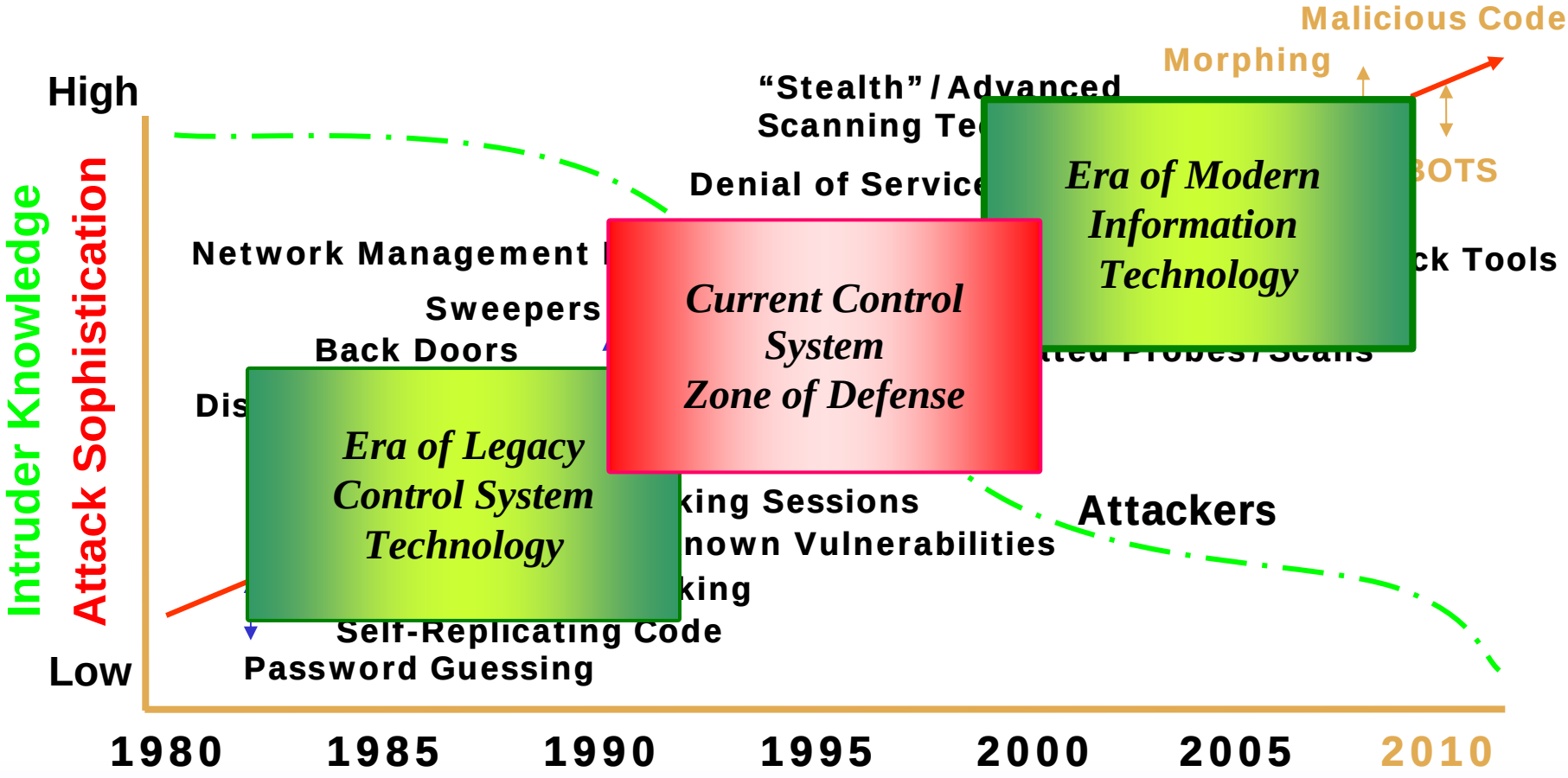


*A Program approach used at AEP

Attack Trends and the Attacker Profile

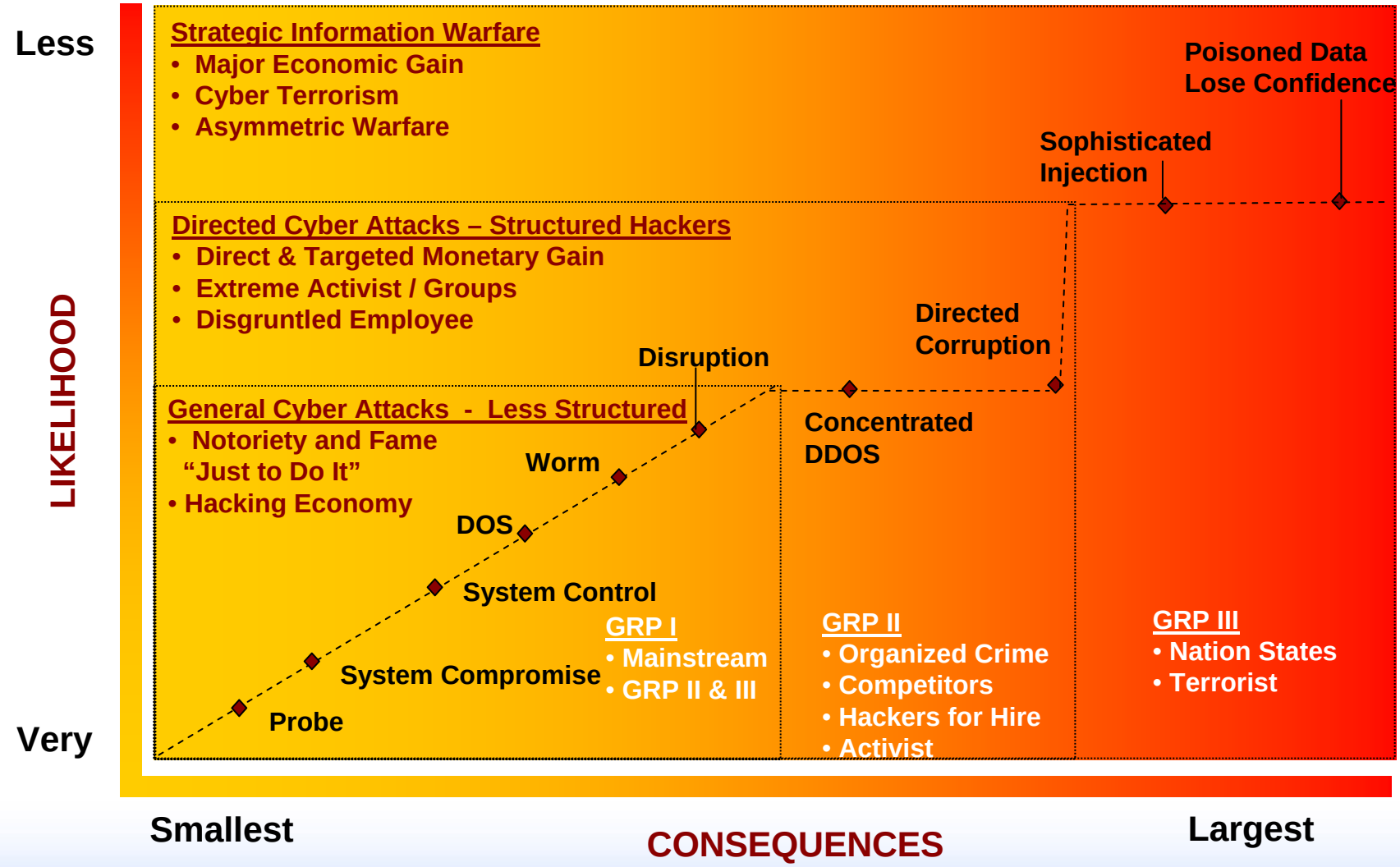
Threat Trends

- 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.

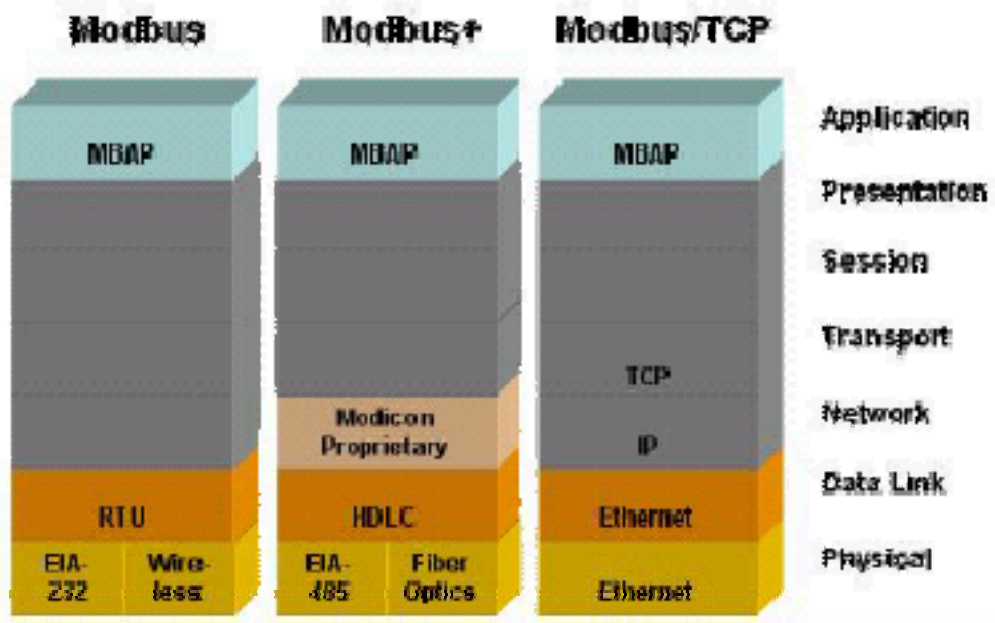
Cyber Threats: The Flattening of the Line



Idaho National Laboratory

Protocol Vulnerabilities

- No authentication amongst ‘isolated’ components
- Modbus/ICCP/DNP3 fully published and open for review
- OLE for Process Control (OPC)



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 Server heap buffer overflow vulnerability

Overview

LiveData ICCP Server contains a heap-based buffer overflow. This vulnerability may allow a remote attacker to crash the server.

I. Description

Inter-Control Center Communications Protocol (ICCP)

According to the LiveData ICCP Server white paper:

> *The Inter-Control Center Communications Protocol (ICCP) is being specified by utility organizations throughout the world to provide data exchange over wide area networks (WANs) between utility control centers, utilities, power pools, regional control centers, and Non-Utility Generators. ICCP is also an international standard: International Electrotechnical Commission (IEC) Telecontrol Application Service Element 2 (TASE.2).*

ISO Transport Service over TCP (TPKT, RFC 1006)

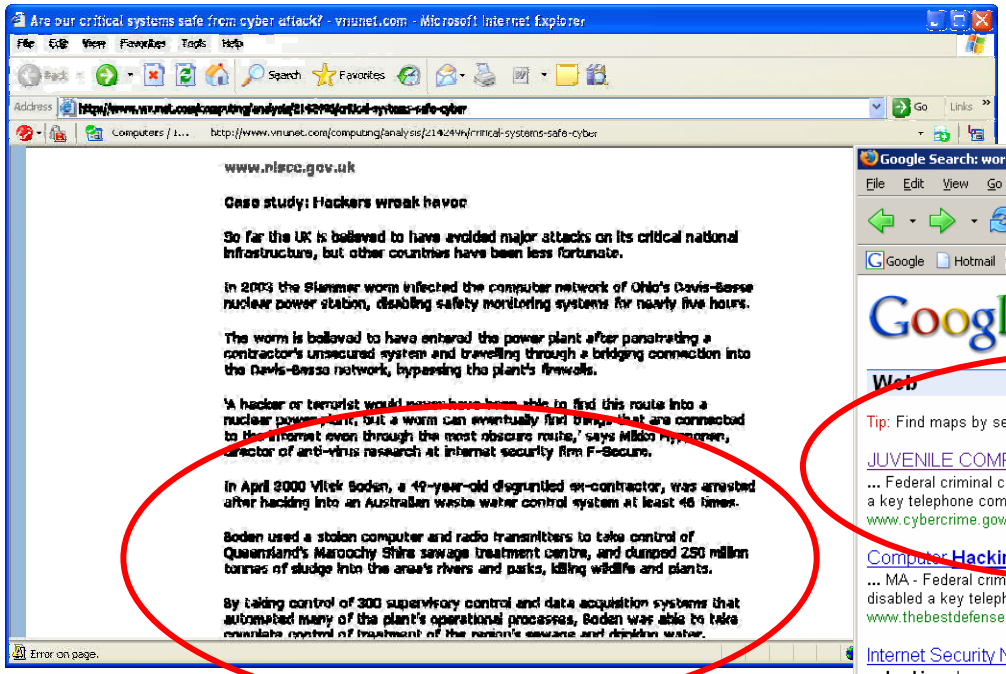
RFC 1006 specifies how to run the OSI transport protocol on top of TCP/IP. In the layered protocol model, RFC 1006 is situated between the TCP and OSI transport layers.

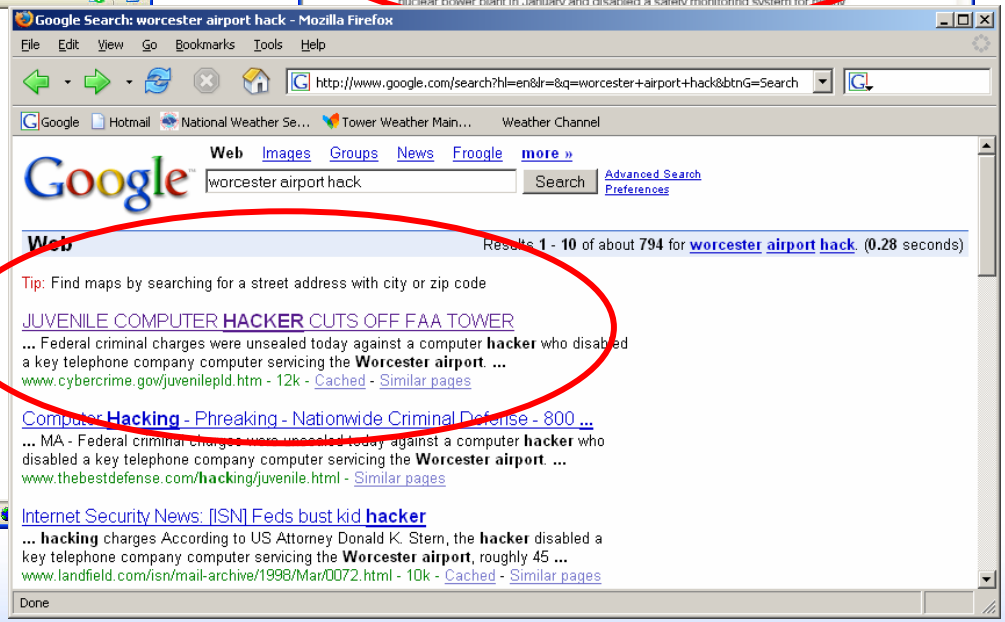
LiveData ICCP Server and LiveData Server

LiveData ICCP Server records and transmits data to other control points in process control networks. According to the LiveData ICCP Server white paper:

Effects of Cyber on Critical Infrastructure

- Davis-Besse Nuclear Power
- Australian Sewage Release
- Worcester Airport

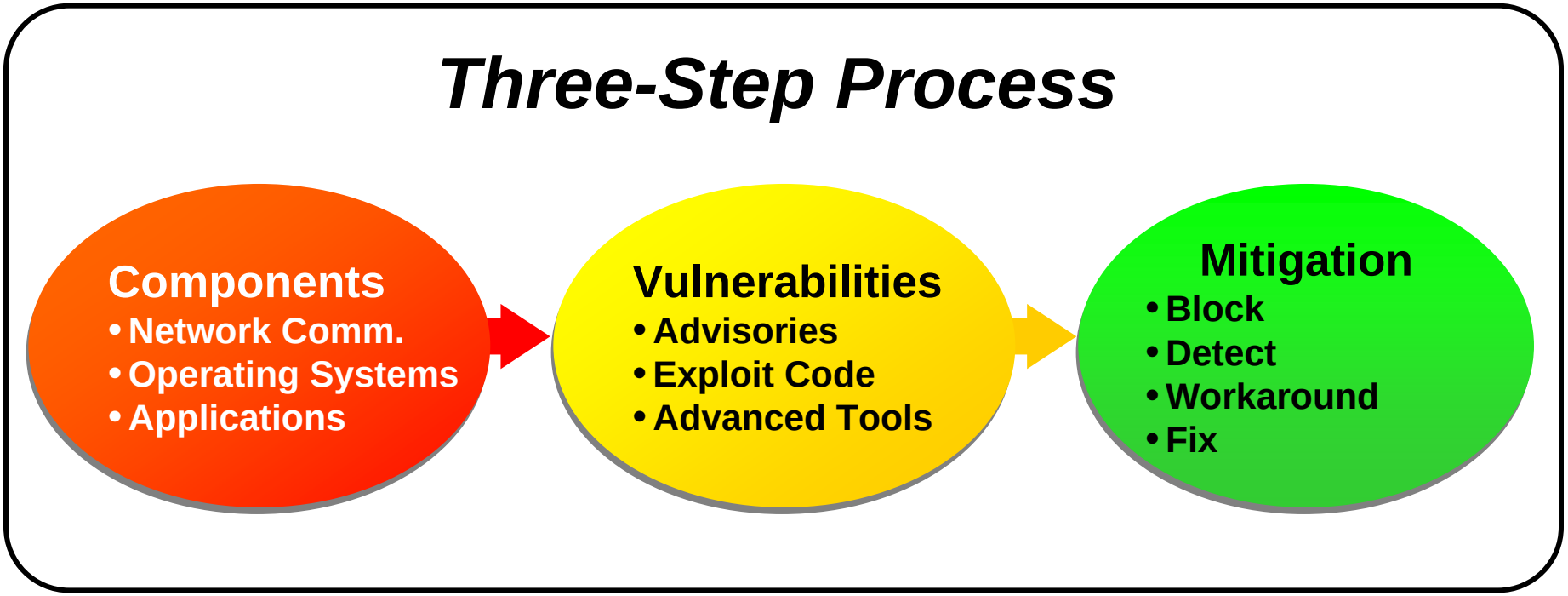




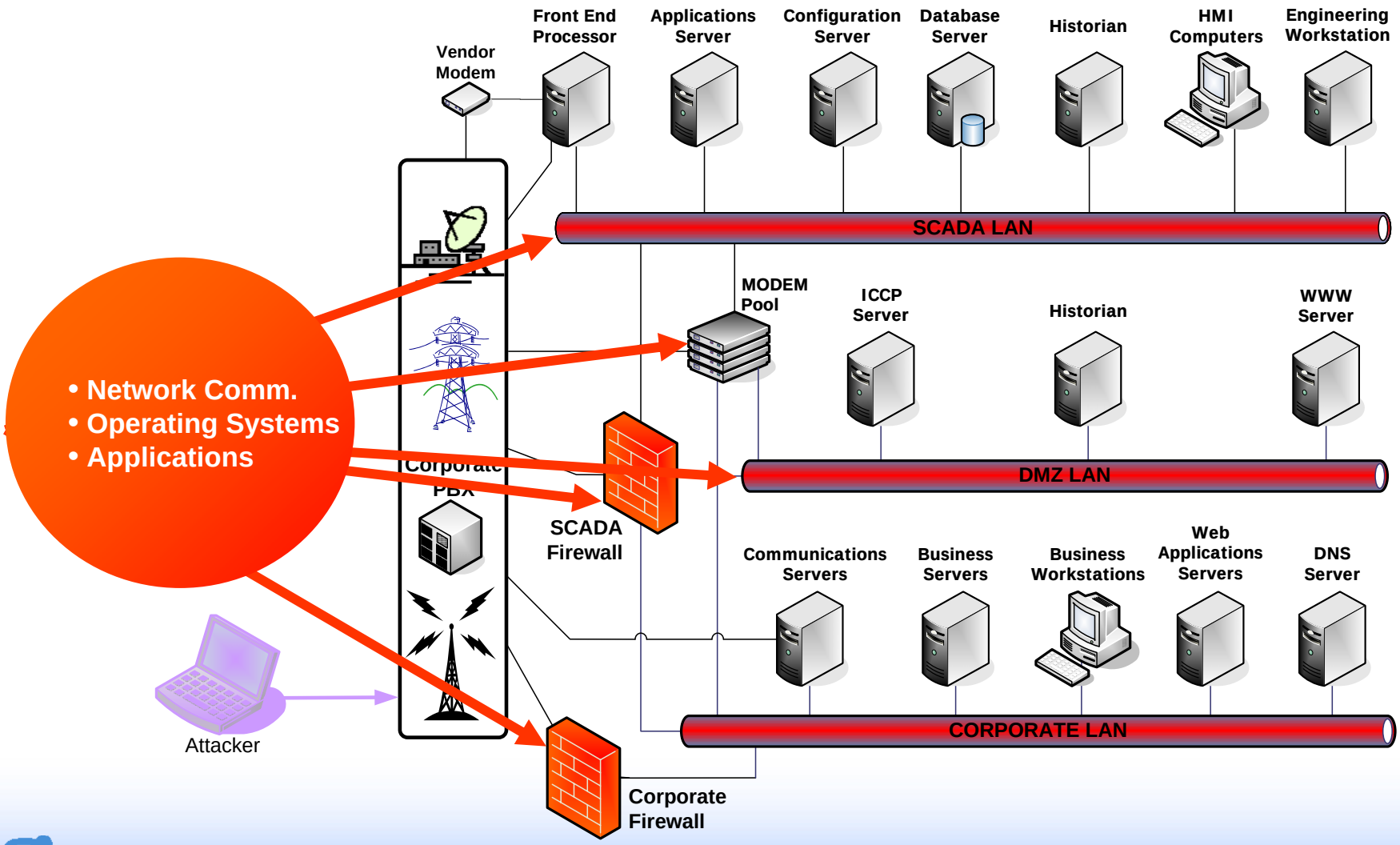
Idaho National Laboratory

Understanding Exposure

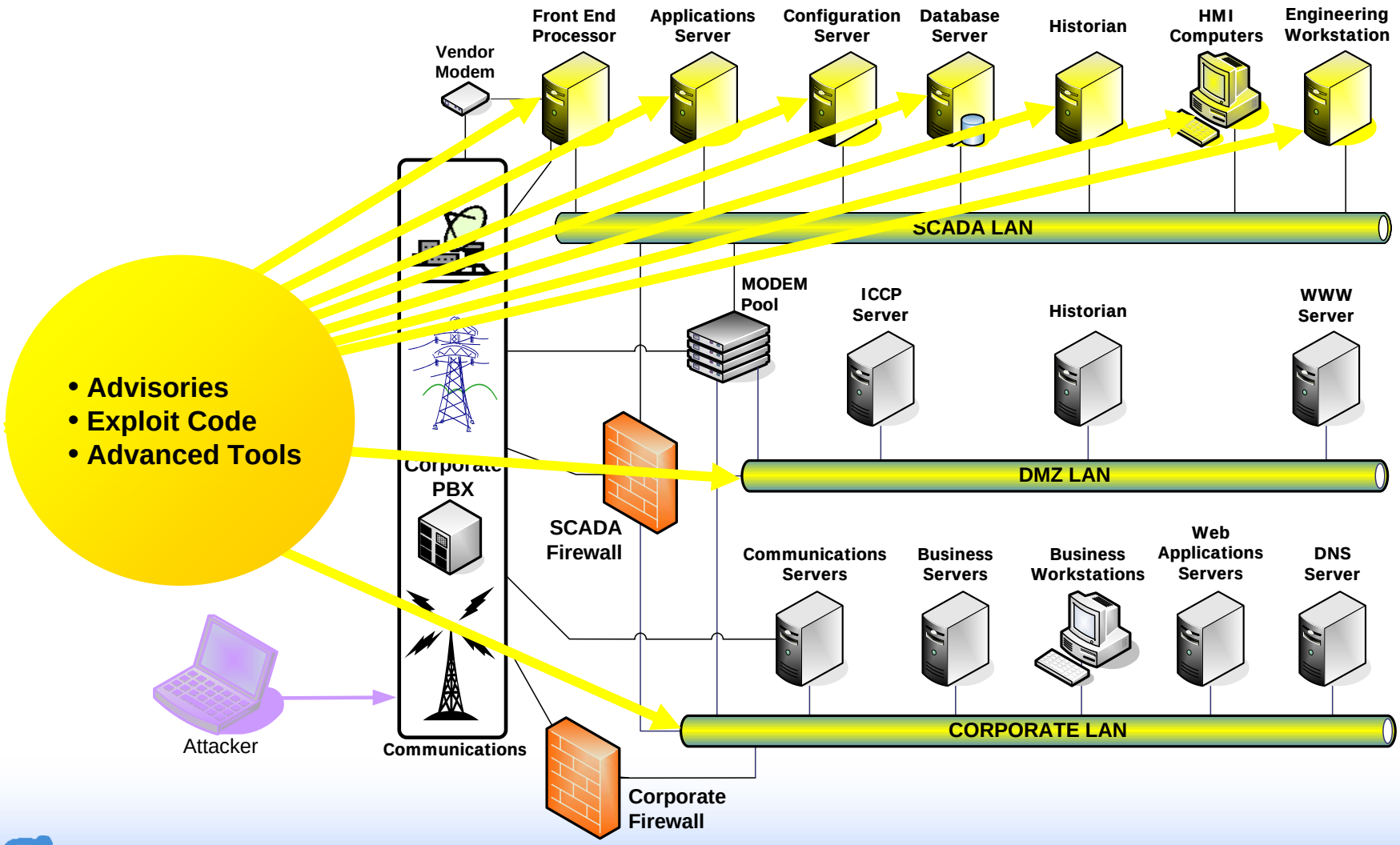
Understanding Exposure



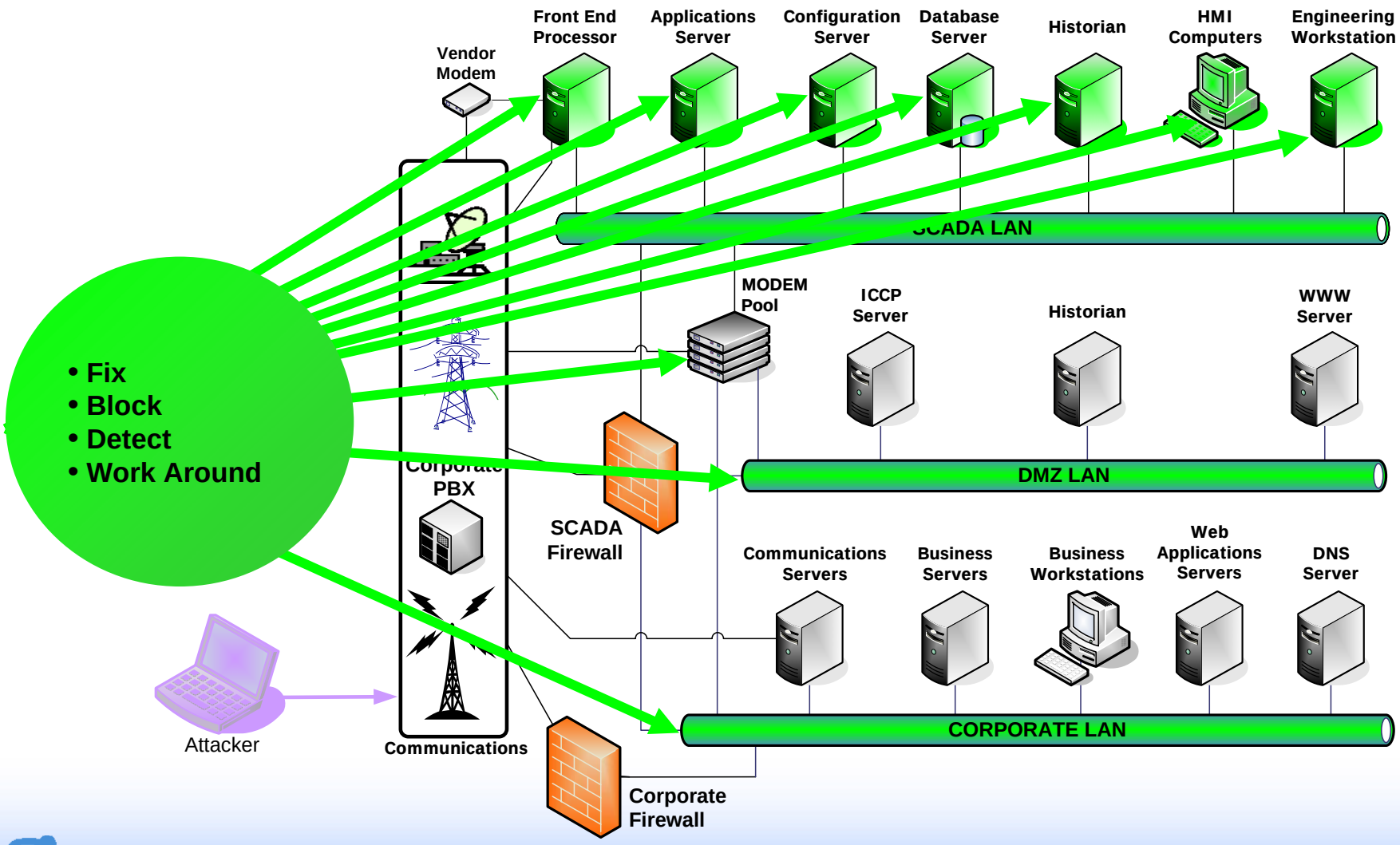
Identify Components



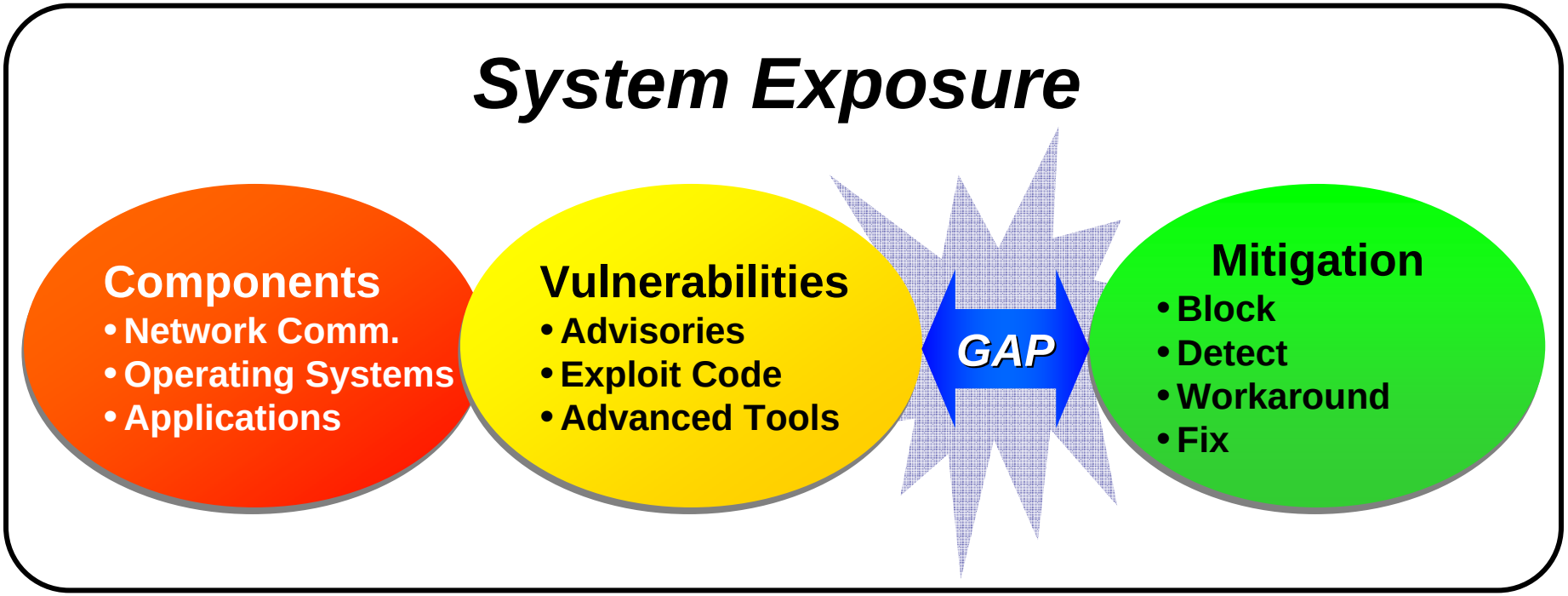
Identify Vulnerabilities



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	Common/widely used	Uncommon/impossible 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	Rare
Time Critical Content	Generally delays accepted	Critical due to safety
Availability	Generally delays accepted	24 x 7 x 365 x forever
Security Awareness	Good in both private and public sector	Poor except for physical
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Remote and unmanned

General Findings

- Vendor default accounts and passwords
- Guest accounts still available
- SCADA use of enterprise services (DNS, etc.)
- No security level agreement with peer site
- No security level agreement 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 SCADA

General Findings: Switches and Routers

- Like most systems, delivered wide open
- Network Administrators have little knowledge how to secure
- In most cases, DEFAULTS are NOT shown in configuration lists
- Enforced port security rare

General Findings: Firewalls

- Rules not commented
- Generic or Simplified rules
- Old/temporary rules not removed
- Rules exist, but nobody knows why
- Logging not turned on
- In some cases, firewall is subverted by direct connection
- Same firewall rules on corporate and internal network

General Findings:
IDS – Intrusion *Detection* System

- New to control system environments (lack SCADA, DCS and PLC signatures)
- Not always employed at corporate level
- No budget or support for staffing and training
- Can not analyze encrypted traffic

General Findings:
IPS – Intrusion *Prevention* System

- New to industry (in general)
- Not fully understood in many applications
- Difficult to employ at corporate level
- No budget or support for staffing and training
- Should not be deployed inside critical real-time system networks

Anatomy of an Attack

Typical Attack Steps

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

Target Identification / Selection

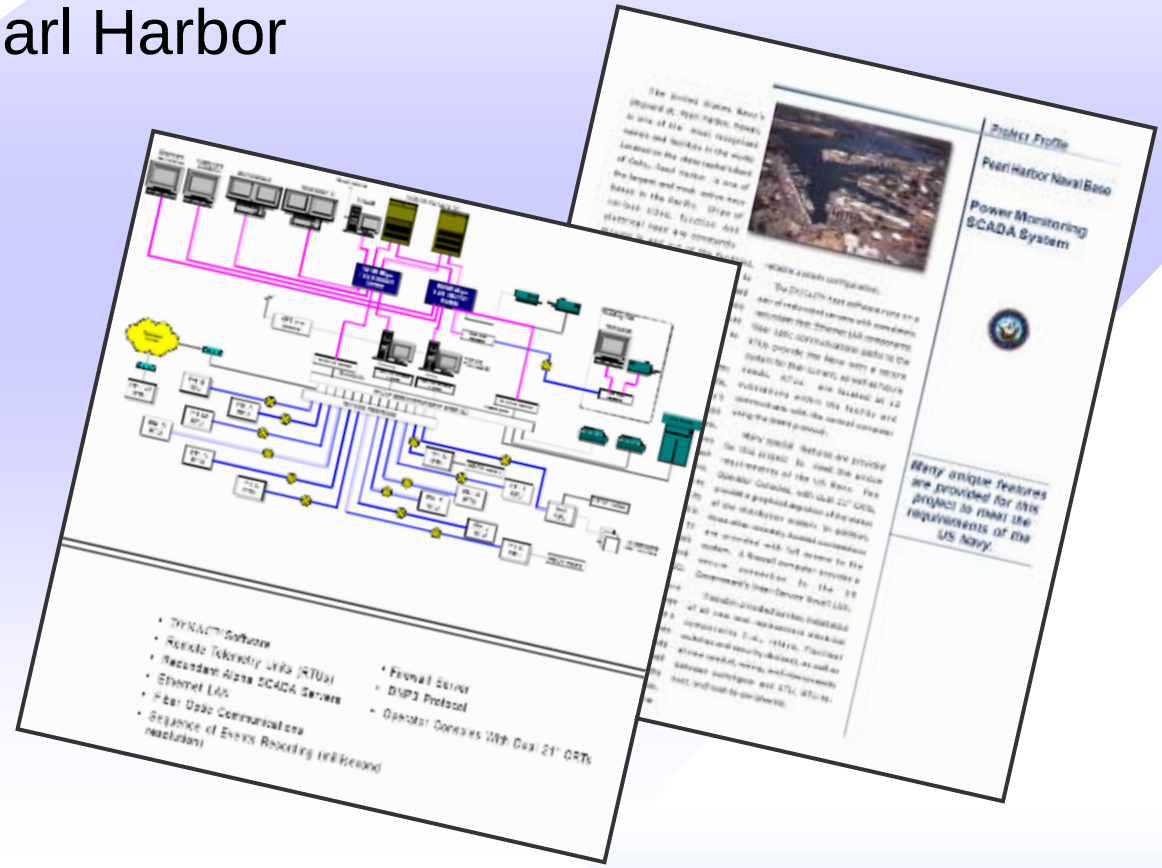
- Dependent on the attacker
- How ‘accessible’ is your company?
  - Internet, media, etc. presence
- How much information is available through your vendor?
- Is your company/utility desirable as a target?
- How do your defenses compare to your neighbors?

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

- Picking on the U.S. Government
  - SCADA at Pearl Harbor



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

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

- 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

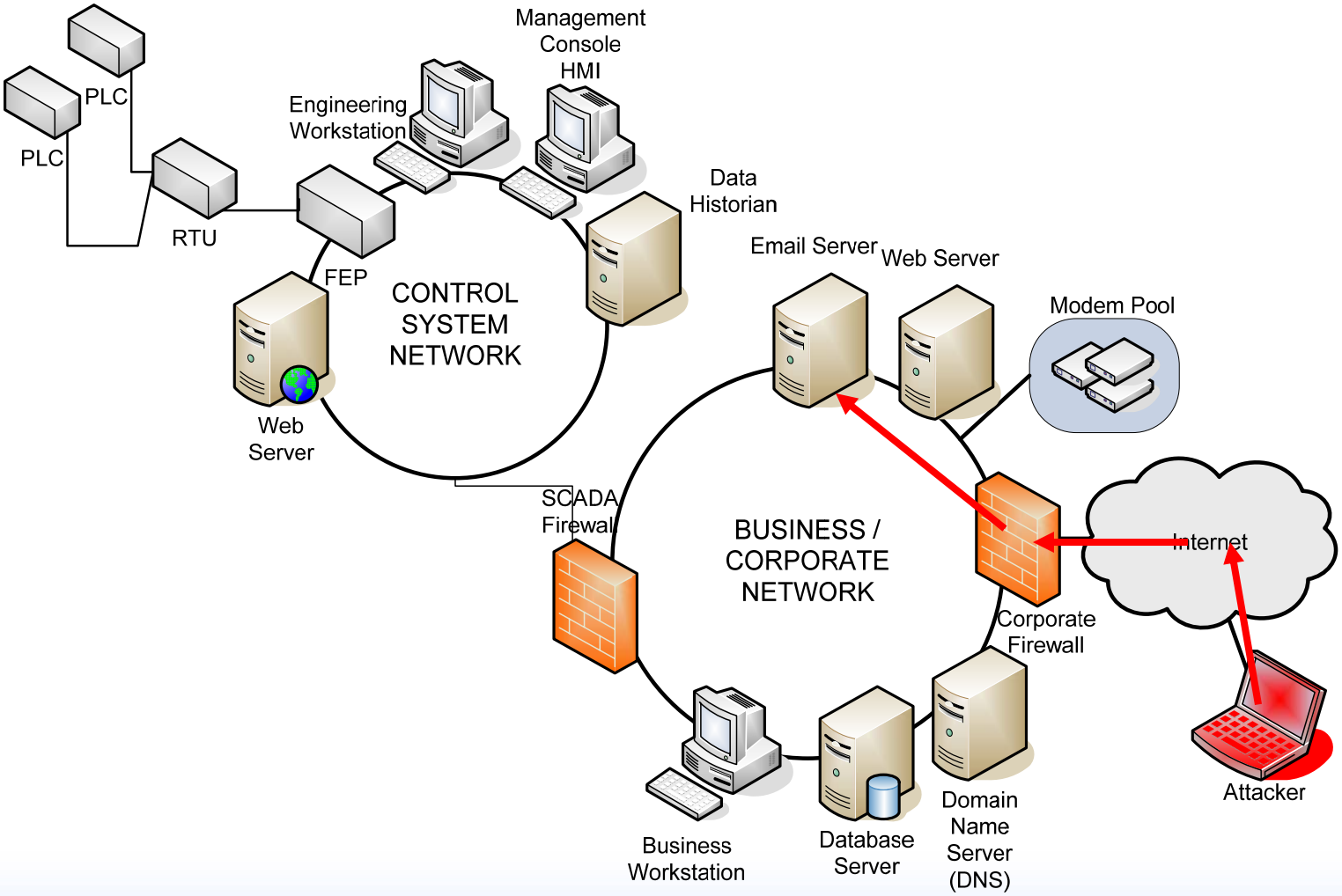
Break

The Demonstration

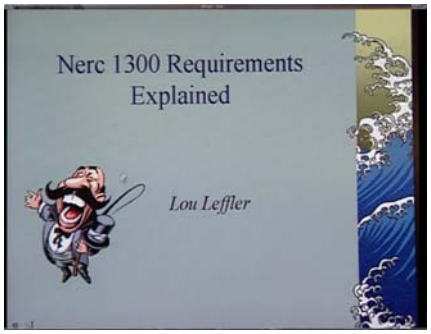
Demonstration Exploits

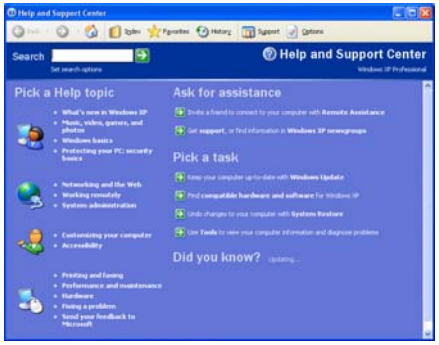
- ‘Phishing’
- HTML HELP Local Code Execution Affects Microsoft Internet Explorer 5.5 SP2 - 6.0 SP1; CVE-2004-0380
- DNS spoofing
- Libpng Overflow (Linux)
  Released in early August 2004
  Affects Linux based systems using libpng version 1.2.5 and earlier; CVE CAN-2004-0597
- SCADA Command Injection

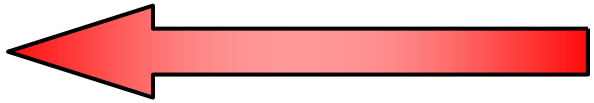
Step #1

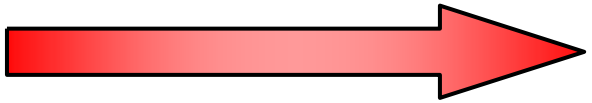

PLC
PLC
RTU
Engineering Workstation
Management Console HMI
Data Historian
FEP
CONTROL SYSTEM NETWORK
Web Server
SCADA Firewall
Email Server
Web Server
Modem Pool
BUSINESS / CORPORATE NETWORK
Corporate Firewall
Internet
Attacker
Business Workstation
Database Server
Domain Name Server (DNS)

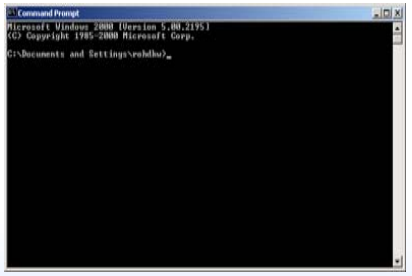
Web Browser / Email Exploitation
HTML Help Exploit





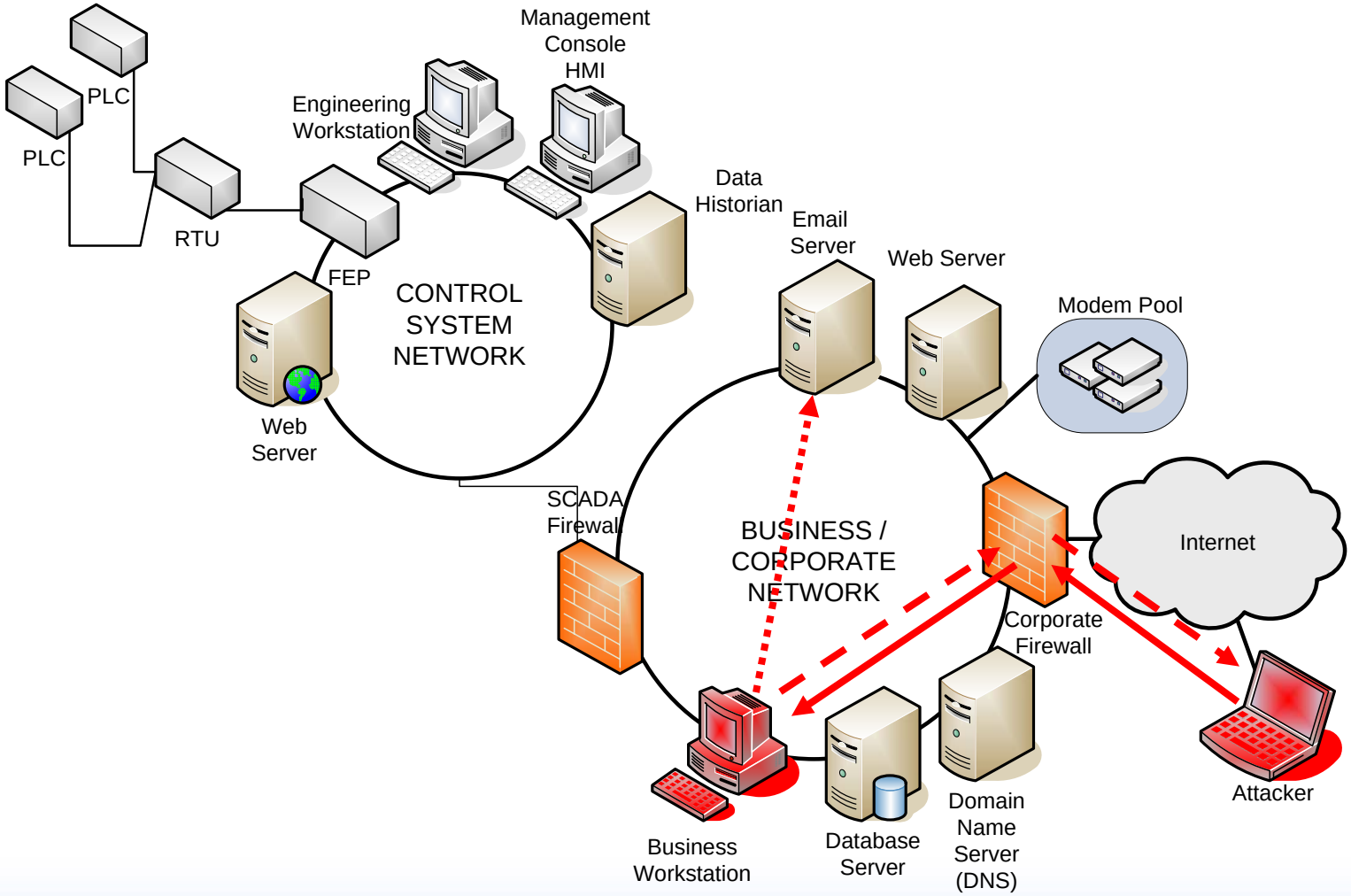




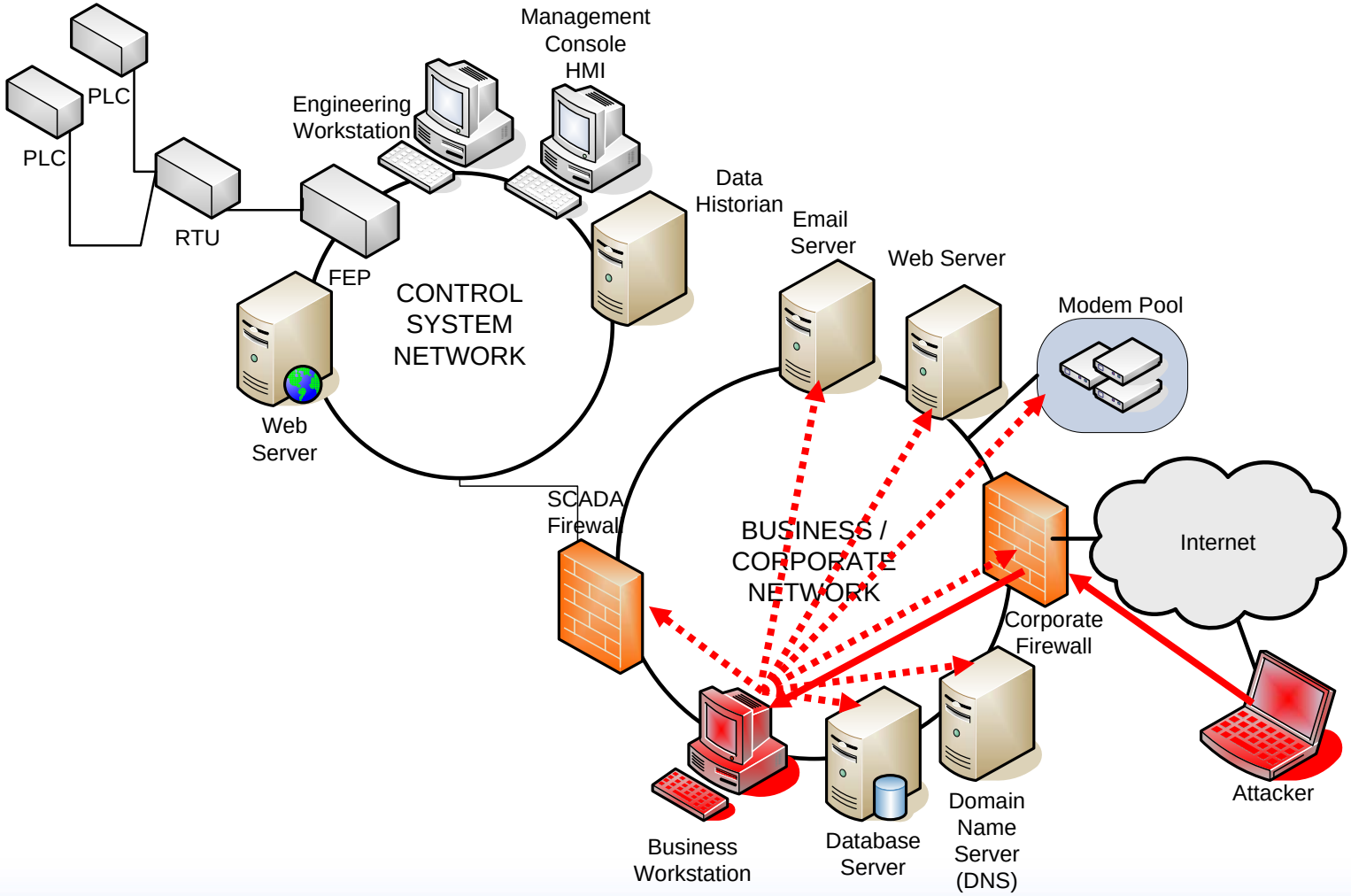


Idaho National Laboratory

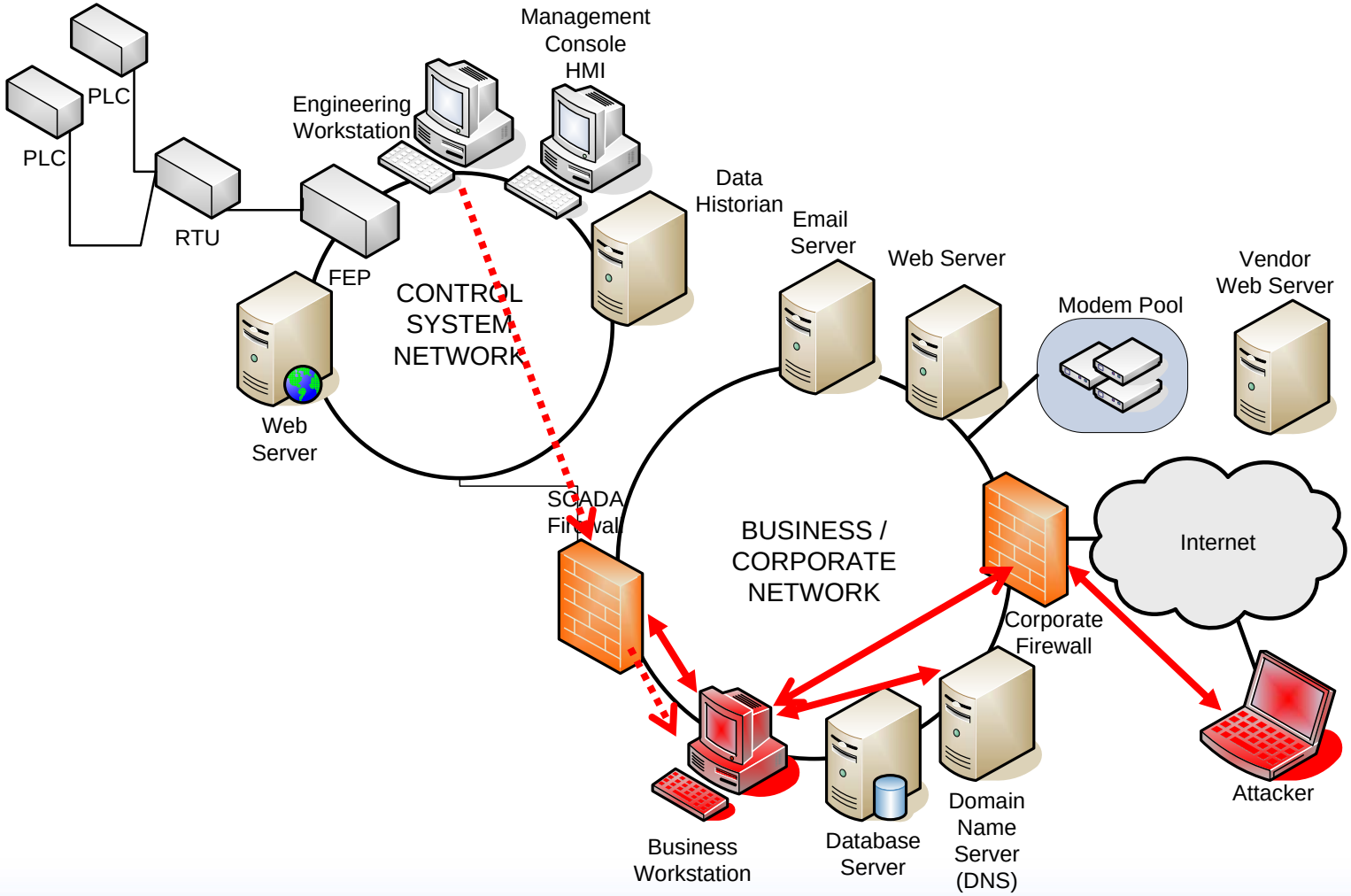
Step #2


PLC
PLC
RTU
Engineering Workstation
Management Console HMI
Data Historian
FEP
CONTROL SYSTEM NETWORK
Web Server
Email Server
Web Server
Modem Pool
SCADA Firewall
BUSINESS / CORPORATE NETWORK
Corporate Firewall
Internet
Business Workstation
Database Server
Domain Name Server (DNS)
Attacker

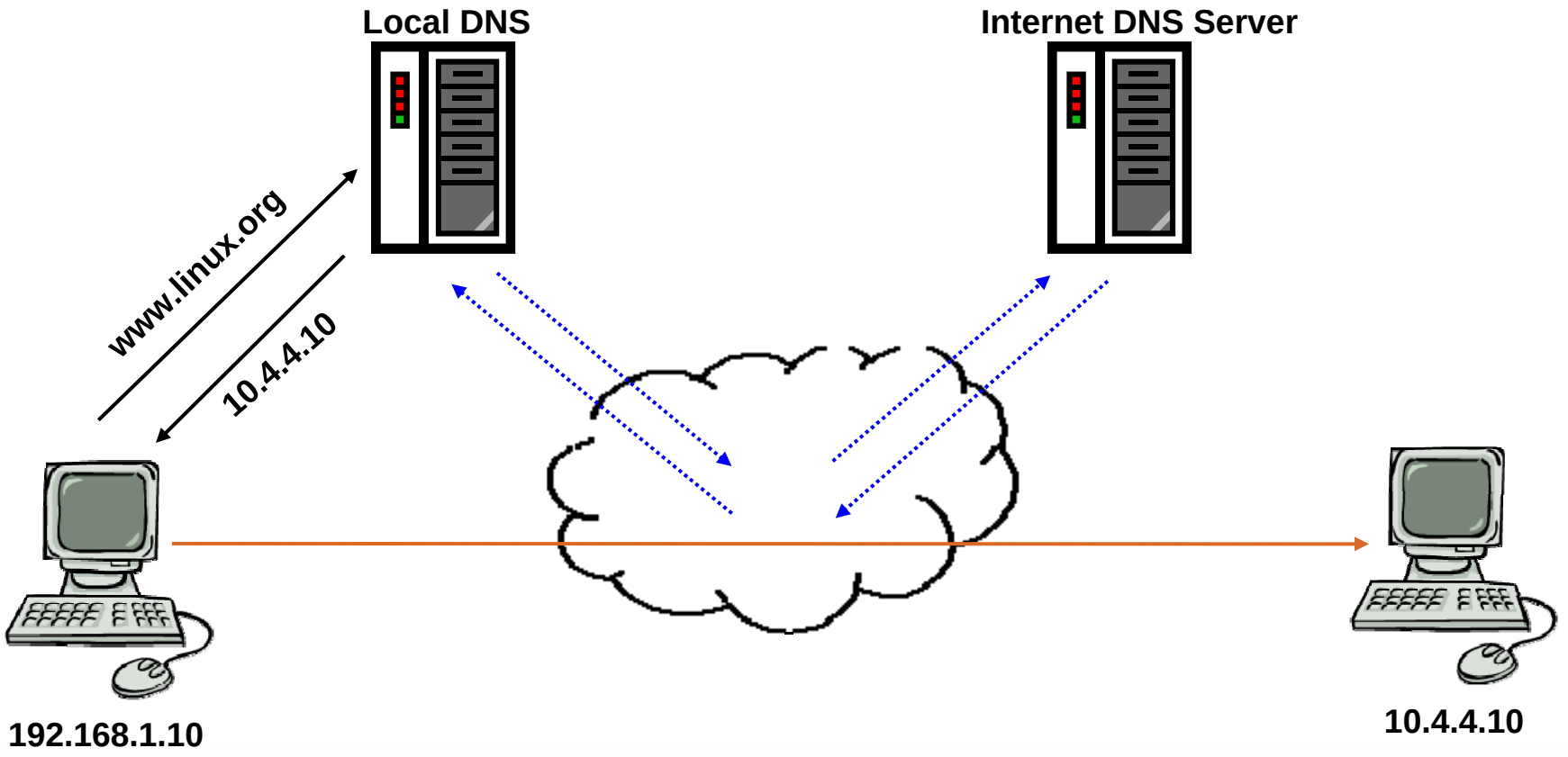
Step #3


Management
Console
HMI
Engineering
Workstation
PLC
PLC
RTU
FEP
Data
Historian
Email
Server
Web Server
Modem Pool
CONTROL
SYSTEM
NETWORK
Web
Server
SCADA
Firewall
BUSINESS /
CORPORATE
NETWORK
Internet
Corporate
Firewall
Attacker
Business
Workstation
Database
Server
Domain
Name
Server
(DNS)

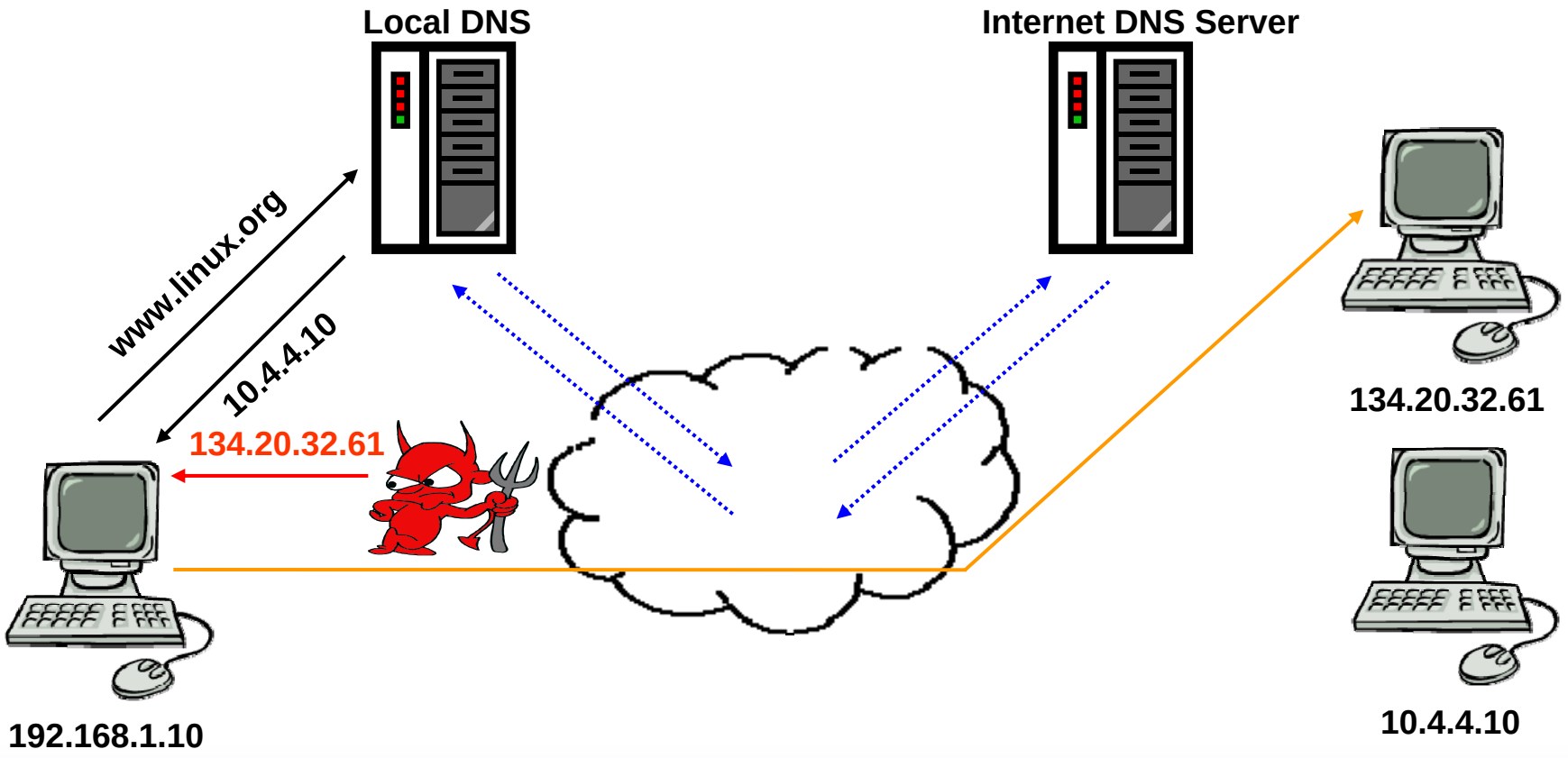
Step #4


Management
Console
HMI
Engineering
Workstation
PLC
PLC
RTU
FEP
Data
Historian
Email
Server
Web Server
Modem Pool
Vendor
Web Server
CONTROL
SYSTEM
NETWORK
Web
Server
SCADA
Firewall
BUSINESS /
CORPORATE
NETWORK
Internet
Corporate
Firewall
Business
Workstation
Database
Server
Domain
Name
Server
(DNS)
Attacker

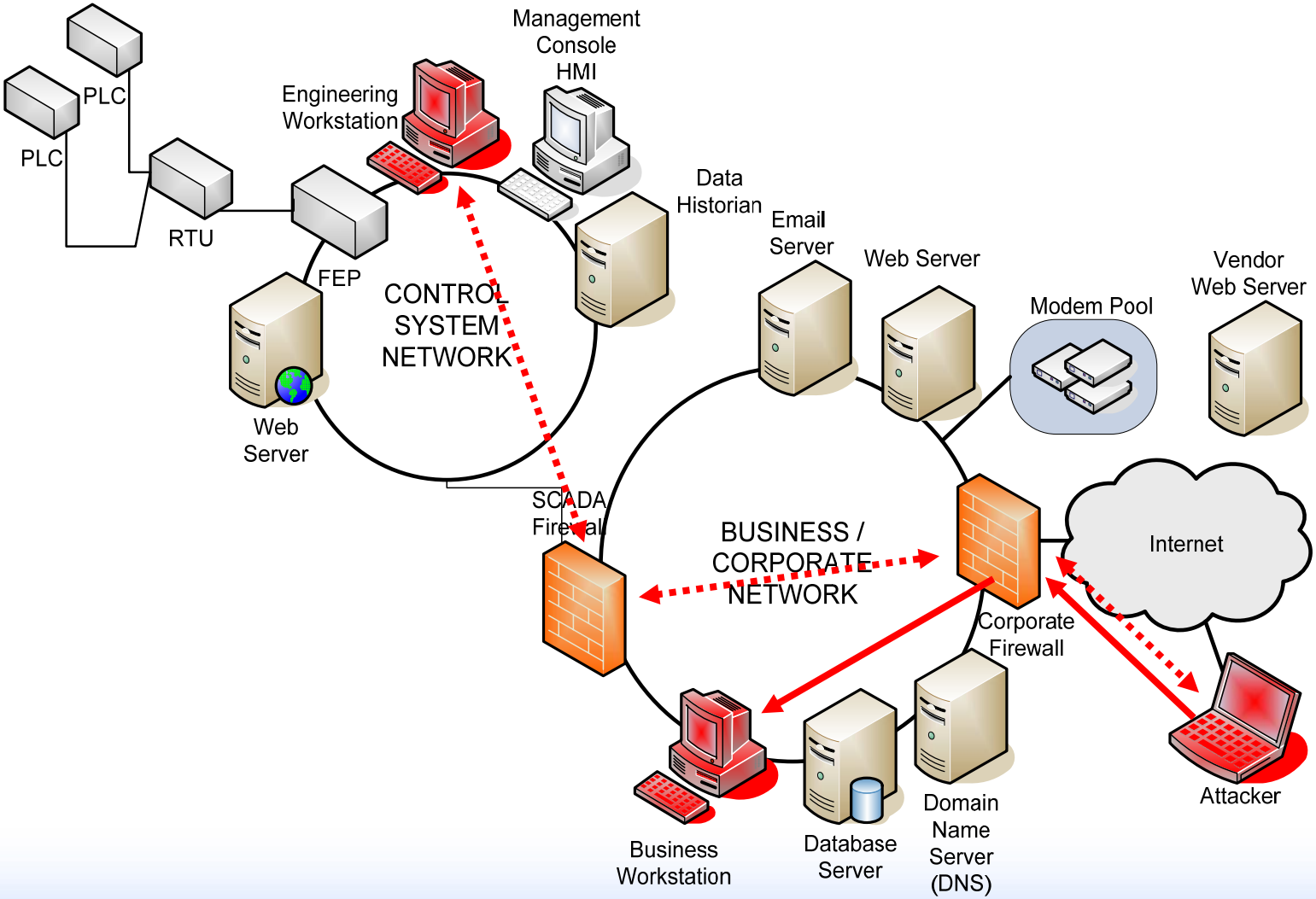
Domain Name Service (DNS)



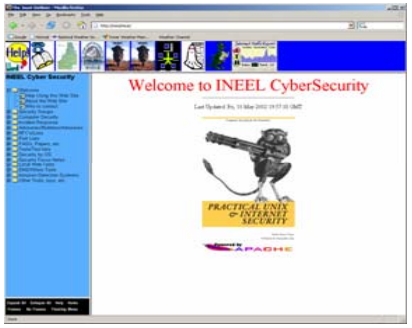
Domain Name Service (DNS) Spoof

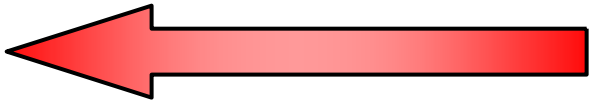


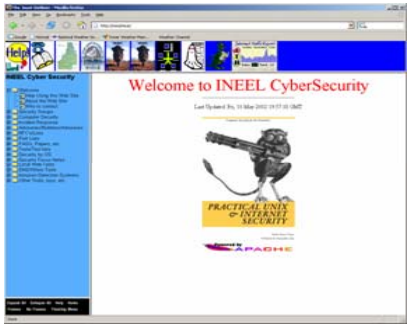
Step #5

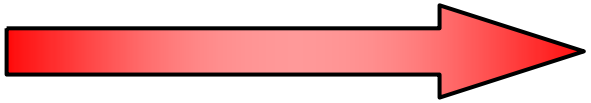

Management
Console
HMI
Engineering
Workstation
PLC
PLC
RTU
FEP
Web
Server
CONTROL
SYSTEM
NETWORK
Data
Historian
Email
Server
Web Server
Modem Pool
Vendor
Web Server
SCADA
Firewall
BUSINESS /
CORPORATE
NETWORK
Corporate
Firewall
Internet
Attacker
Business
Workstation
Database
Server
Domain
Name
Server
(DNS)

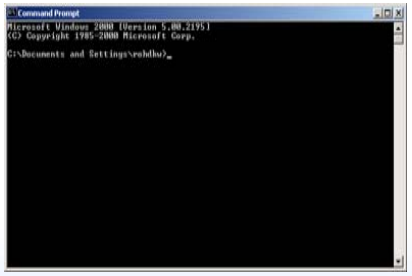
Web Browser Exploitation Infected Image Exploit





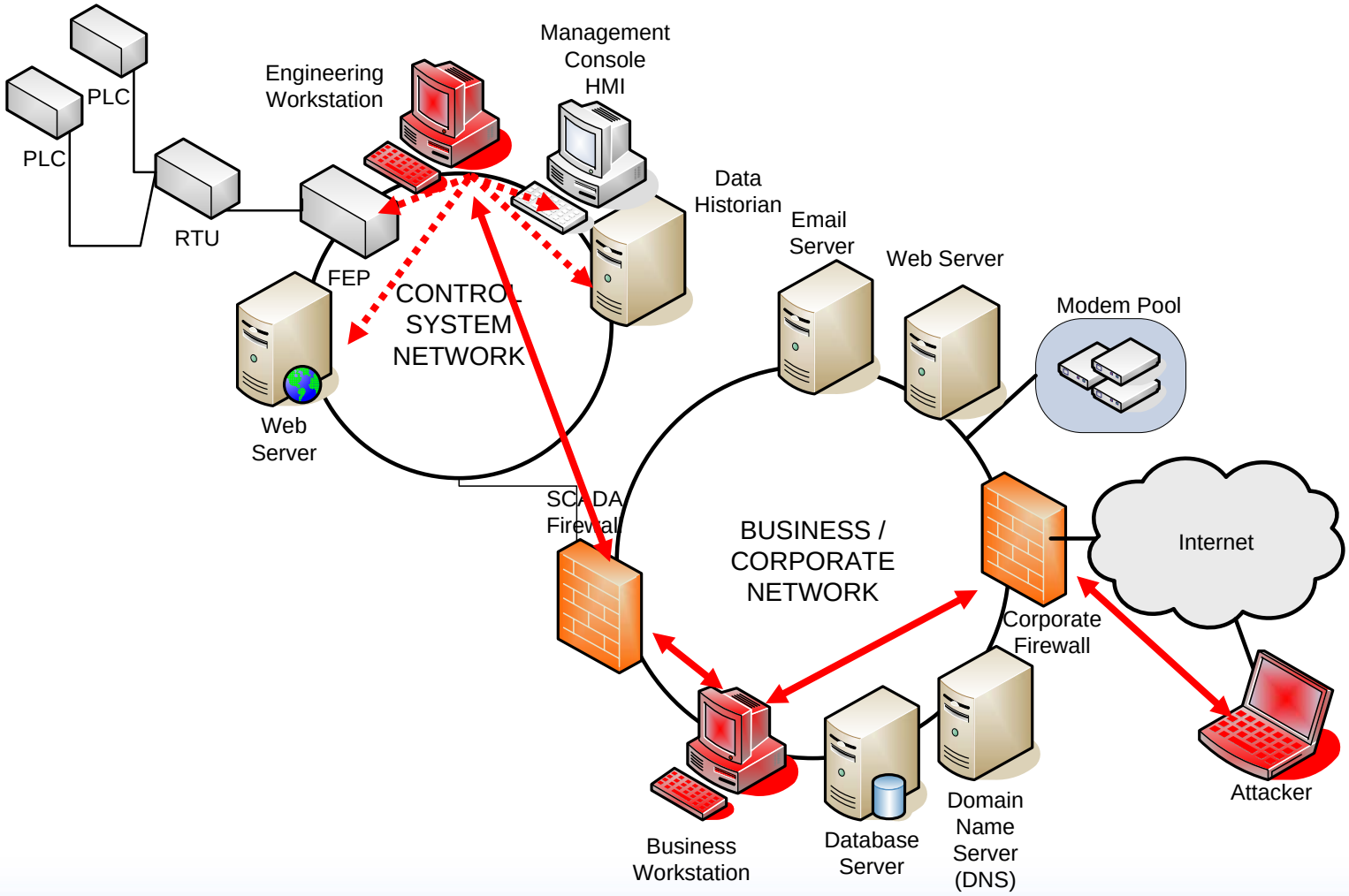




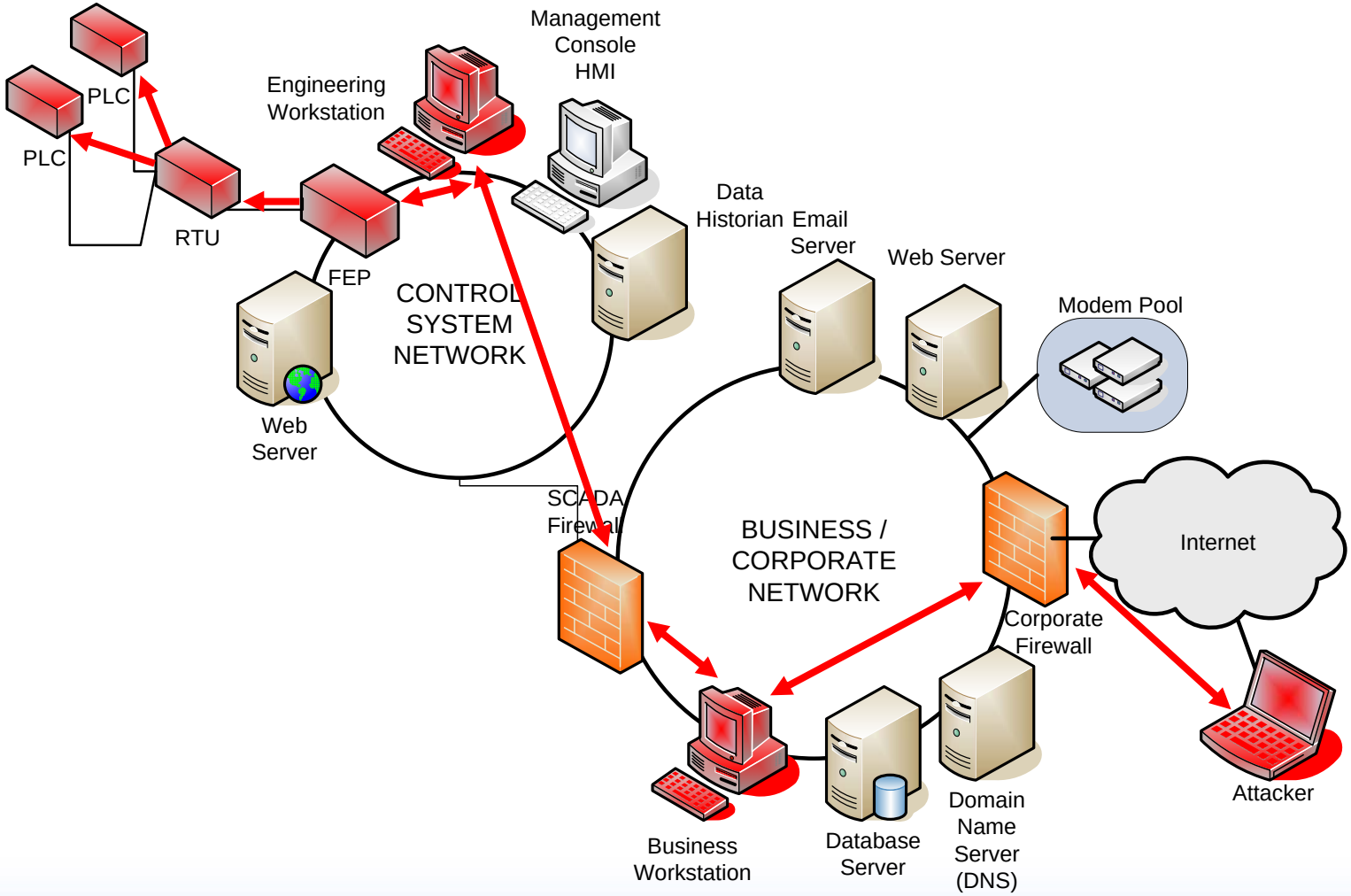


Idaho National Laboratory

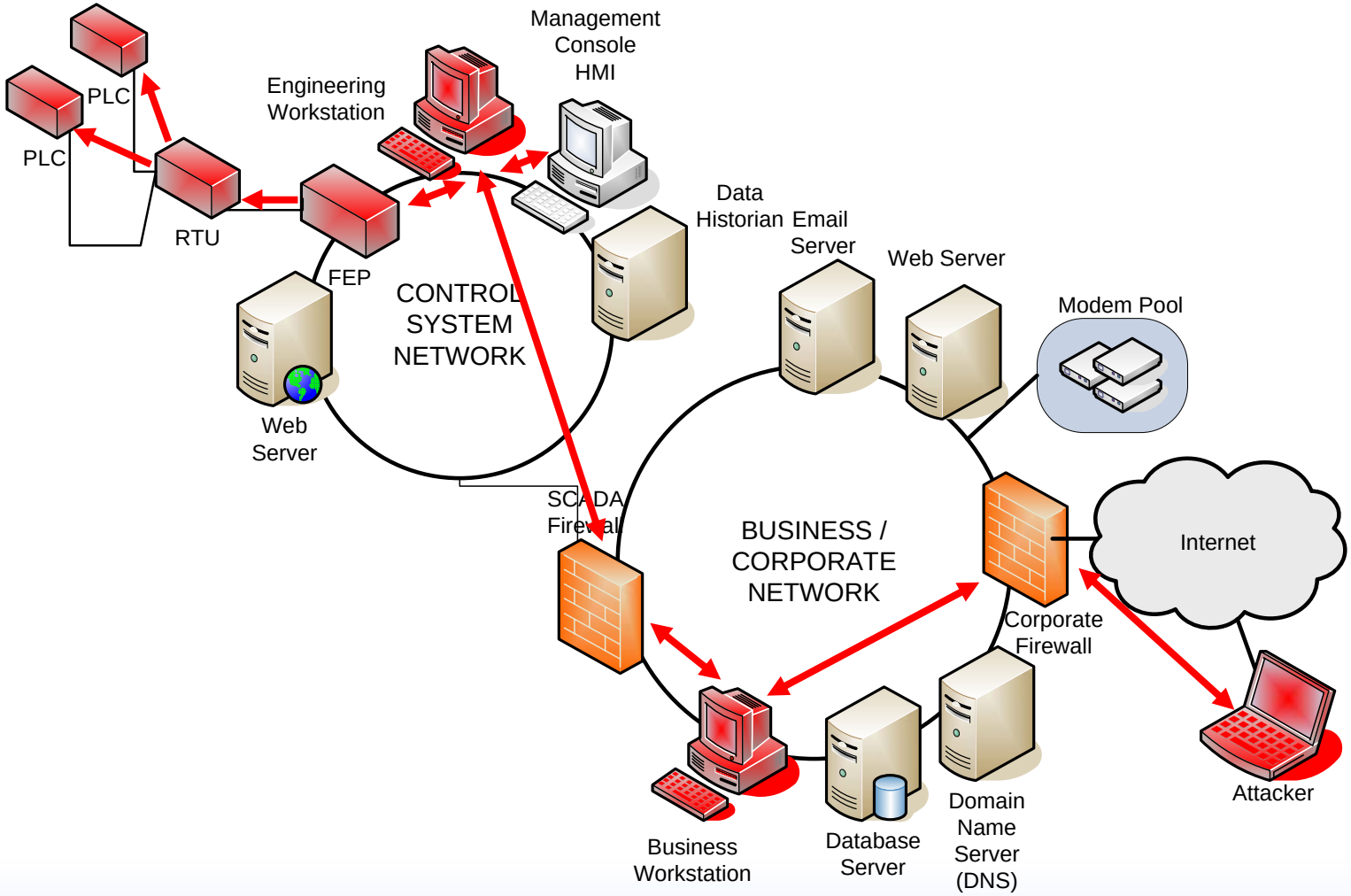
Step #6


PLC
PLC
RTU
Engineering Workstation
Management Console HMI
Data Historian
Email Server
Web Server
Modem Pool
FEP
CONTROL SYSTEM NETWORK
Web Server
SCADA Firewall
BUSINESS / CORPORATE NETWORK
Internet
Corporate Firewall
Business Workstation
Database Server
Domain Name Server (DNS)
Attacker

Step #7


Management
Console
HMI
Engineering
Workstation
PLC
PLC
RTU
FEP
CONTROL
SYSTEM
NETWORK
Web
Server
Data
Historian
Email
Server
Web Server
Modem Pool
SCADA
Firewall
BUSINESS /
CORPORATE
NETWORK
Corporate
Firewall
Internet
Attacker
Business
Workstation
Database
Server
Domain
Name
Server
(DNS)

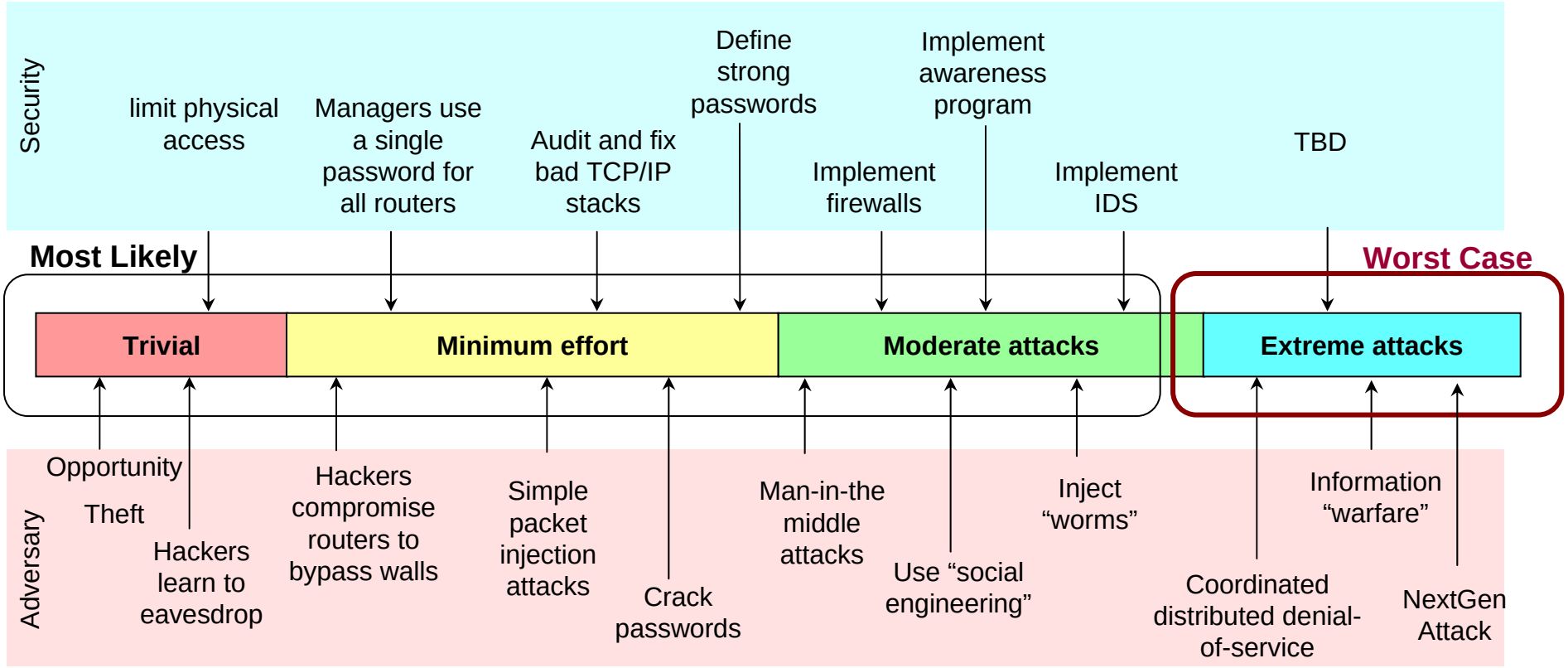
Alternate Step #7

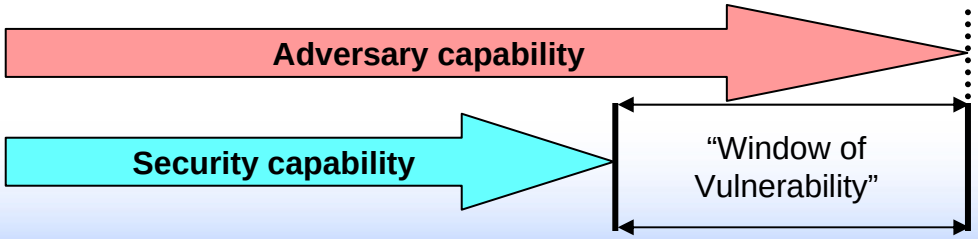


Mitigation Strategies

- Phishing
  - training/policy
- HTML Help exploit
  - updates and IDS
- ARP scanning
  - IDS
- DNS spoofing
  - no browsing from SCADA network
- Libpng buffer overflow
  - Updates and patches
- SCADA Command injection
  - Authentication for SCADA communications

The electronic arms race of cyber security





Other Attack Techniques

Other Attack Examples

- Password Cracking
  - Default or Simple Passwords
  - Short or Minimum Significant Characters
- Denial of Service
- Typical Flooding Attacks
  - Man-in-the-Middle (Dropping Packets)
  - Remote Service Crashes
  - Resource Consumption
    - CPU
    - Bandwidth
    - Disk Space

Other Attack Examples

- Vendor Specific Application Exploitation
  - Binaries with SETID bit
  - Command-line Parameters
  - Simple Reverse Engineering
  - Protocol Overflows
- Fragmentation Attacks
- Core Dumping Attacks

Other Attack Examples

- Remote Service Exploitation
  - Web Services
  - Uncrypted Services (telnet, rshell, rlogin, X11)
  - Database Management Systems (Data Base Attack)
  - Remote Procedure Calls (RPC)
  - Sendmail
  - Samba

The Myth

Vendor Says:

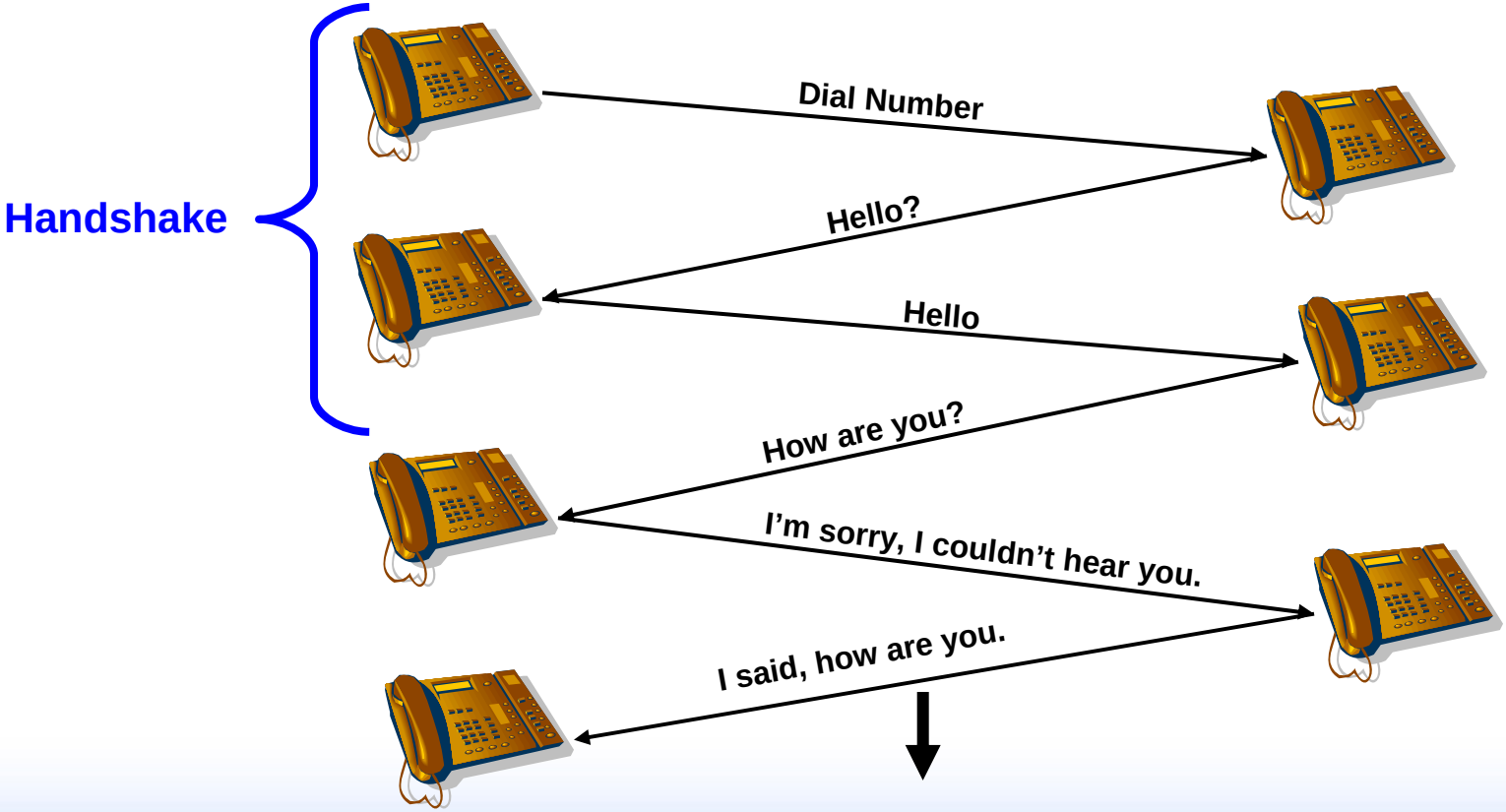
“Data only flows to the corporate Data Base”

IT Says:

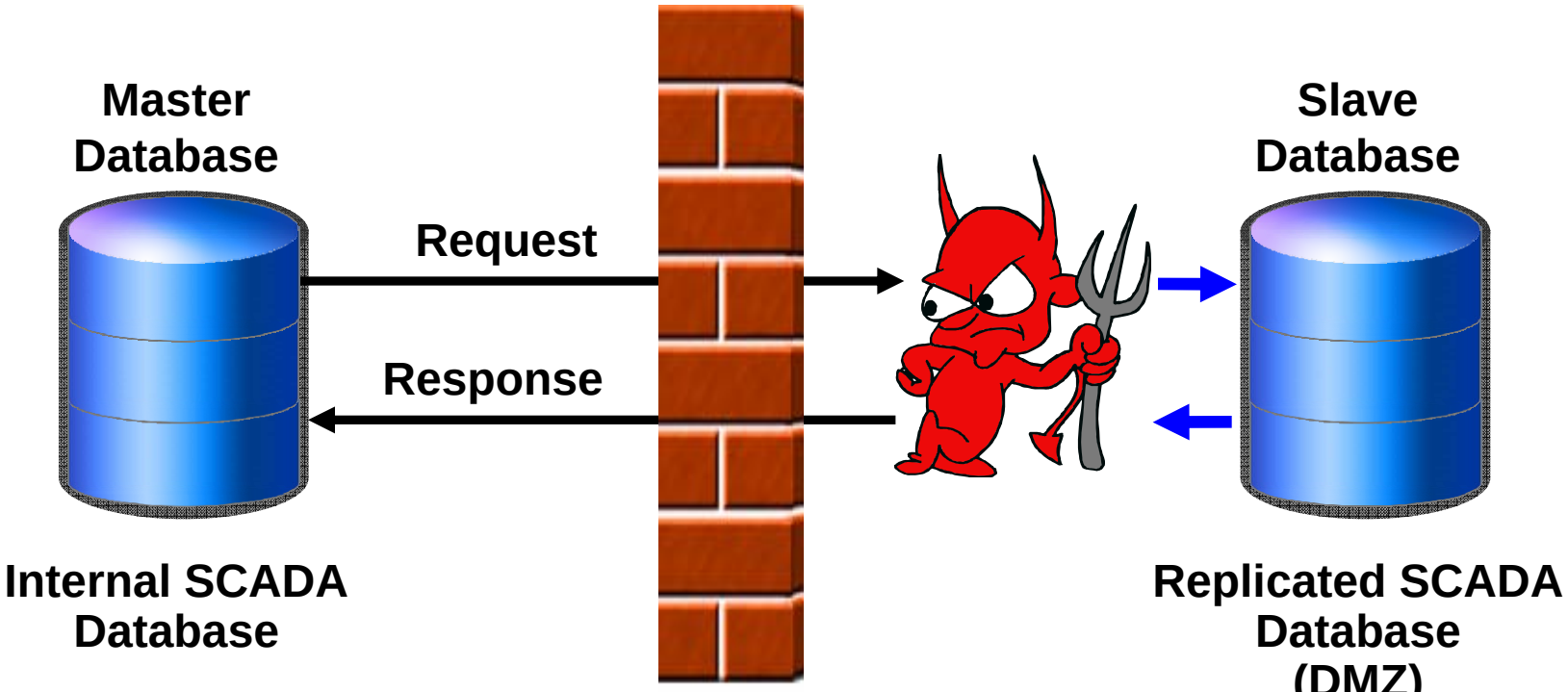
“Traffic is not permitted through the firewall from the Corporate Data Base”

Communication Basics

- TCP is a reliable, stateful communications protocol
- Three-way handshaking
- There are no one-way communications with TCP



Firewall Exception – Database



Vulnerability Testing

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

Vulnerability Assessment – CIP-007 R6

The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: (paraphrased)

1. **Modem and port discovery**
2. **Default account management controls**
3. **Security patch and anti virus**
4. **Result documentation and action plan**
5. **Minimal assessment for remote (unmanned) sites prior to upgrades**

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

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

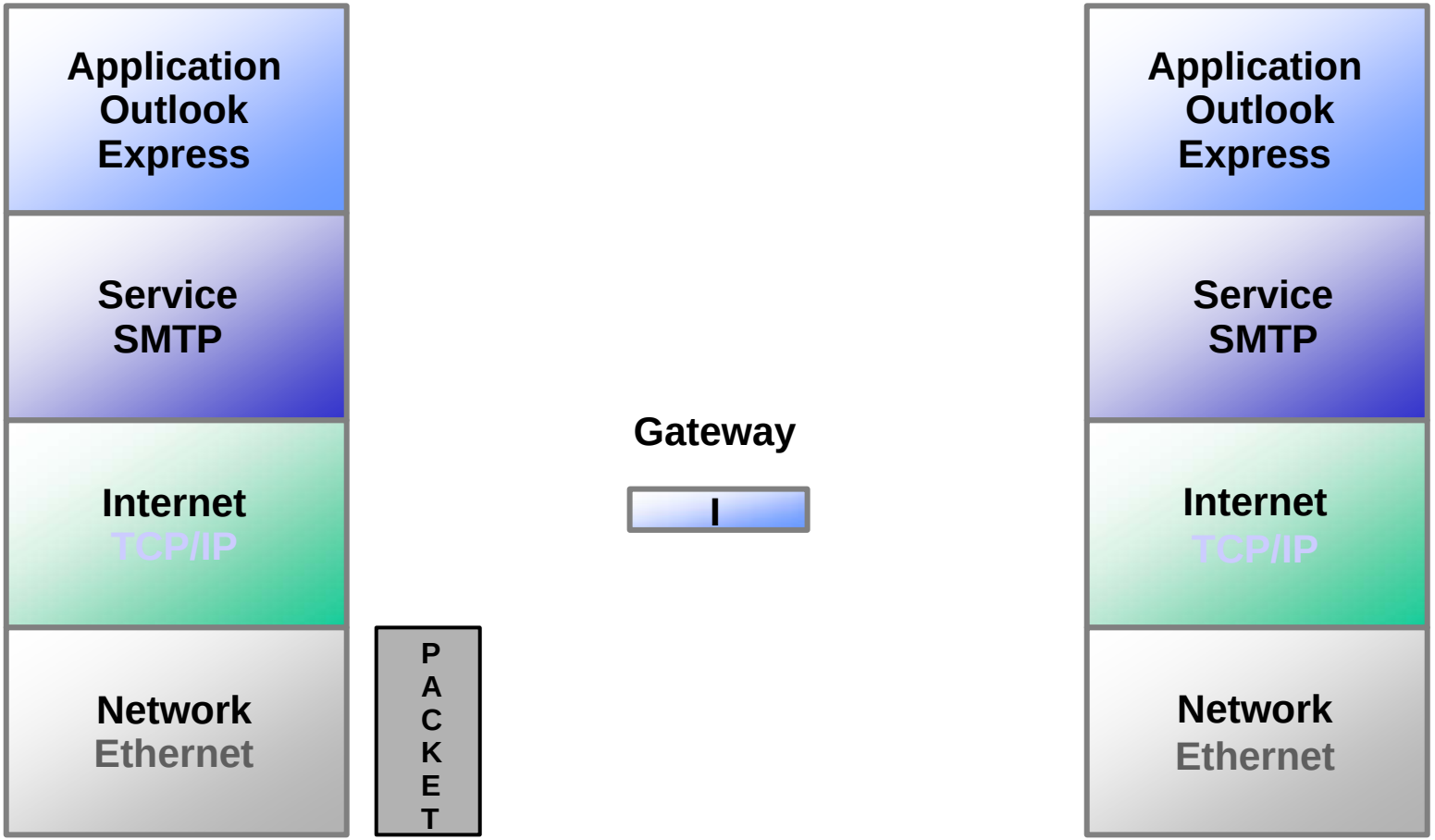
- **US-CERT**

  http://www.uscert.gov

Break

Network Components and Architecture

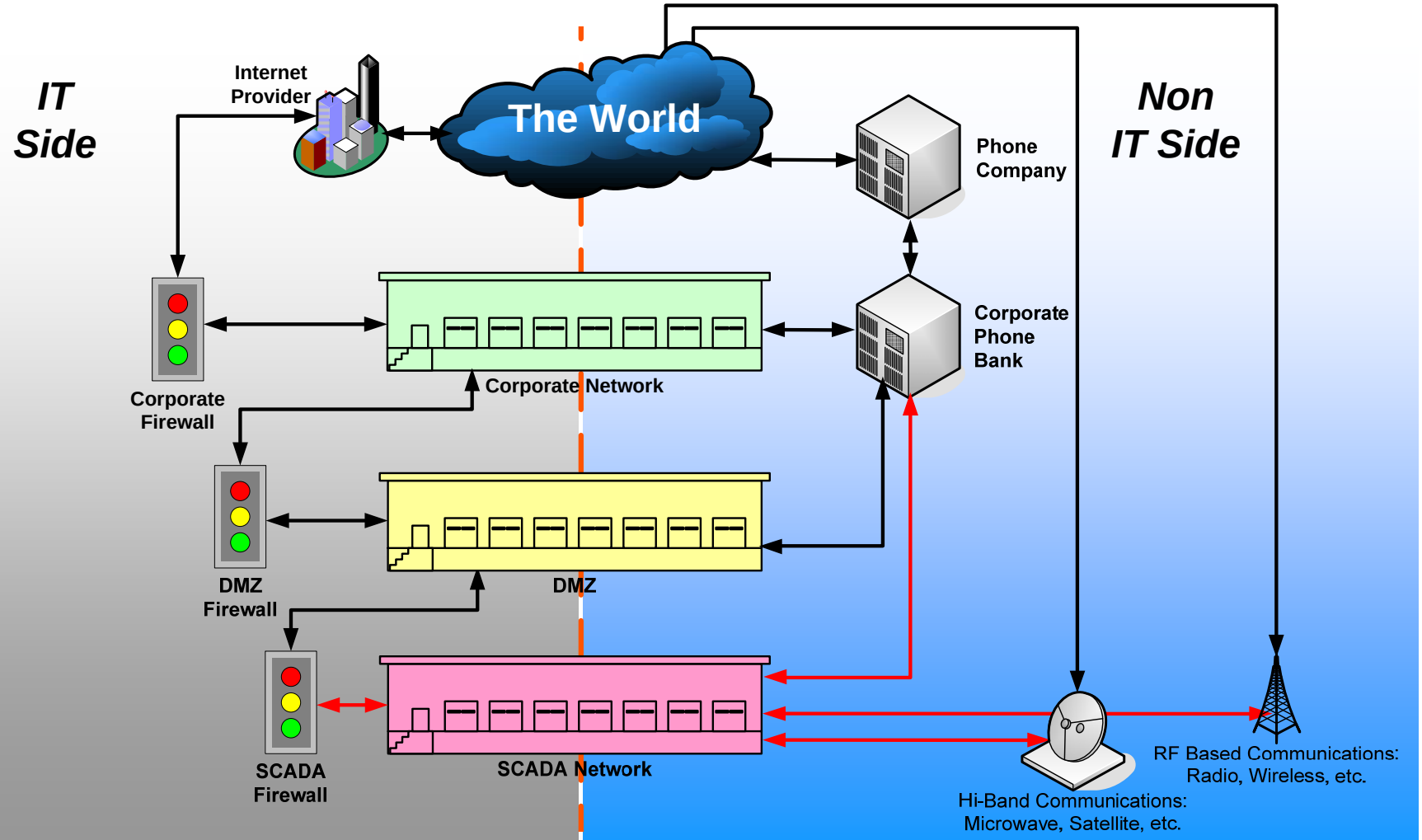
A Packet in Time



What is the emerging risk to SCADA?

- Evolution of SCADA/PCS protocols is allowing for robust interconnectivity
- What as once isolated comms is now using open systems connectivity (like TCP)
- Future implications for DNP3, DeviceNet, UCA, ControlNet, Profibus etc.

Electronic Perimeter



Network Devices

Hubs, Switches and Routers

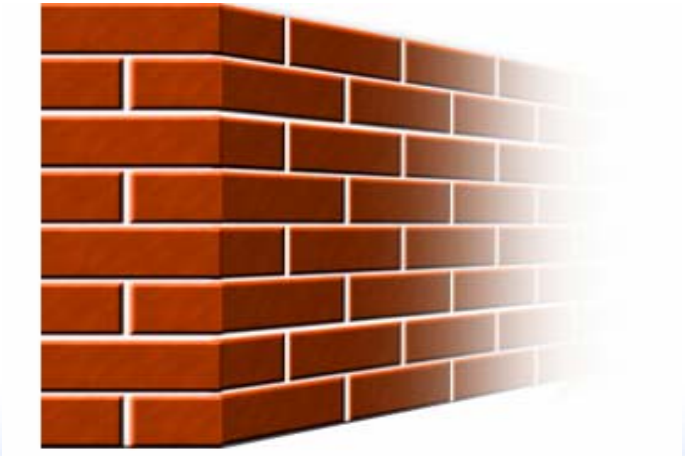
- Provide network communication
- Provide network routing
- Allow for multiple network paths
- Provide first level of defense
- Create Virtual Private Networks (VPN's)
- Enforce Access Control Lists (ACL's)

Firewall Functions

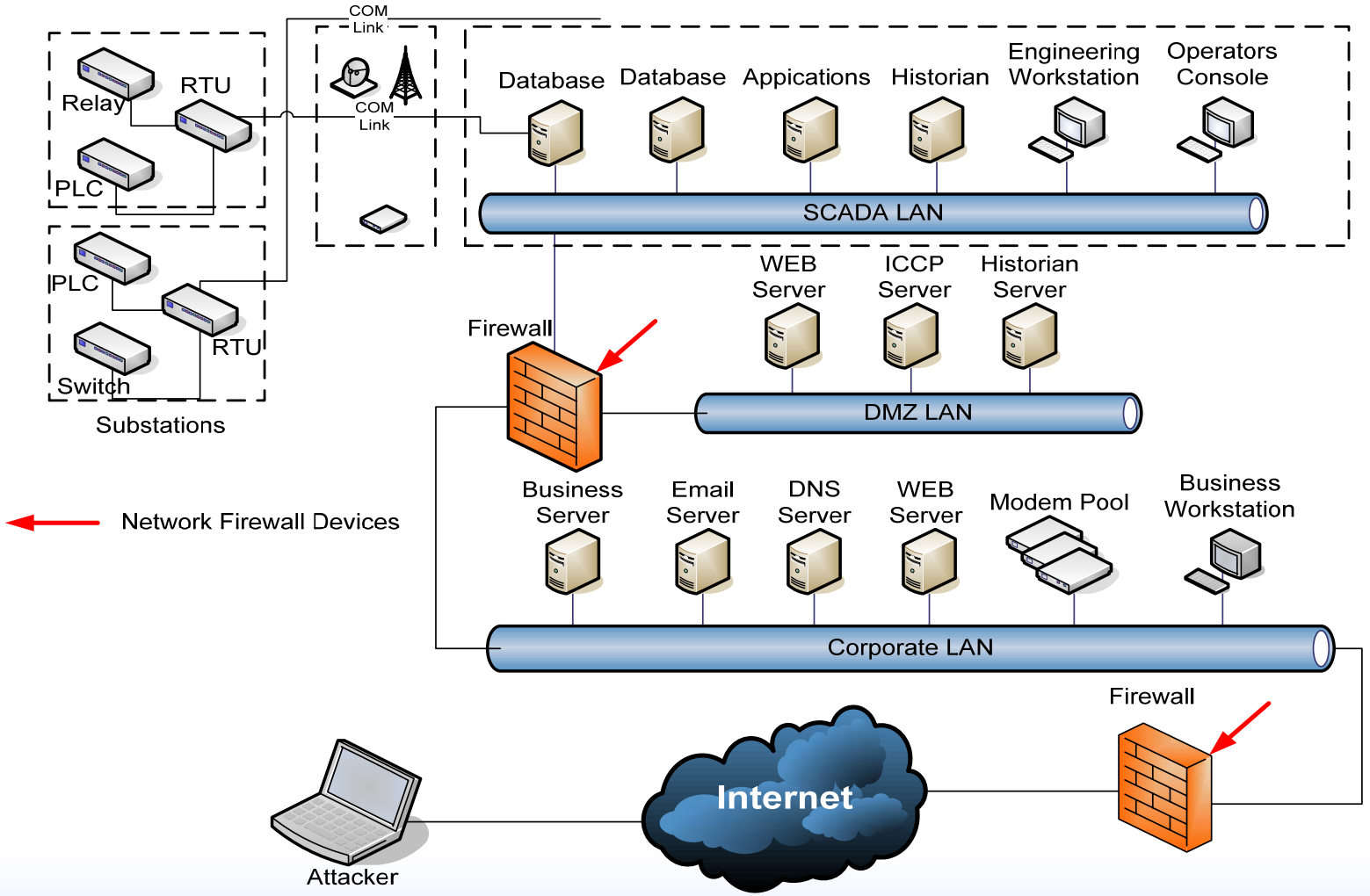
- Protect the inside from the outside
- Protect the outside from the inside
- Enforce Security Policy
- Track Network Activity

Firewall Rules

- Actions to be taken:
  - Accept: Allow the traffic,
  - Drop: Stop with no return to source,
  - Reject: Stop the packet and tell source
- Monitoring firewalls: Logs, IDS, TESTING
- Writing rules: best practices
- Data collection
- Use ‘whitelist’ connections



Firewall Placement Overview



Key FW ‘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

Concerns for SCADA and Firewalls

- 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 (OOTB) modifications lead to:
  - Transformation of FW into router
  - FW becomes a simple proxy gateway
  - Broken on-stack DNS (Divulge internal naming structure)
- FW often introduce massive architecture rebuilds

The Common Wisdom

"Never mix your office LAN with your industrial-control LAN. They should be separated by a firewall, or at minimum, a bridge or router."

The Ten Commandments of Industrial Ethernet,
B&B Electronics Manufacturing Company,
March 30, 2004

Misapplication of IT Security Assumptions

- There are important differences between IT networks and SCADA/PC networks
- Problems occur because IT assumptions may not be valid on the plant floor:
  - Valid types of outbound traffic;
  - The importance of web “customers”;
  - The protection from DoS attacks.

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 FW for the SCADA domains

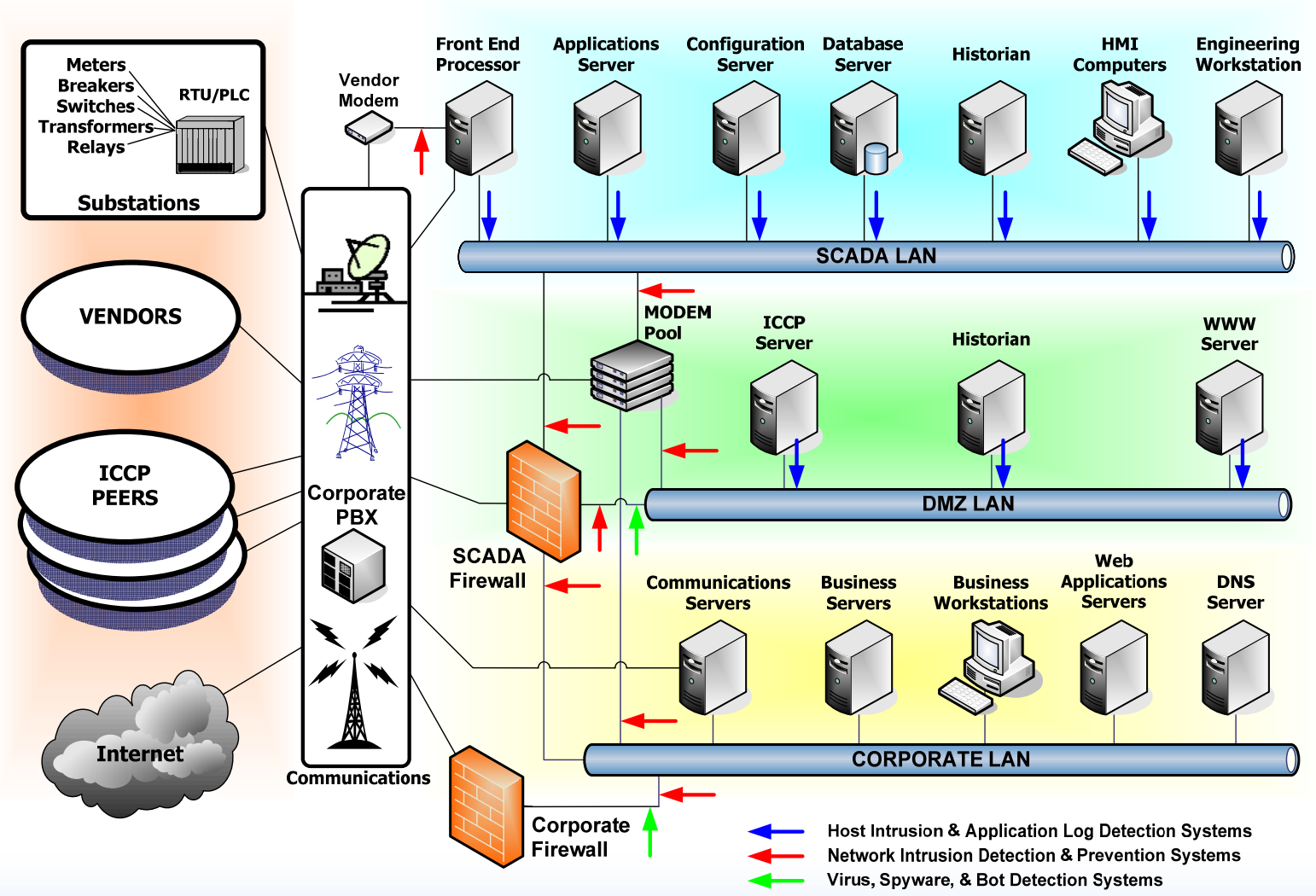
IDS Functions

- **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)*

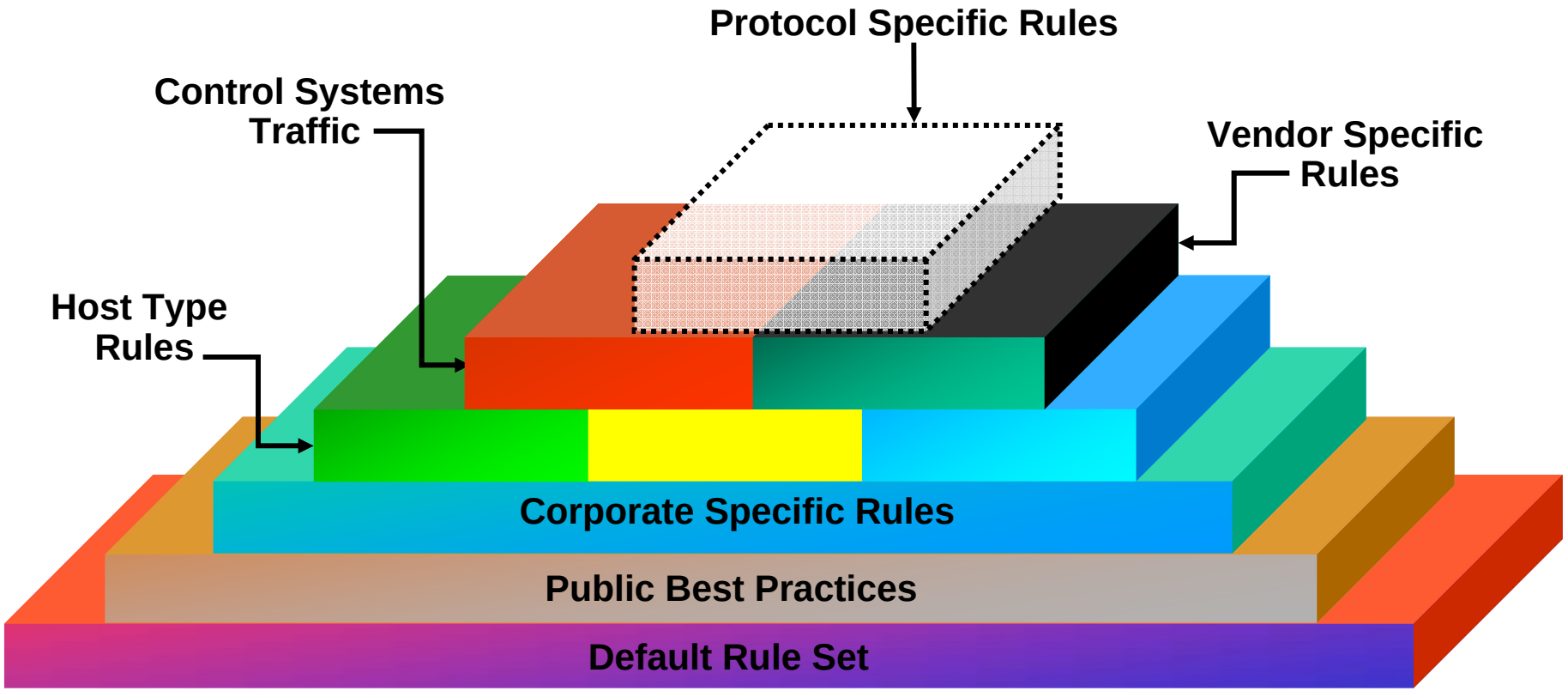
Rule Sets

- **Actions taken: notification, alerting**
- **Writing rules**
- **Data collection**
- **Monitoring IDS**

IDS Placement Overview



Rule Strategy



Rule Set Should Build Upon Existing Rules

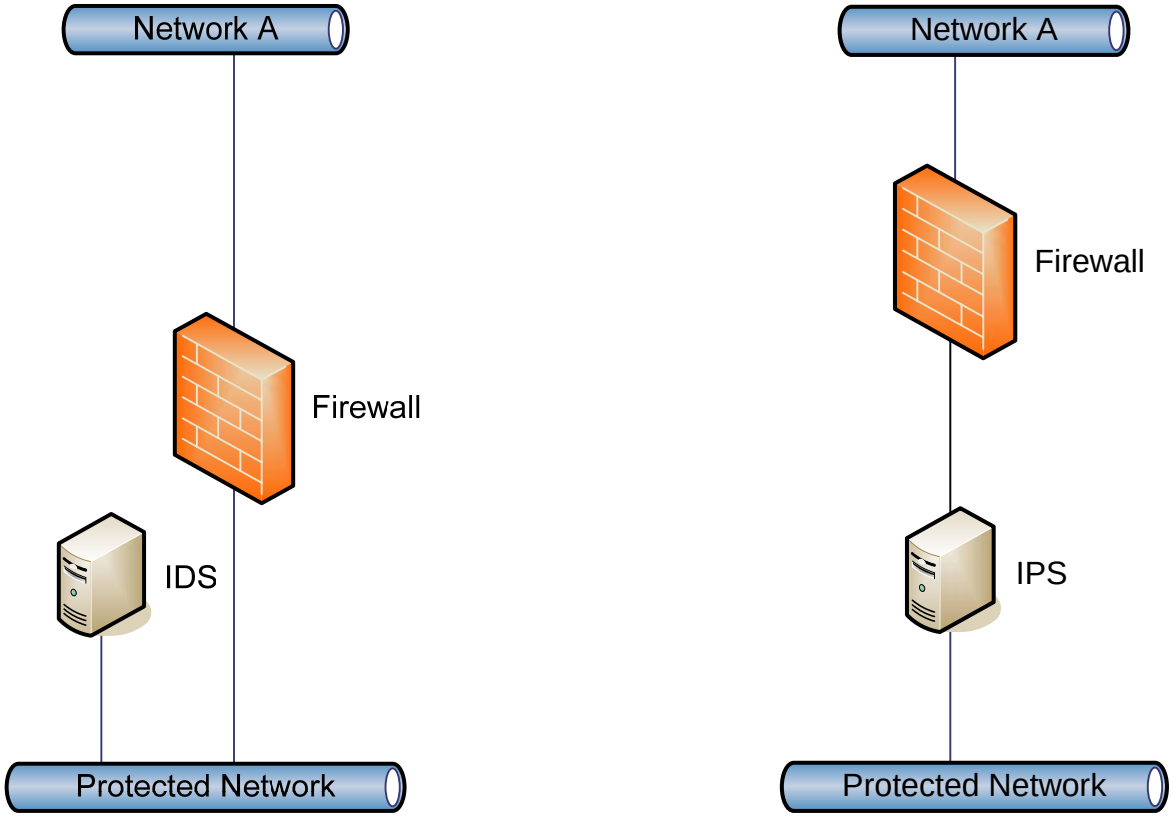
CAUTION: OLE for Process Control (OPC)
- **HMIs assume field devices are COM objects**
- **Use of RPC for DCOM**
- **Windows XP SP2 can break OPC over DCOM**

Adding SCADA Intelligence

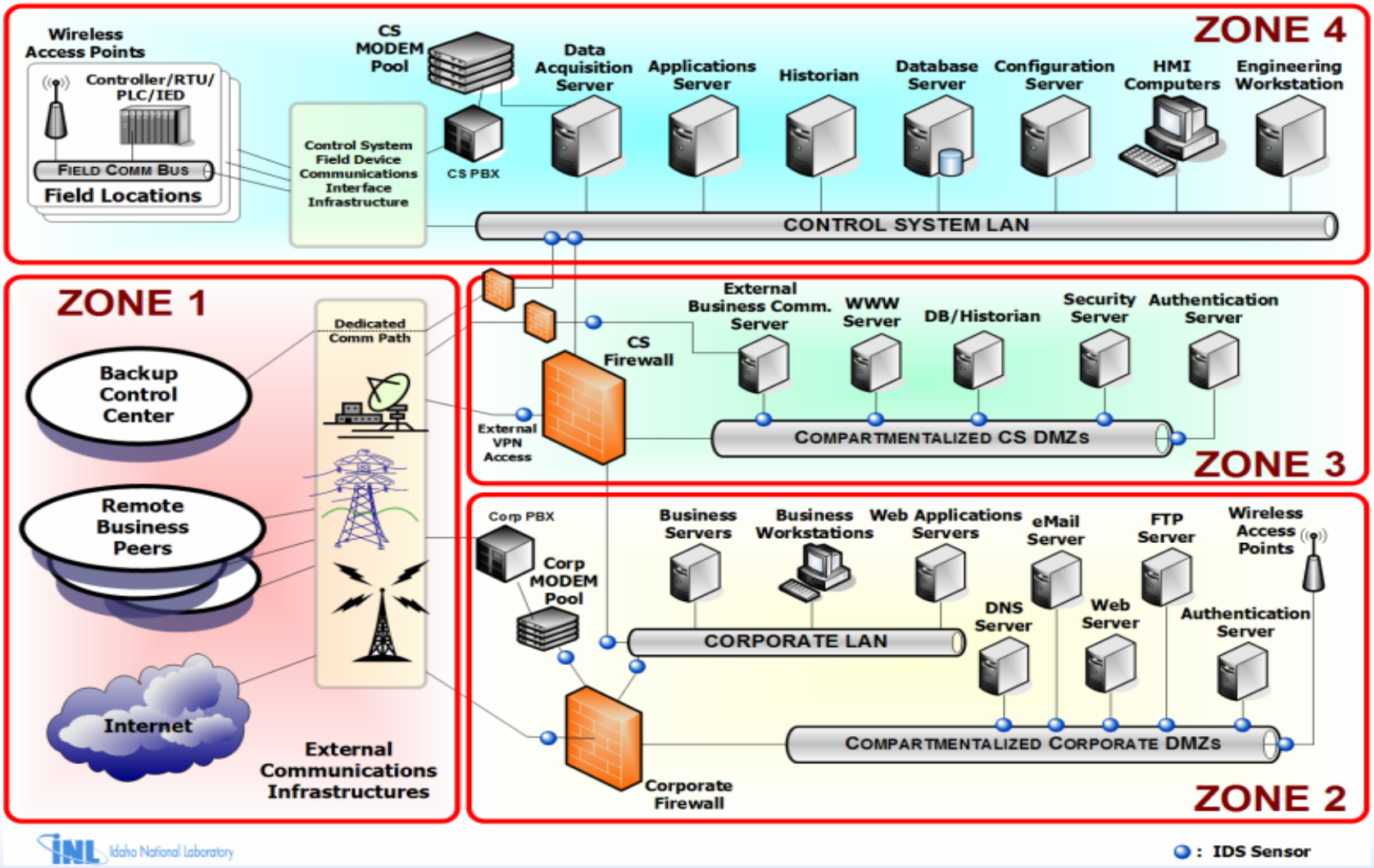
- **Agnostic Snort IDS rules for SCADA Protocols**
  - **Phase I – Modbus TCP, DNP3, OPC**
- **Data Dictionary for SCADA Application Logs**
  - **Phase I – 19 Events**
- **Funded by a DHS Research Contract**
- **Invited proposal for Phase II Research Contract**

This work is supported by a contract from the Homeland Security Advanced Research Projects Agency (HSARPA)

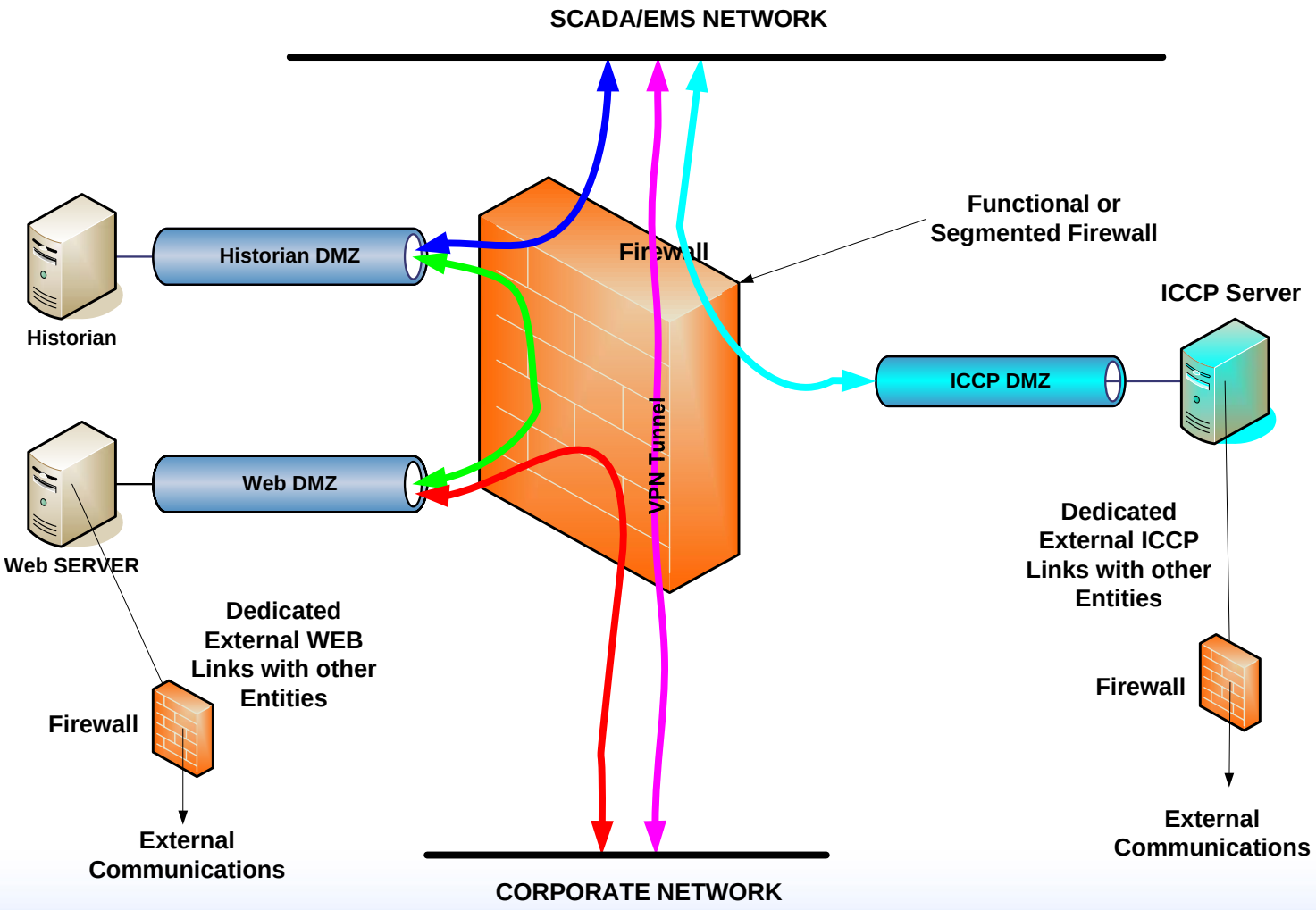
NIDS vs. IPS Placement



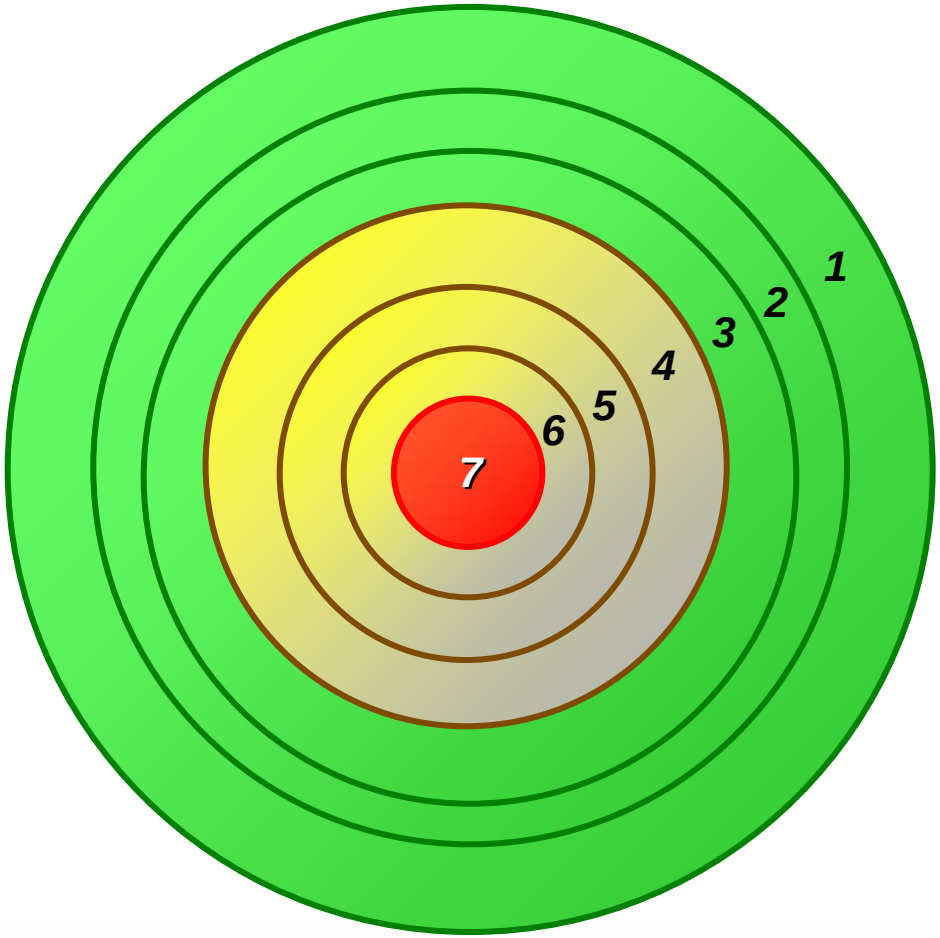
Zones in Control Systems



Firewall Segmented DMZ



Defense in-Depth Security



1 Perimeter Controls –
Internet & 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

Common Sense for Control Systems

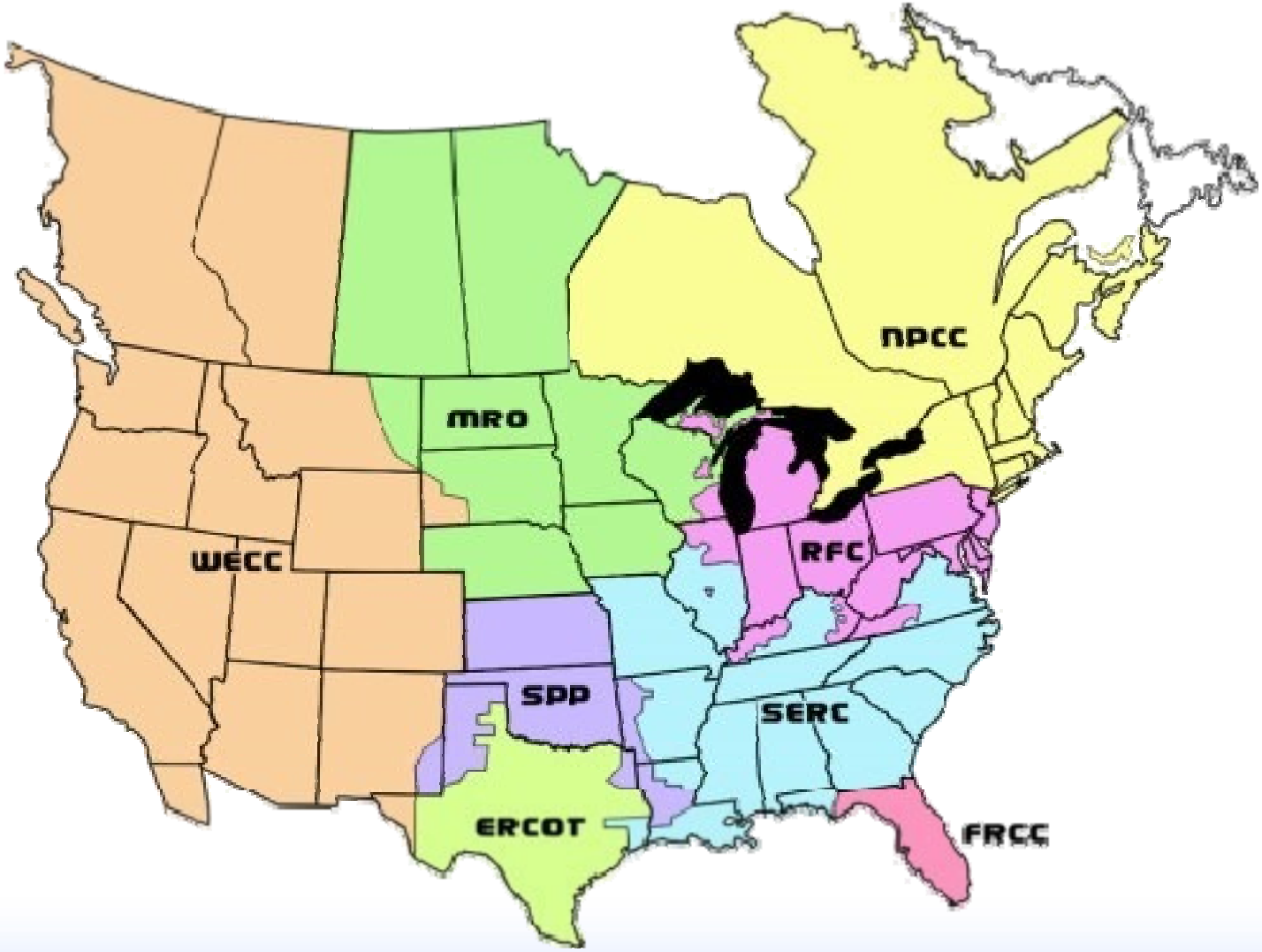
- ICCP links should only move ICCP traffic
- Secure critical clear text traffic
- Use static addressing instead of dynamic (e.g., host tables)
- Reconsider ICMP or other network management protocols on the CS LAN
- Update default parameters (e.g., account names, passwords)
- Remove unused services (disable 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 (VNC etc.)

Layered Security Model

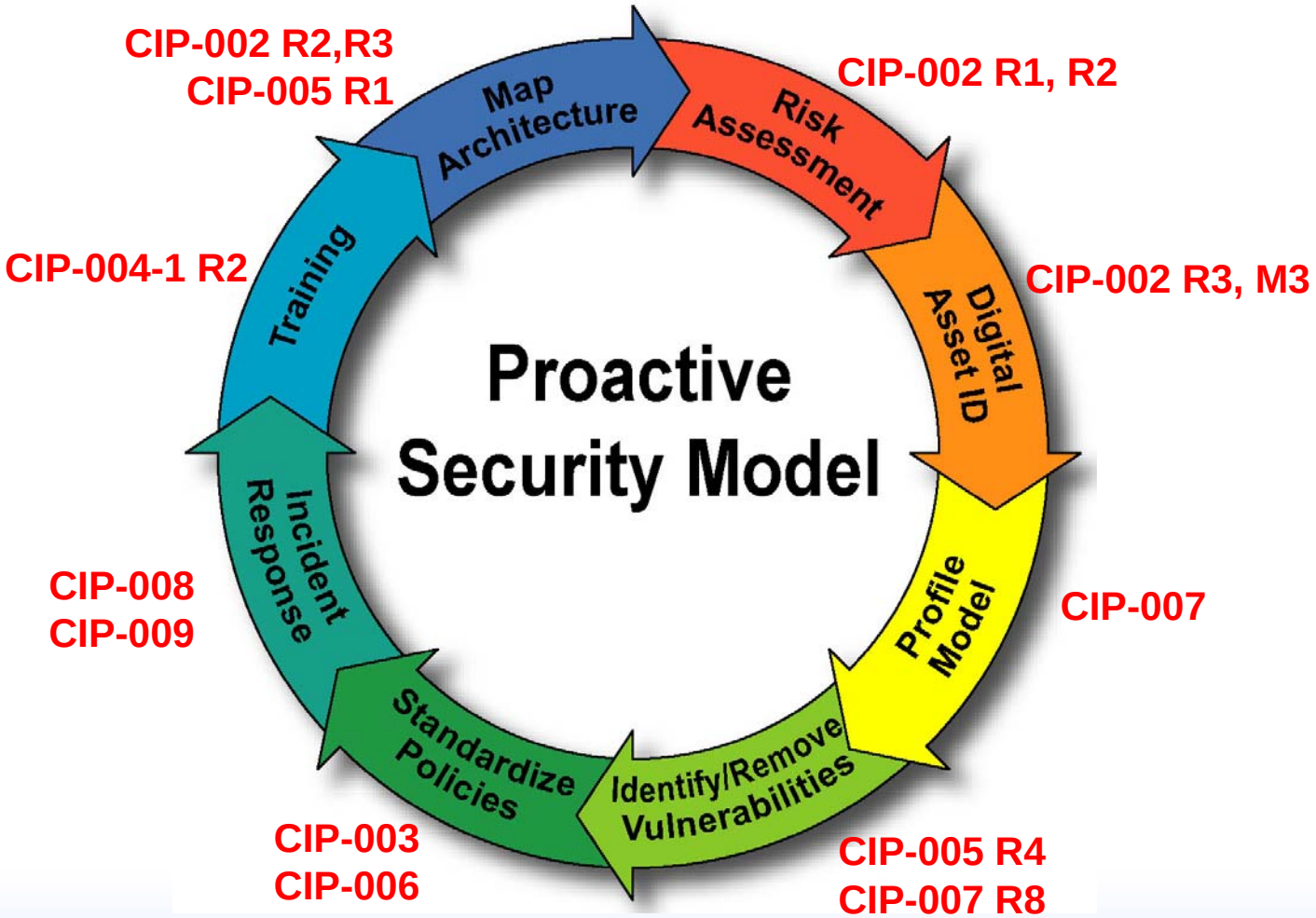
Break

NERC Mitigation Activities

NERC CIP



Security is a Never Ending Process



2005 “Top 10” Vulnerabilities

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

Homeland Security

U.S. DEPARTMENT OF ENERGY

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.

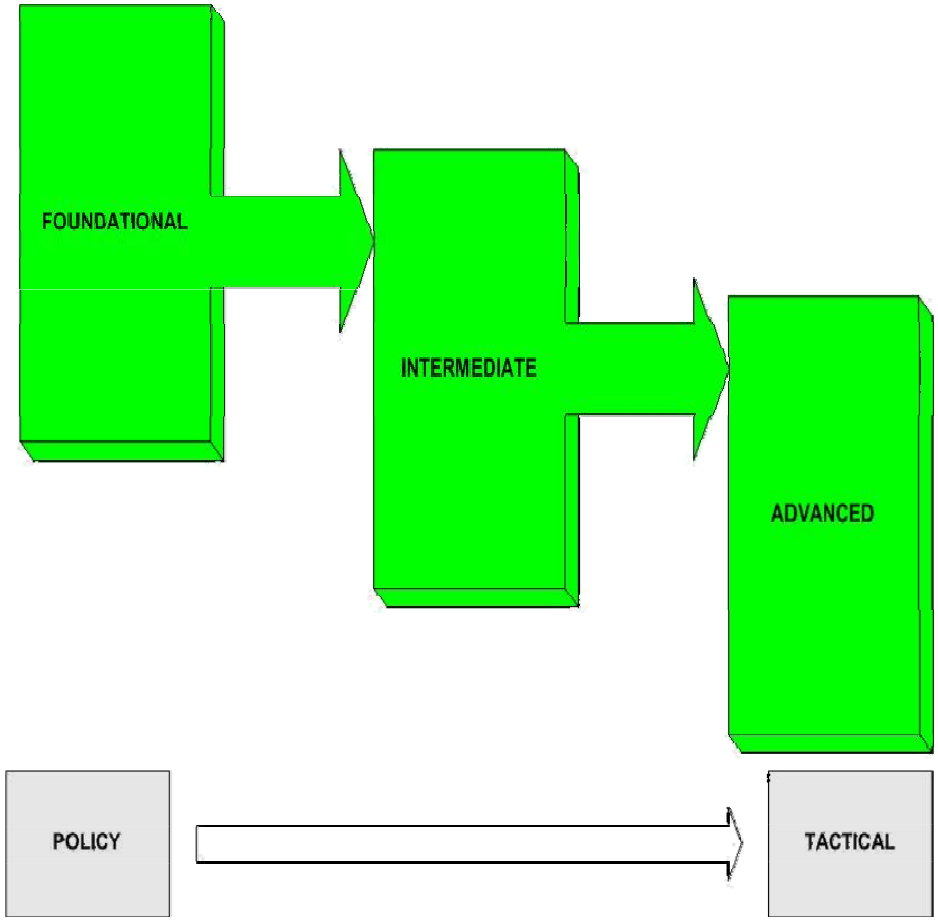
These are not in any order of importance

Preface

- The following mitigation strategies may be applicable to some electricity sector organizations and not applicable to others.
- Each organization must determine the risk 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

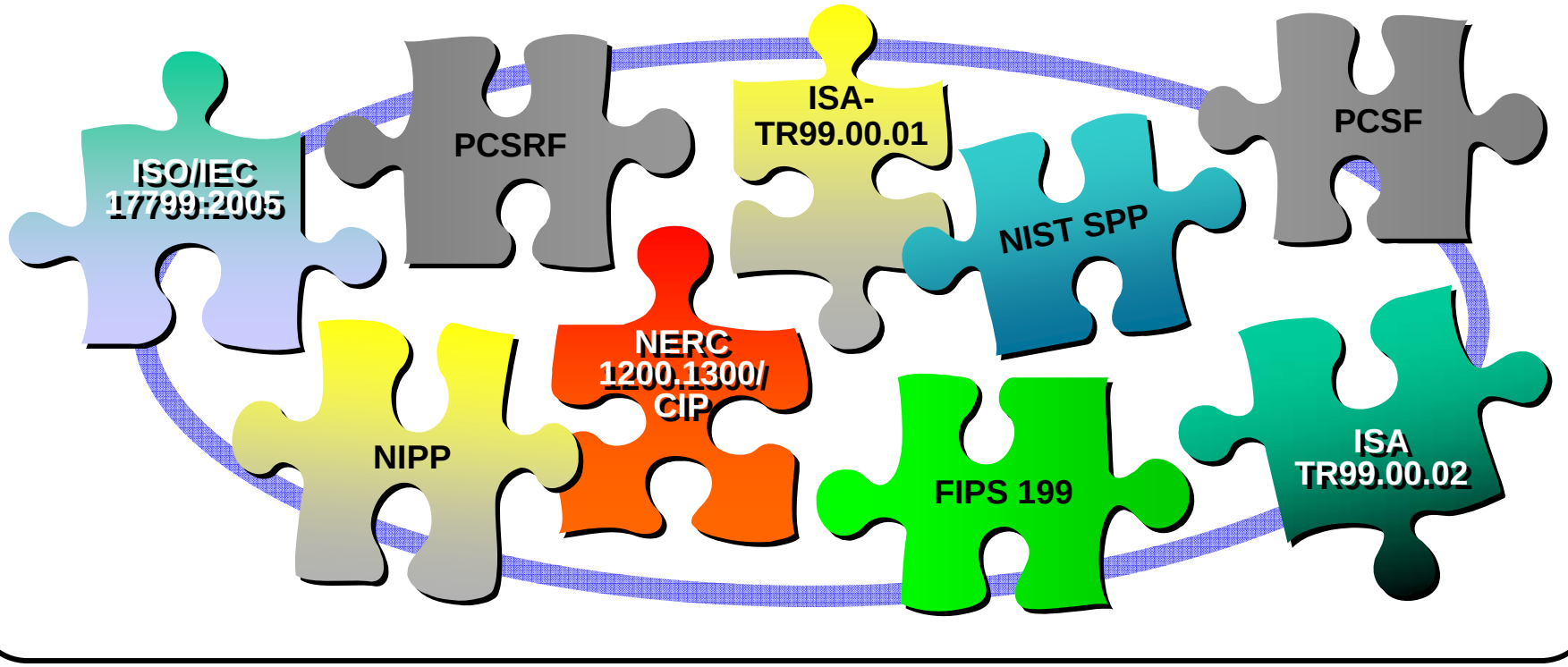
- *Foundational*
  - Implement policies and procedures governing control system security. (ref: NERC CIP Standards)
- *Intermediate*
  - Share industry best practices in security policy structure and topics.
  - Enforce policies and procedures governing control system security.
- *Advanced*
  - Adopt 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

Effective Tools – How to Start?

There Is An Entire Set of Tools to Improve Industry's Resilience and Security Posture



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

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.

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.)

Interactive Exam Discussion

Open Discussion

Legacy Systems?

Questions?

NERC CIP?

For Information - Contact:

Email: scadasummit@inl.gov

Phone: 866-495-7440

Gary J. Finco: gary.finco@inl.gov

Off: 208 526-7048

Ethan Huffman: ethan.huffman@inl.gov

Off: 208 526-0660