Improving SCADA Security

Jerry Litteer, GCIA

Ken Rohde

PCSF Security Workshop Dallas, TX

May 2005

Idaho National Laboratory

Process Control Systems Forum

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.

Workshop Agenda

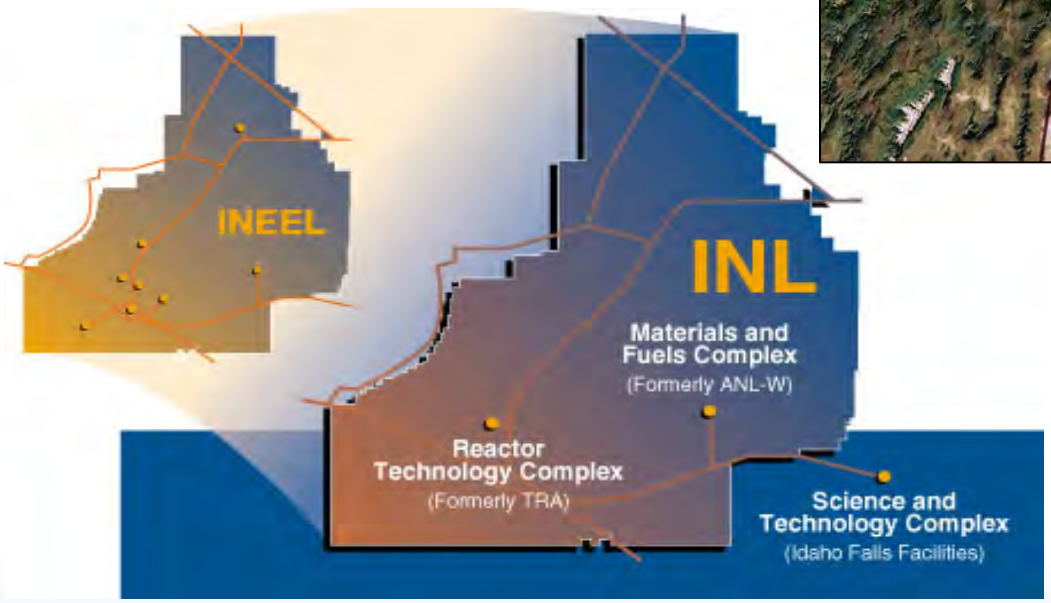
- The INL – Who are we?
- Experiences from field visits
- Demonstration (aka., 'blinky-light-show')
- 10 Minute BREAK
- Anatomy of an Attack
- Network Components and Architecture
- Firewalls and IDS's
- Vulnerability Testing
- Tools and Resources Available
- 20 Minute BREAK
- Hands-On Exercises

INL

Who Are We?

INL

890 square miles
85% size of Rhode Island
National asset since 1940
Dedicated Power Grid
Entire Communications Network



Cyber Security Programs

- Office of Energy Assurance – DOE
- Homeland Security
- National SCADA Testbed
- Control Systems Security Test Center
- National Wireless Testbed

Experiences from Field Visits

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)
- Enforcement of Port Security rare

General Findings

- Dynamic instead of static tables
- Unused software still on systems
- Unused services still active
- Writeable shares
- Direct VPN from off site allowed

Switches and Routers

- Like most systems, delivered wide open
- Network Administrators have little or NO knowledge how to secure (INDUSTRY WIDE)
- In most cases, DEFAULTS are NOT shown in configuration lists
- Enforced Port Security rare

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

IDS

- New to Electric Utility industry (~ NERC 1300)
- Not even employed at corporate level
- No scope for staffing and training

NERC 1300 (1304)

- The identification of the electronic (also referred to as logical) security perimeter(s) inside which critical cyber assets reside and all access points to these perimeter(s),
- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical assets within them, and
- The implementation of processes, tools, and procedures to monitor electronic (logical) access to the perimeter(s) and the critical cyber assets.

(3) Monitoring Electronic Access Control:

The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized

Page 17 of 35

Draft Version 1.0
September 15, 2004

Standard 1300 — Cyber Security

DRAFT

access to the electronic perimeter(s) and critical cyber assets within the perimeter(s), 24 hours a day, 7 days a week.

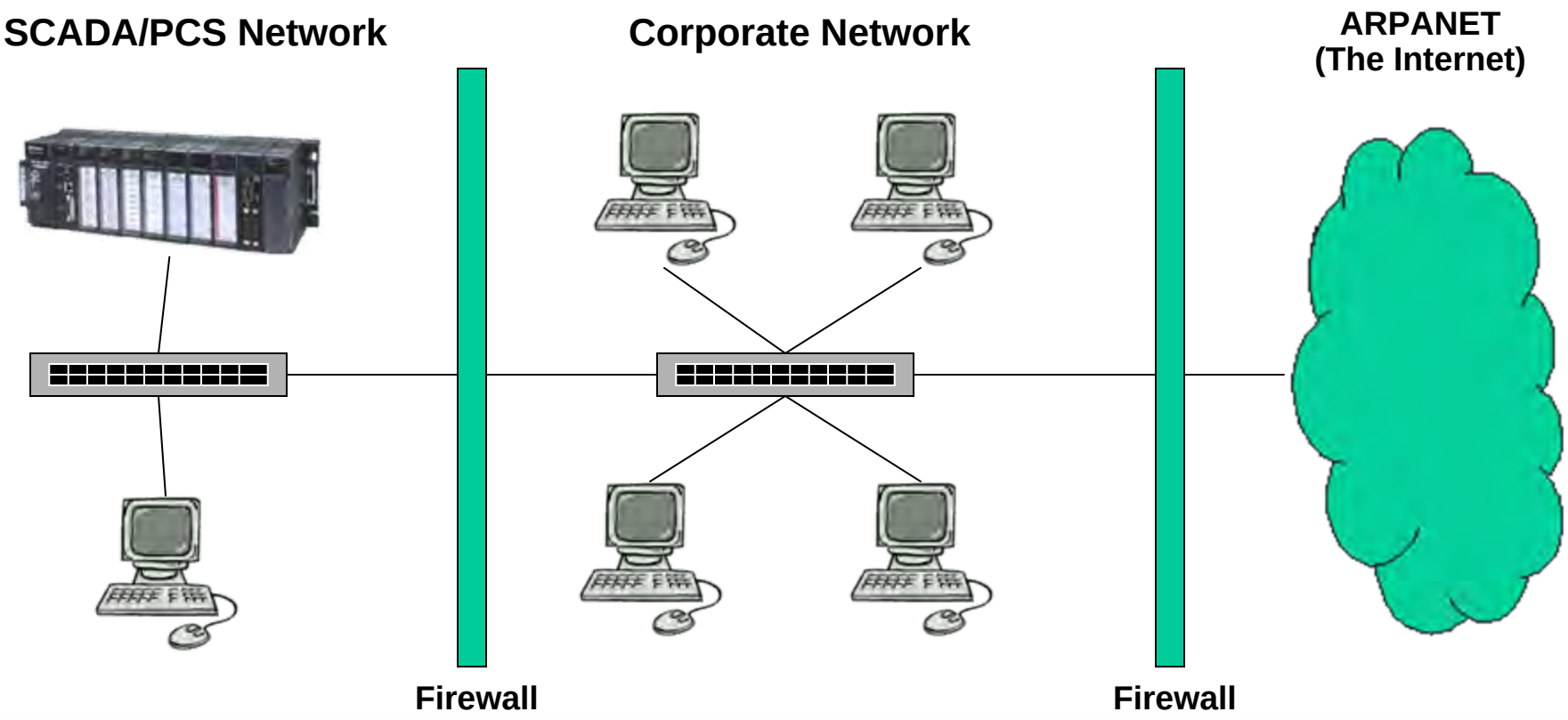
Evolution of IT Security vs. PCS Security

© 2002 PA Knowledge Limited

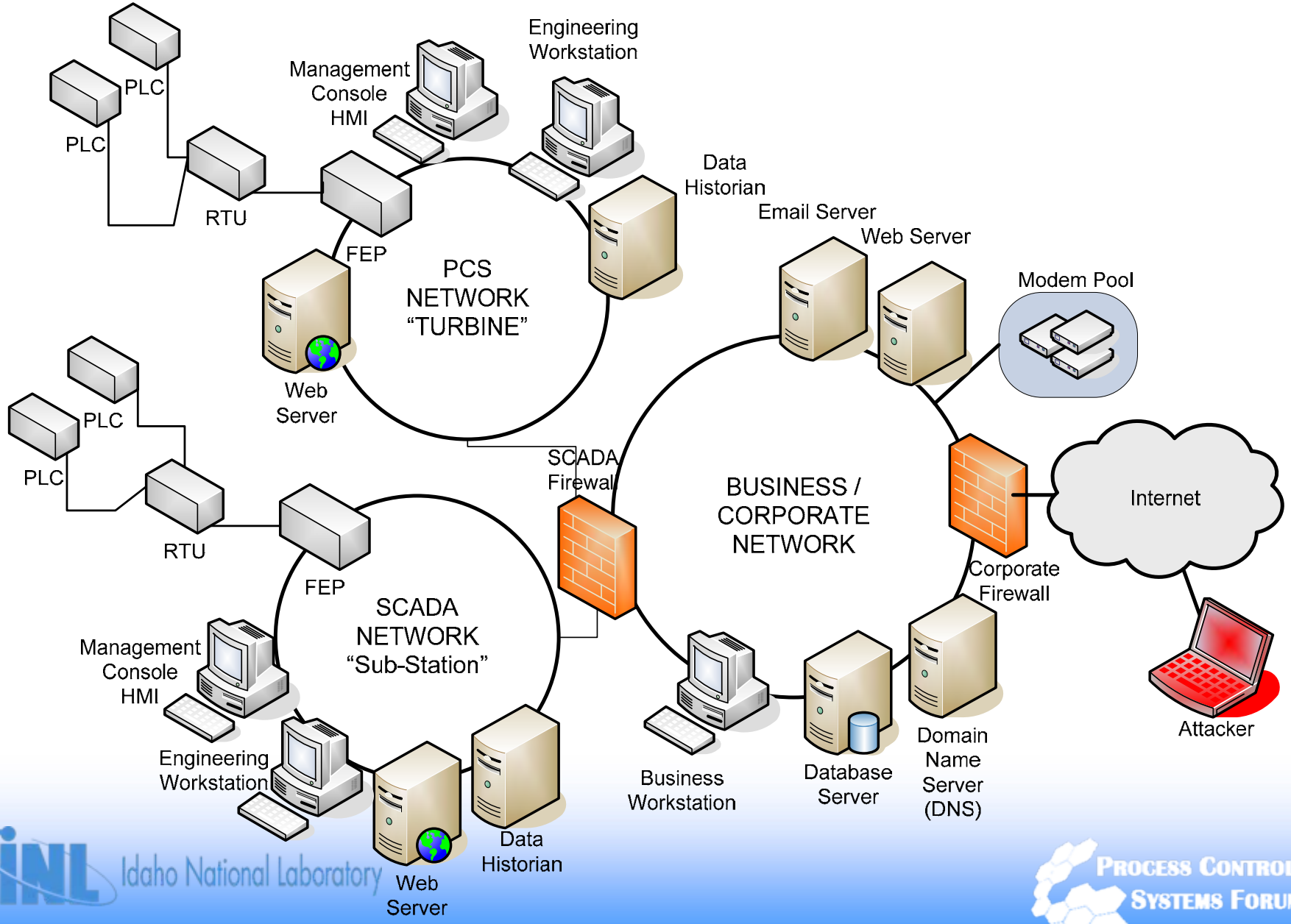
TOPIC	INFORMATION TECHNOLOGY	PROCESS CONTROL
Anti-virus/Mobile Code	Common/ Widely Used	Uncommon/Impossible to deploy
Support Technology Lifetime	3-5 Years	Up to 20 Years
Outsourcing	Common/Widely Used	Rarely used
Application of Patches	Regular/Scheduled	Slow (Vendor specific)
Change Management	Regular/Scheduled	Rare
Time Critical Content	Generally delays accepted	Critical due to safety
Availability	Generally delays accepted	24x7x365xforever
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

The Demonstration

The Evolution of the Internet



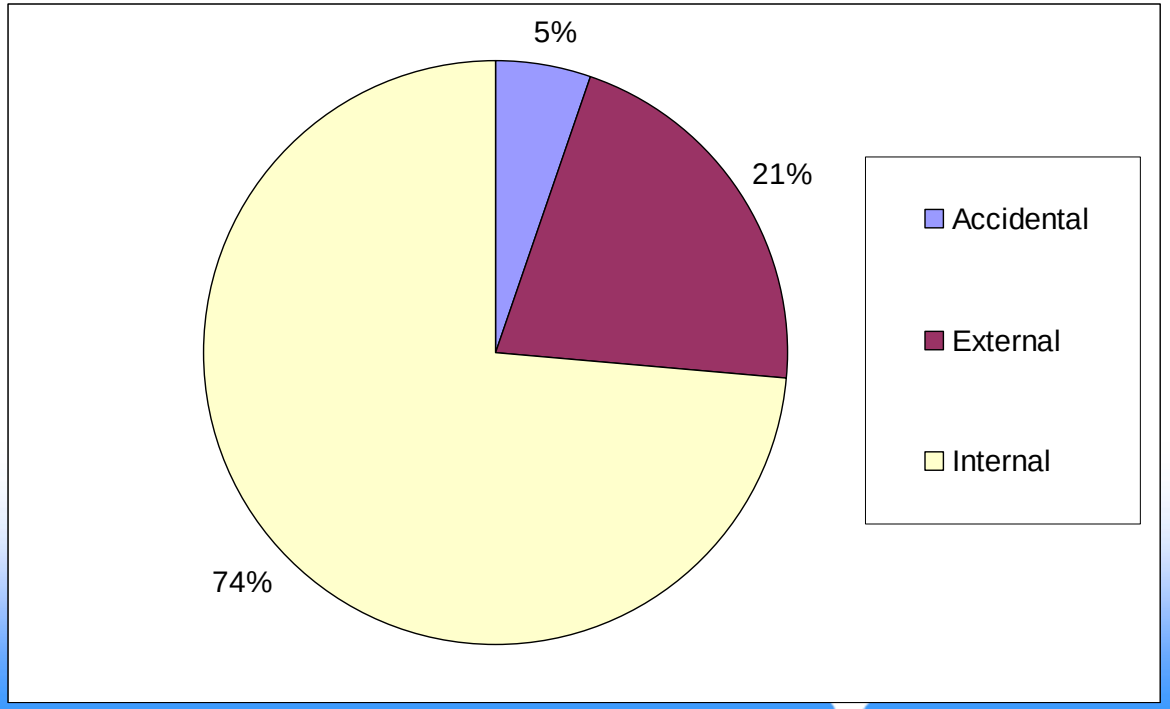
Common Control System Architecture



Industrial Cyber Incidents 1982 - 2000

Threats are primarily Internal:

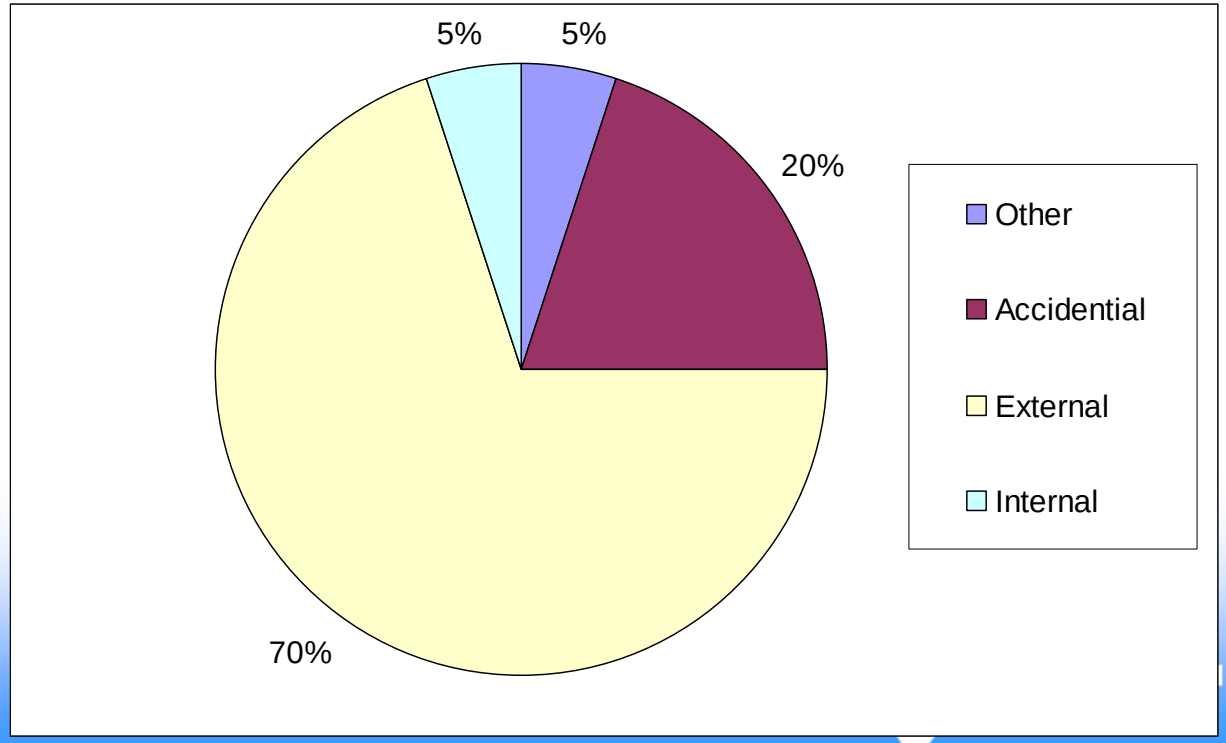
- **Accidental**
- **Inappropriate employee activity**
- **Disgruntled employees**



Idaho National Laboratory

Industrial Cyber Incidents 2001 - 2003

In 2001 the threat source shifts…. Why?



Idaho National Laboratory

Changing Vulnerabilities: Common OS Weaknesses

Common operation systems (i.e. Windows) and applications (e.g. SQL Server) now dominate the HMI systems.

- Often come configured more appropriately to business requirements.
- Vulnerable to a wide variety of IT attacks and viruses.

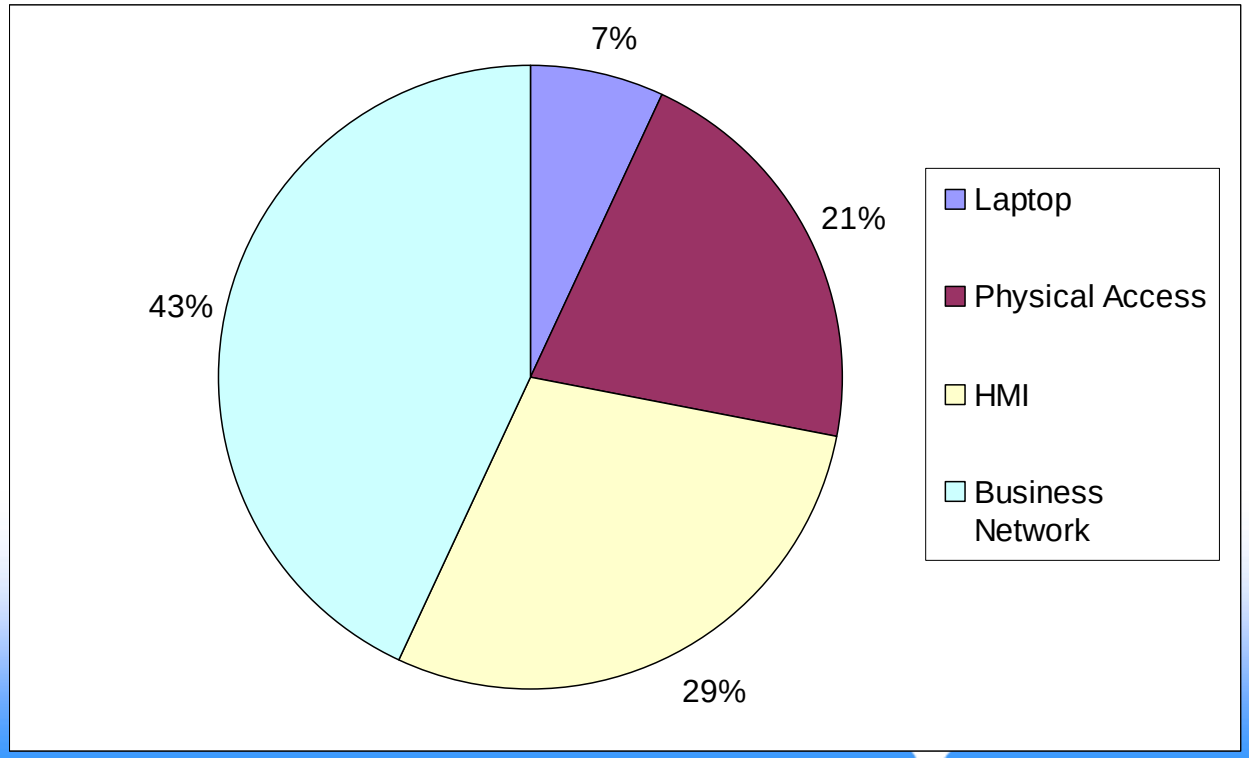
Changing Vulnerabilities: Common Network Weaknesses

- Ethernet and TCP/IP now dominate the process control network.
- COTS network hardware common in plant.
- Vulnerable to:
  - Hardware-specific exploits (e.g. HP printers);
  - Attacks against TCP/UDP services (e.g. SNMP).

How They Get In (Local Entry)

The business network is the major local source of incidents.

- **Direct physical access is significant.**

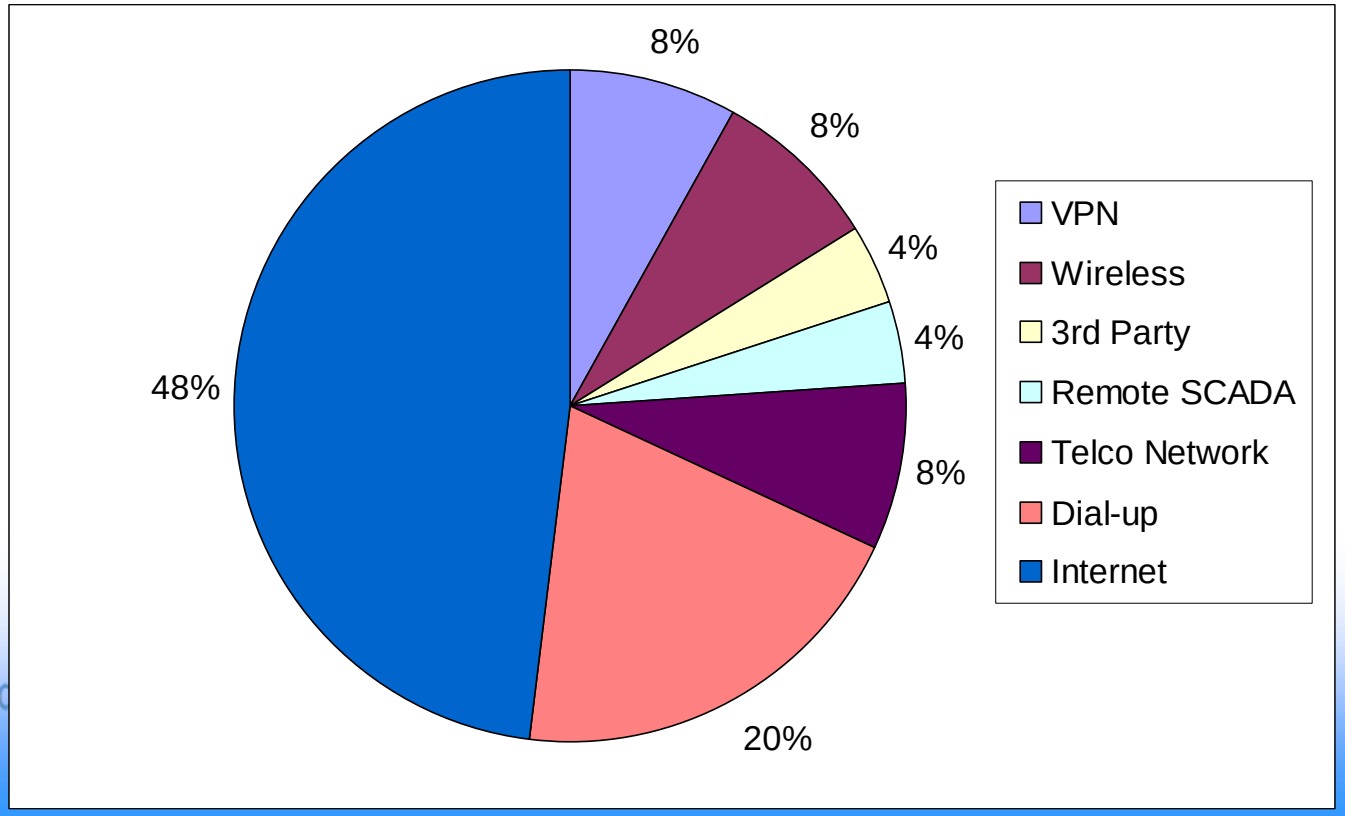


Idaho National Laboratory

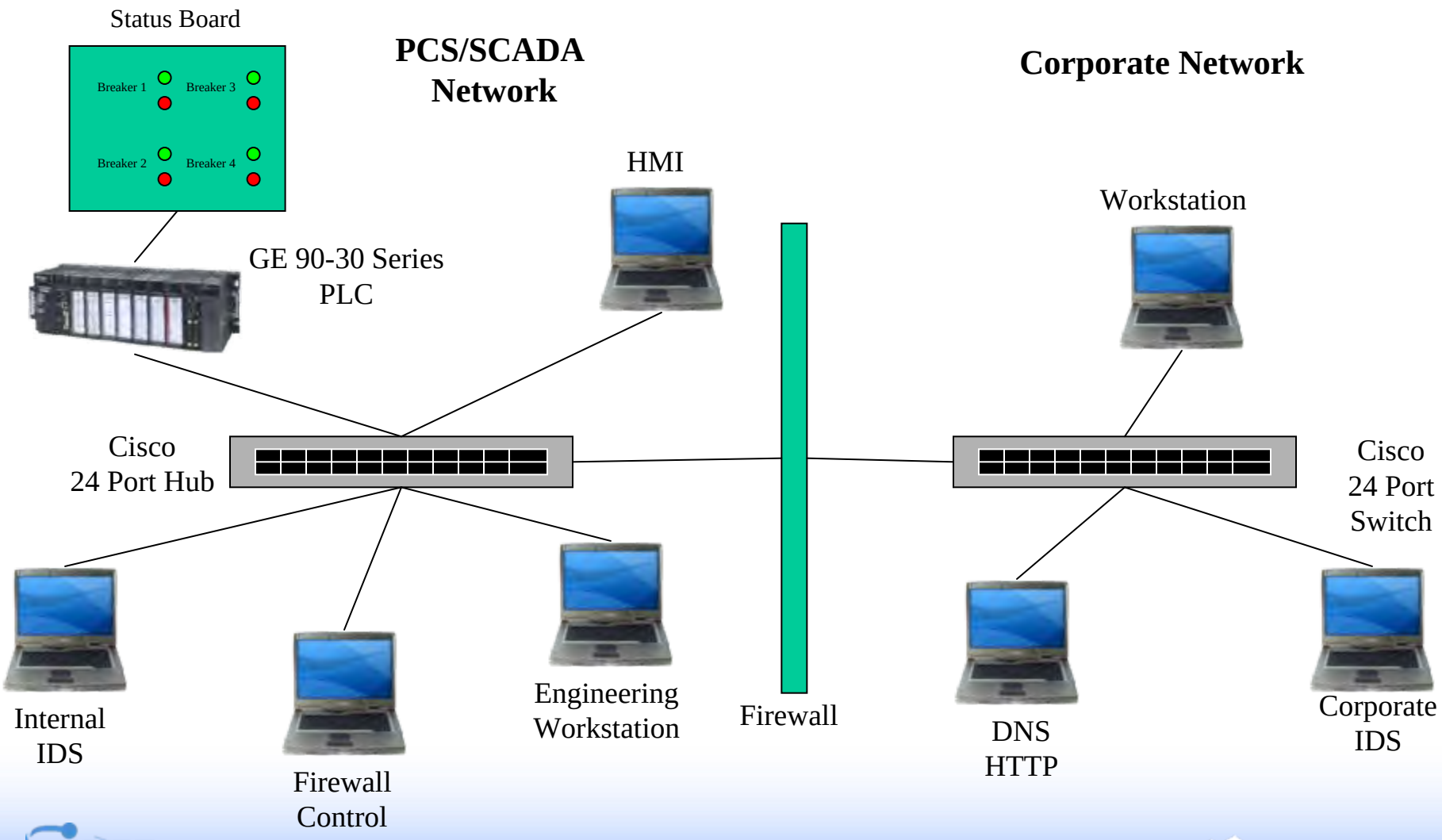
How They Get In (Remote Entry)

The Internet is a major source (but we don't always really know the route in).

- **Dial-up, VPN, Telco, Wireless, 3rd Party are all contributors.**



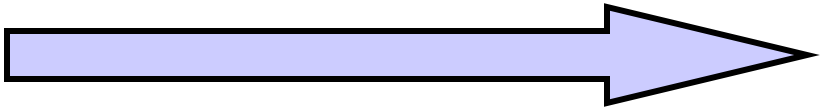
Mobile Network Overview

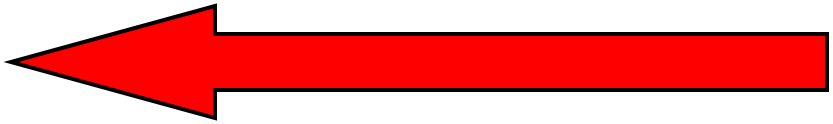


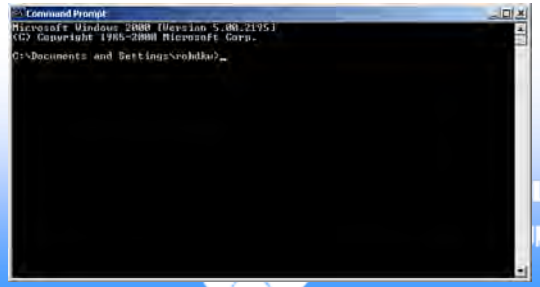
Demonstration Exploits

- **Internet Explorer Drag & Drop**
  Announced in early August 2004
  Affects all versions of IE on all Windows OS
- **GDI+ JPEG Overflow (MS Windows)**
  Announced in late September 2004
  Affects all software using the Microsoft GDI+ library
- **Libpng Overflow (Linux)**
  Released in early August 2004
  Affects Linux based systems using libpng version 1.2.5 and earlier

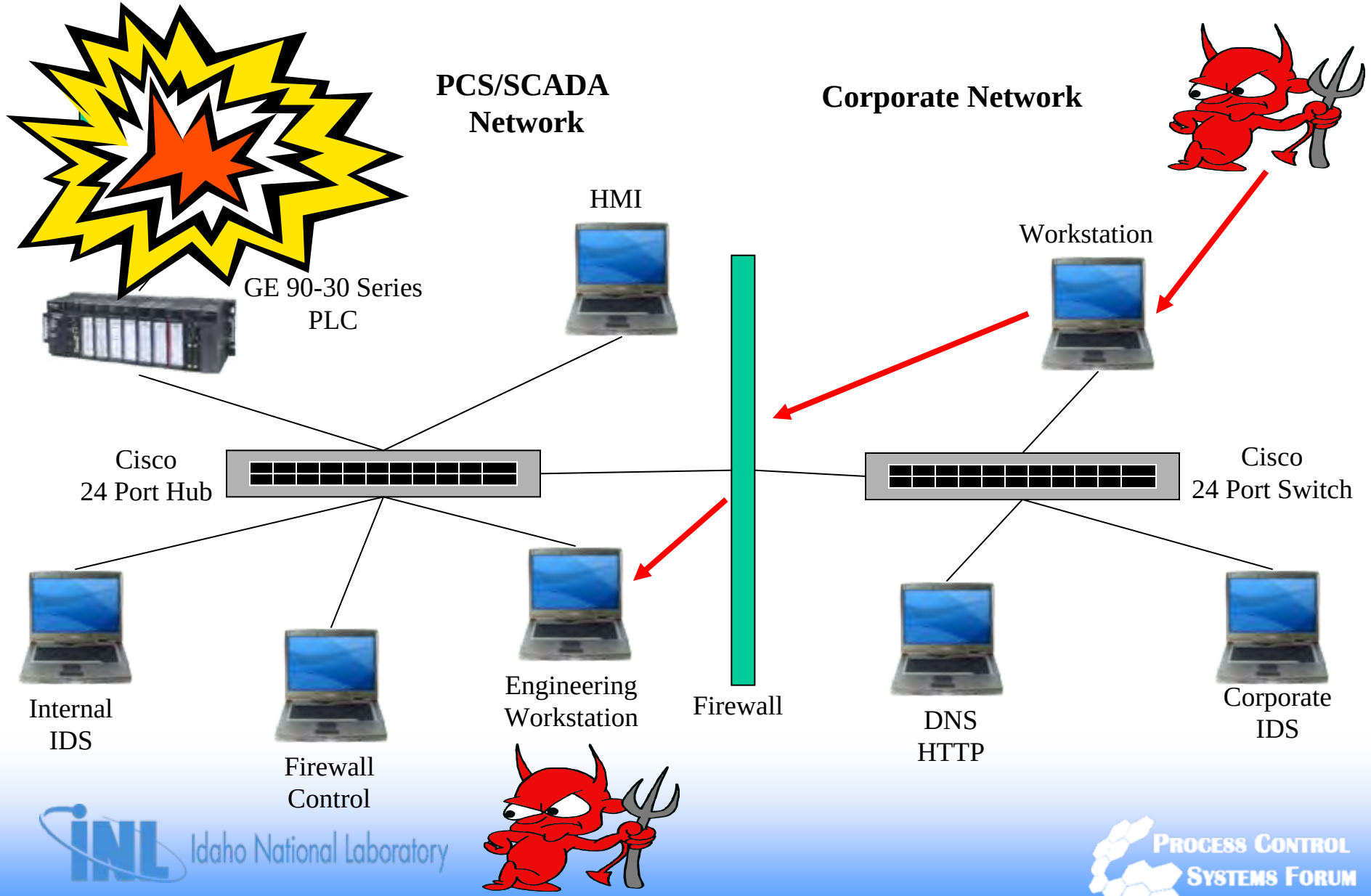
Infected Image Exploits







Attack Overview

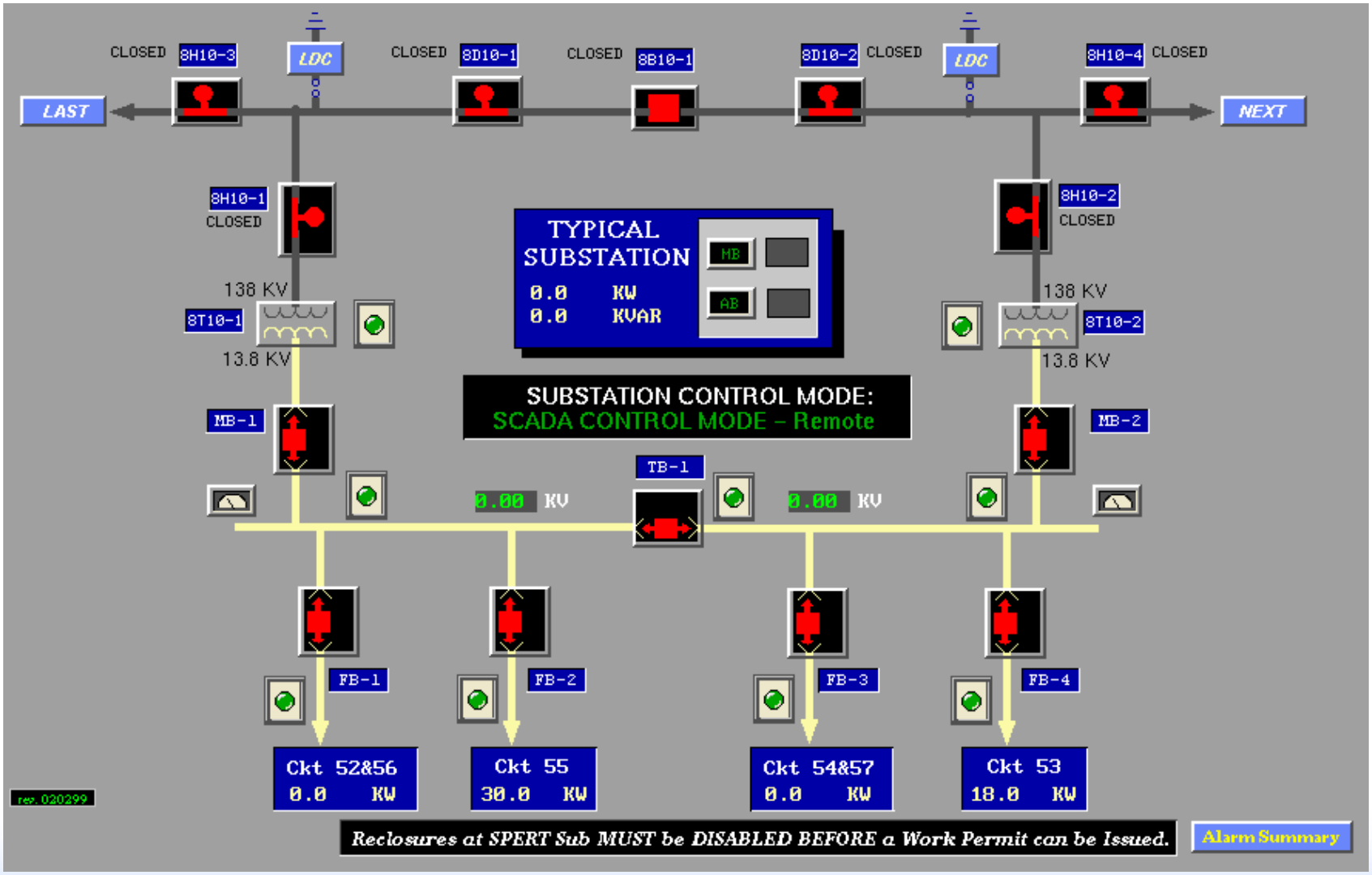


Man in the middle

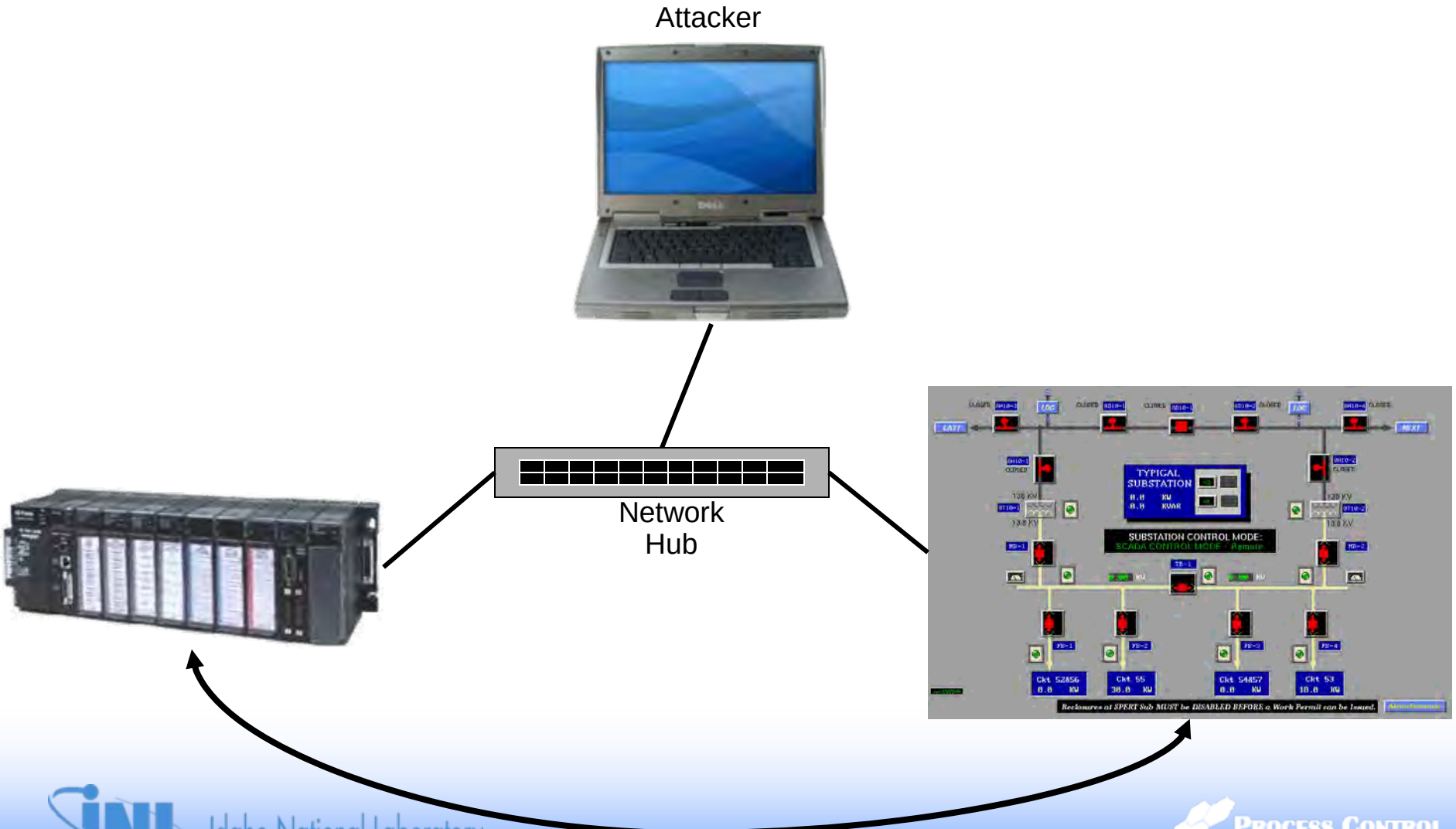
Man-in-the-middle: Components

- HMI – The operators console
- Control Systems Equipment
- ARP Spoofer – Listens to all traffic between two nodes
- Attacker – Controls the equipment or the HMI without the others knowledge

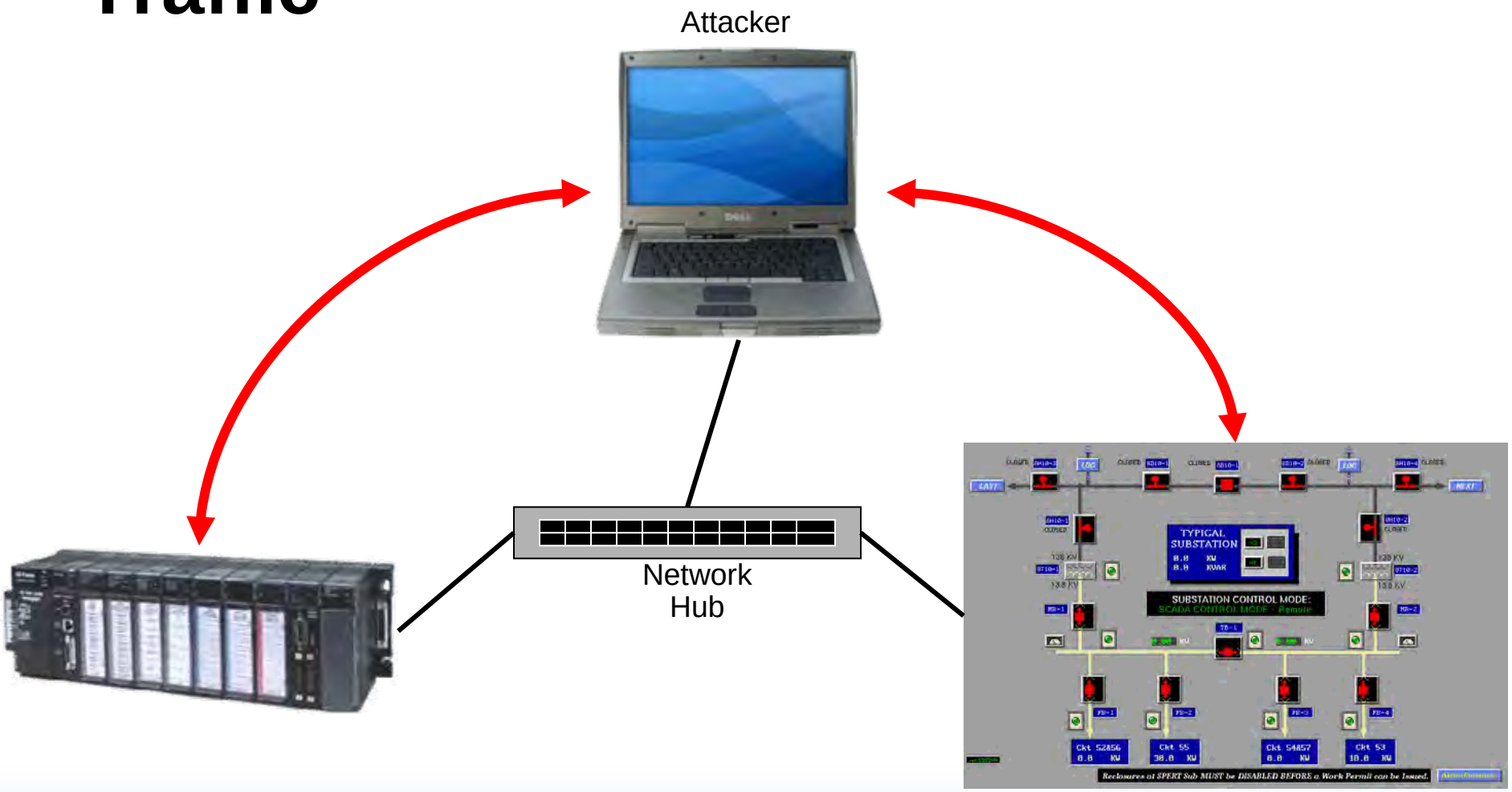
Typical Management Display (HMI)



Man-in-the-middle: Normal Traffic



Man-in-the-middle: Controlled Traffic



Break Time

Anatomy of an Attack

The Risk Equation

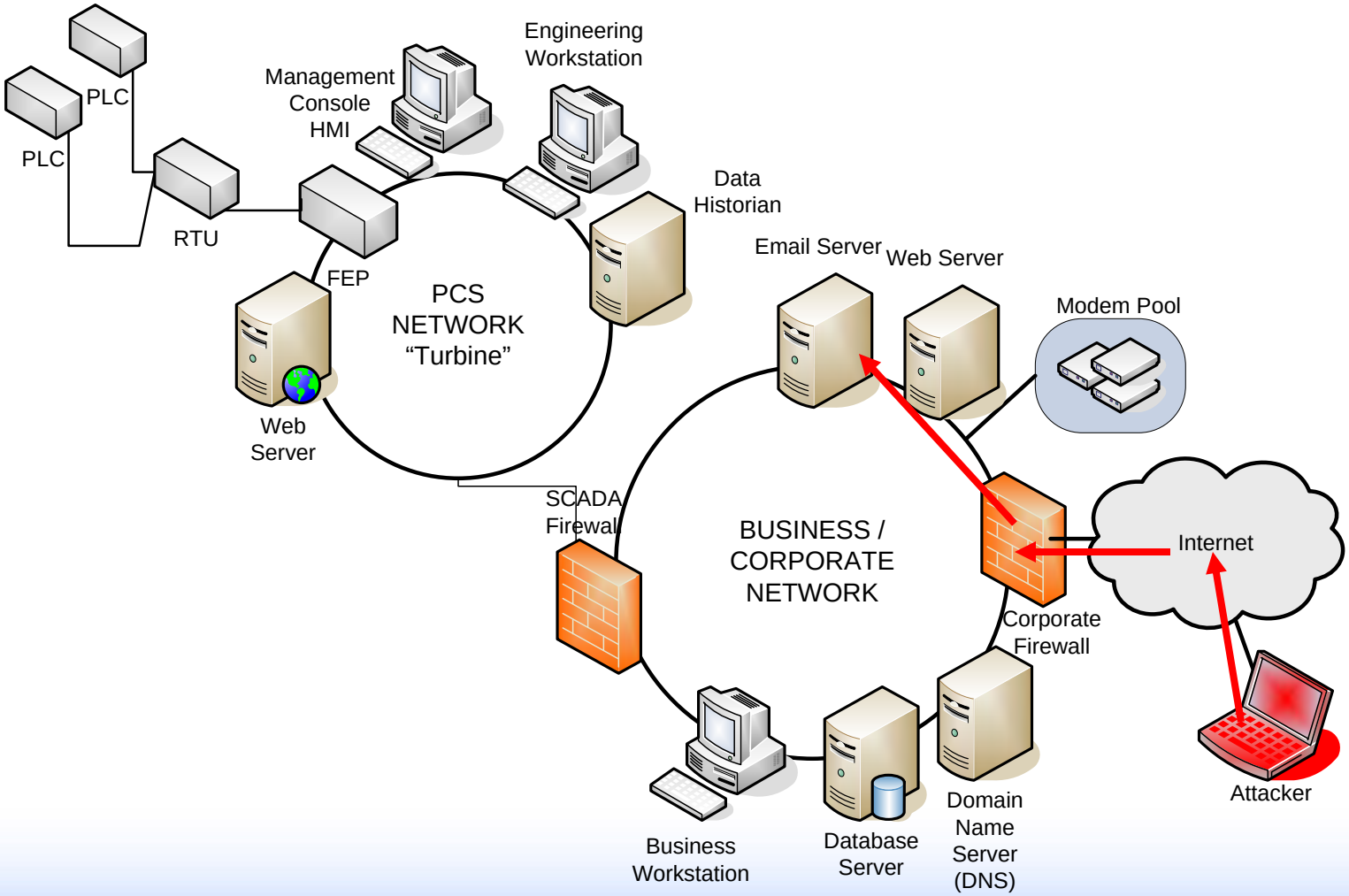
Risk = Threat x Vulnerability x Consequence

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

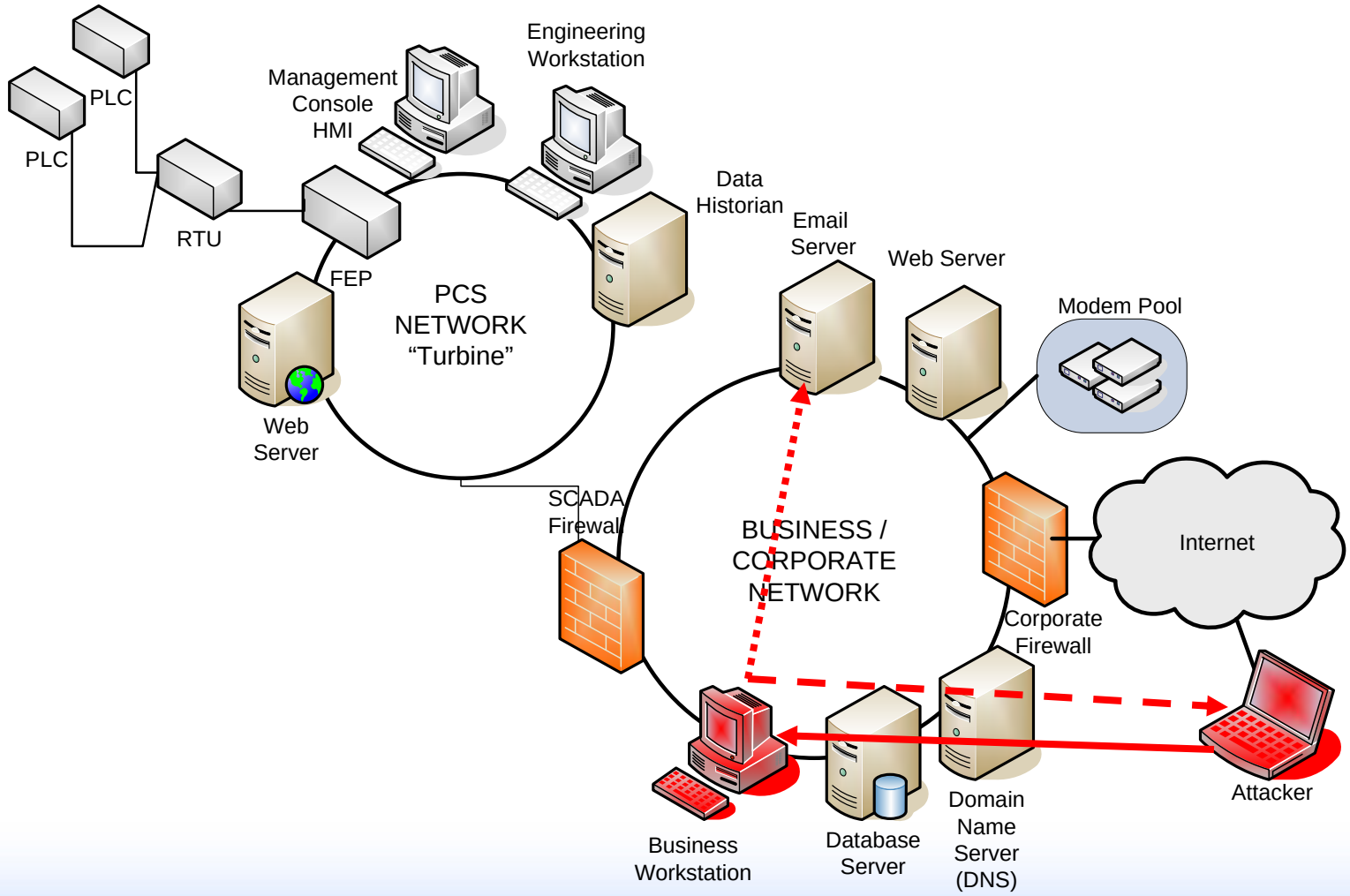
A Simple Example

Attacker

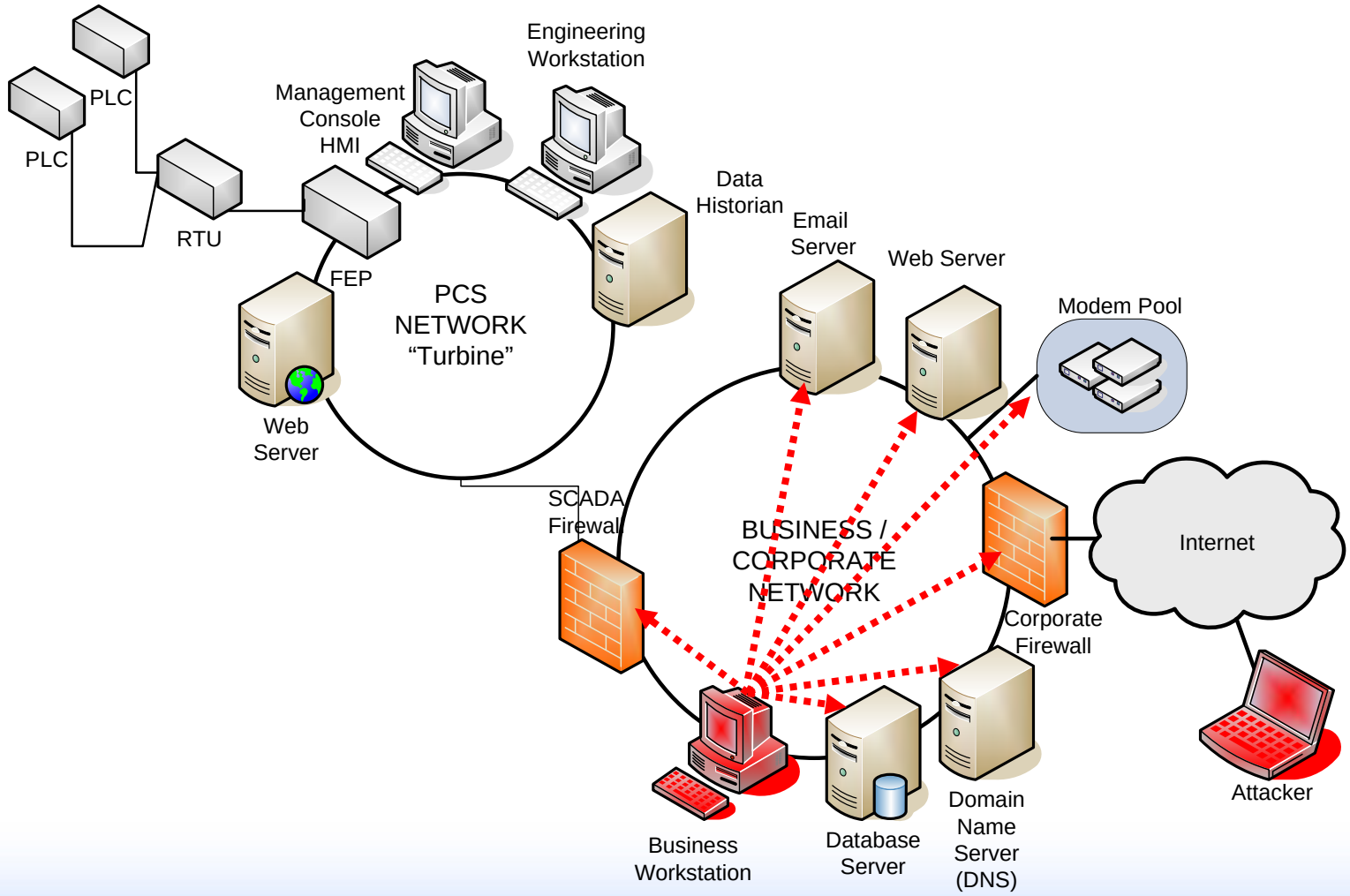
Step #1


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

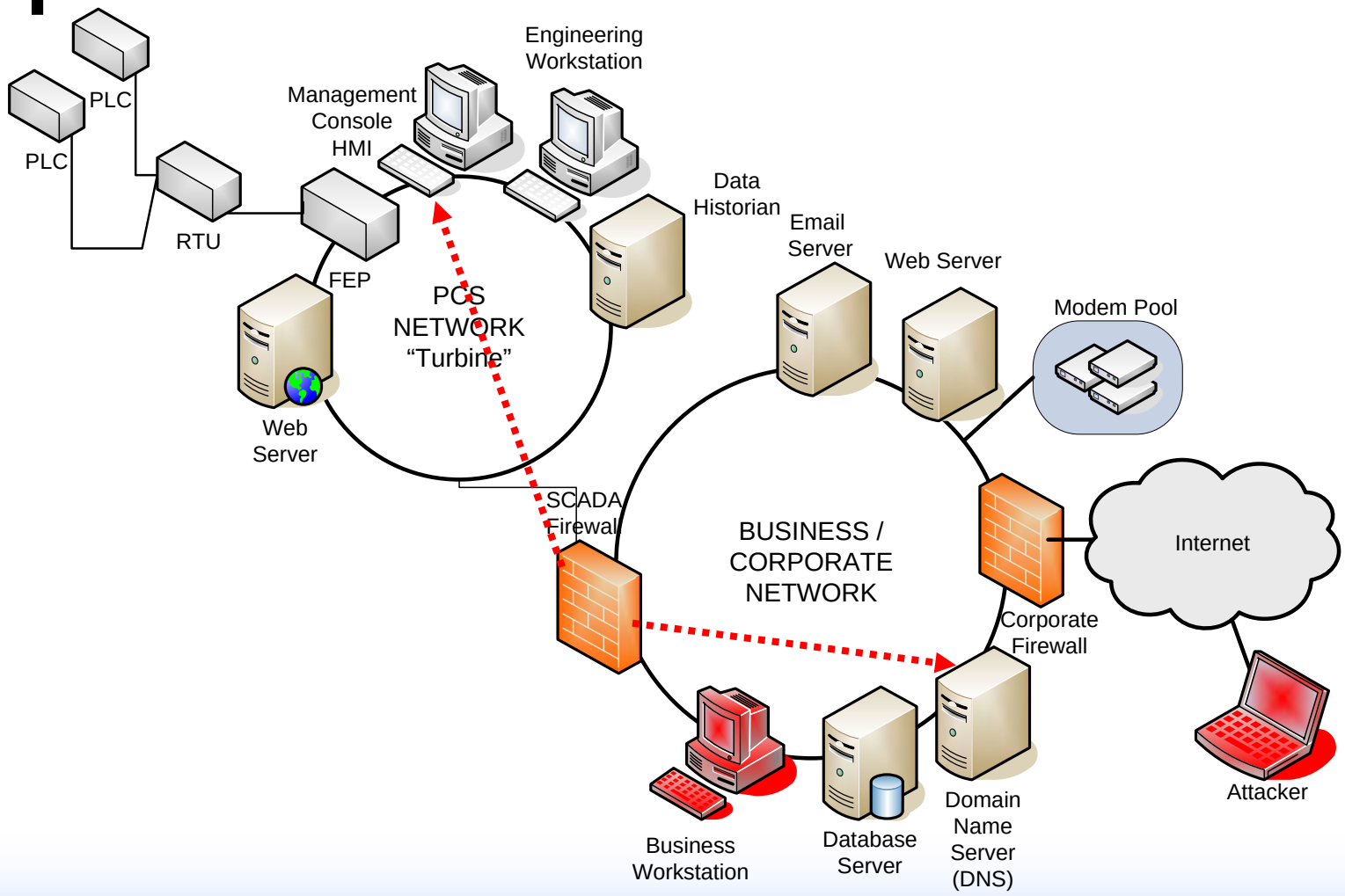
Step #2


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

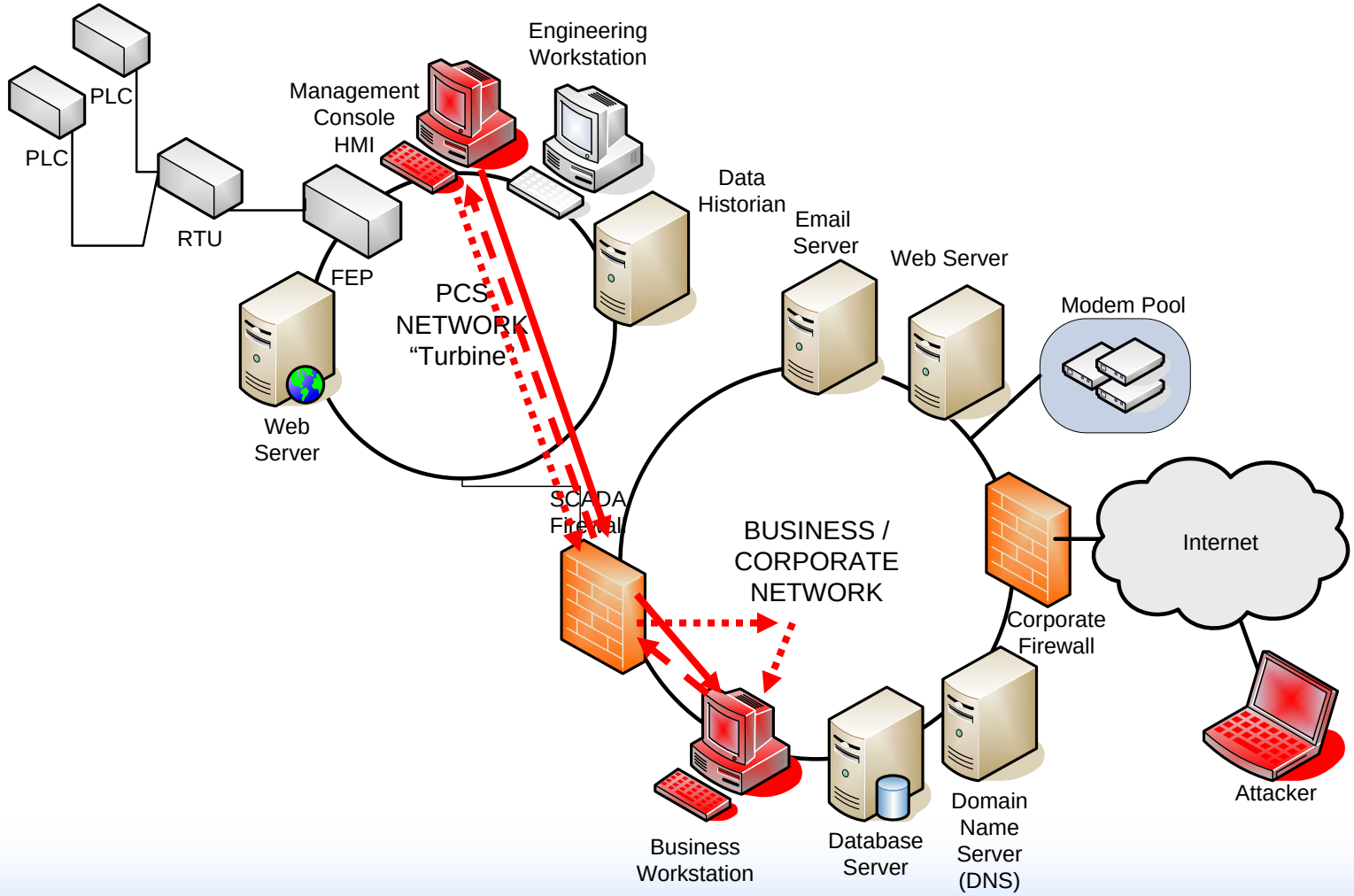
Step #3


PLC
PLC
RTU
Management
Console
HMI
Engineering
Workstation
FEP
Data
Historian
PCS
NETWORK
"Turbine"
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

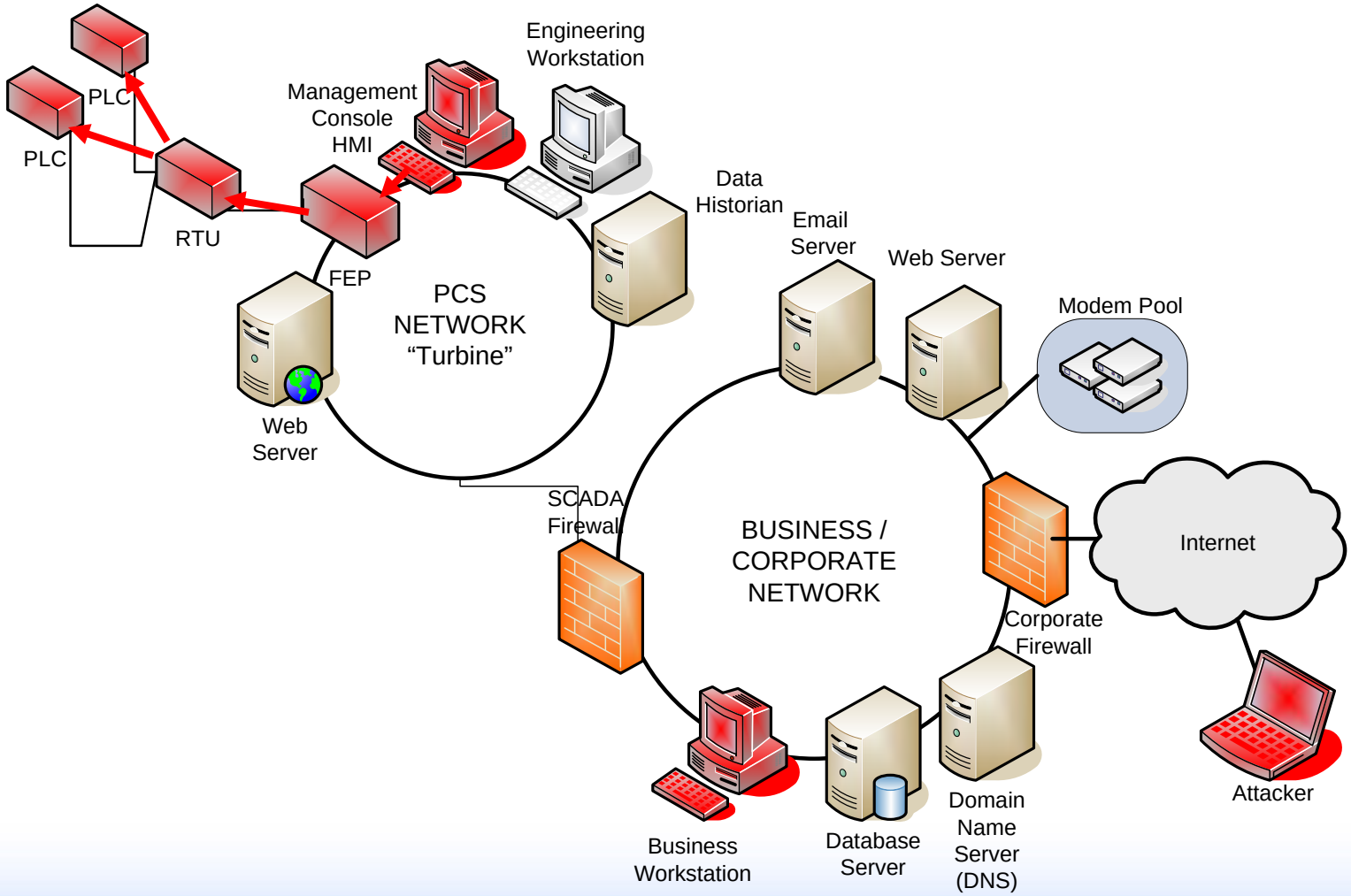
Step #4


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

Step #5


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

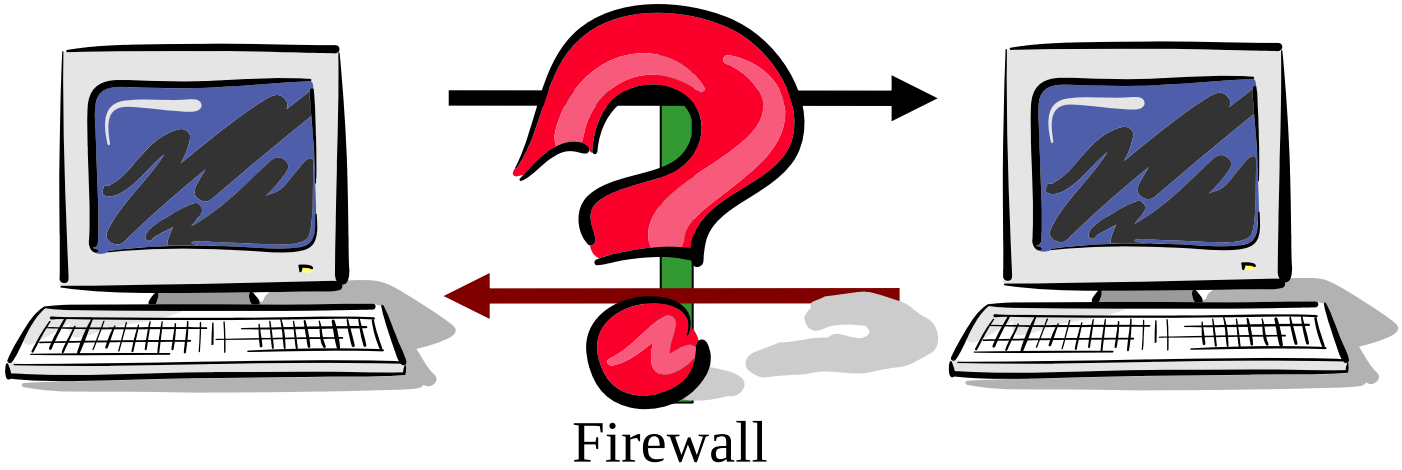
Step #6


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

Changing Vulnerabilities

- Common Operating System Vulnerabilities
- Common Application Vulnerabilities
- Common Network Vulnerabilities

Myth Busters



SCADA Data Base **Corporate Data Base**

The Myth

Vendor Says:

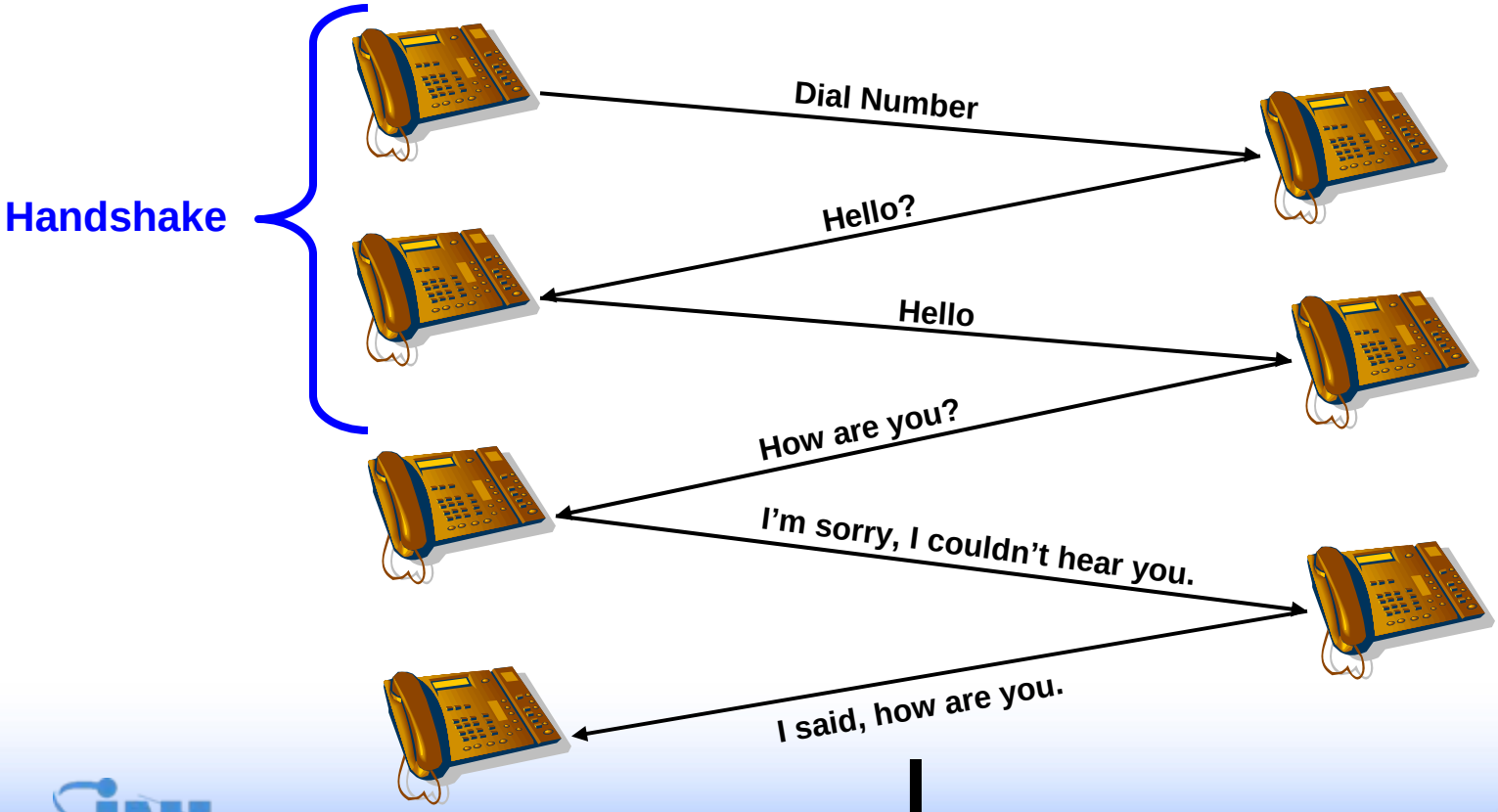
- **“Data only flows to the corporate Data Base”**

IT Says:

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

Communication Basics

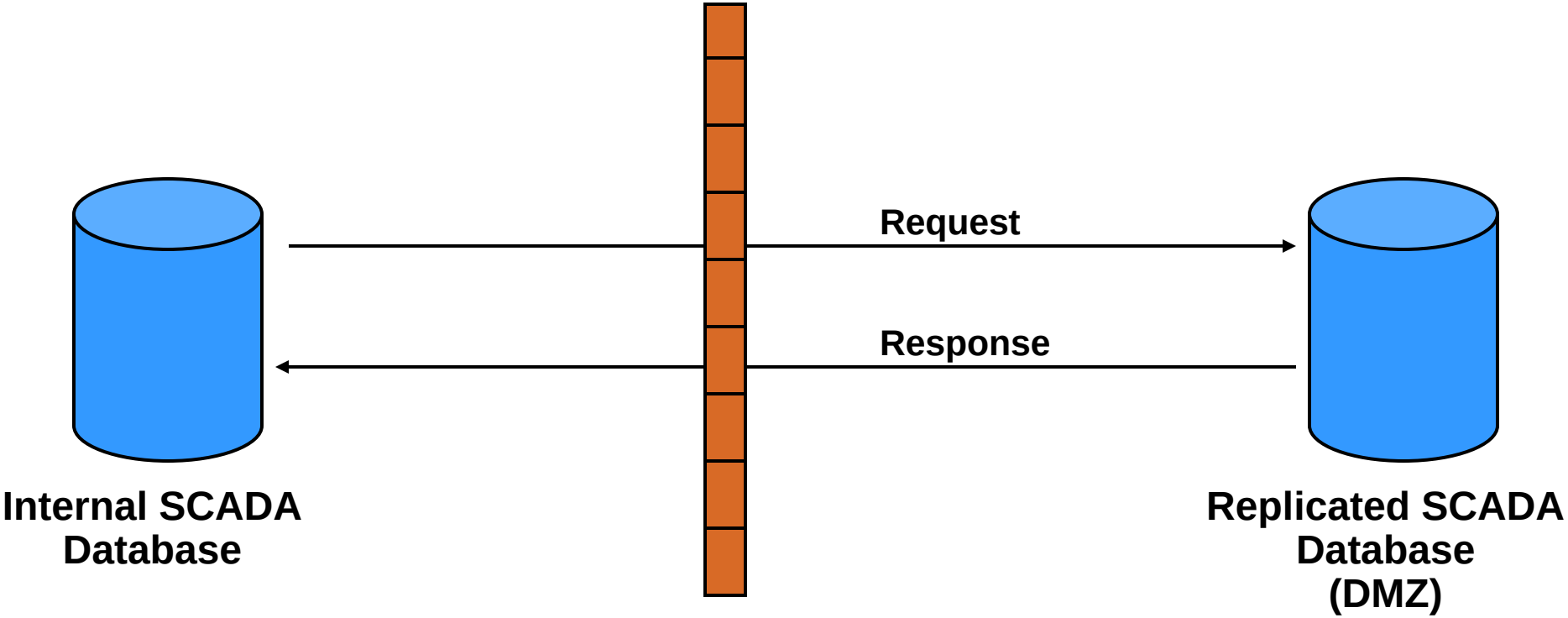
- TCP is a reliable, stateful communications protocol
- Three-way handshaking
- There are no one-way communications with TCP



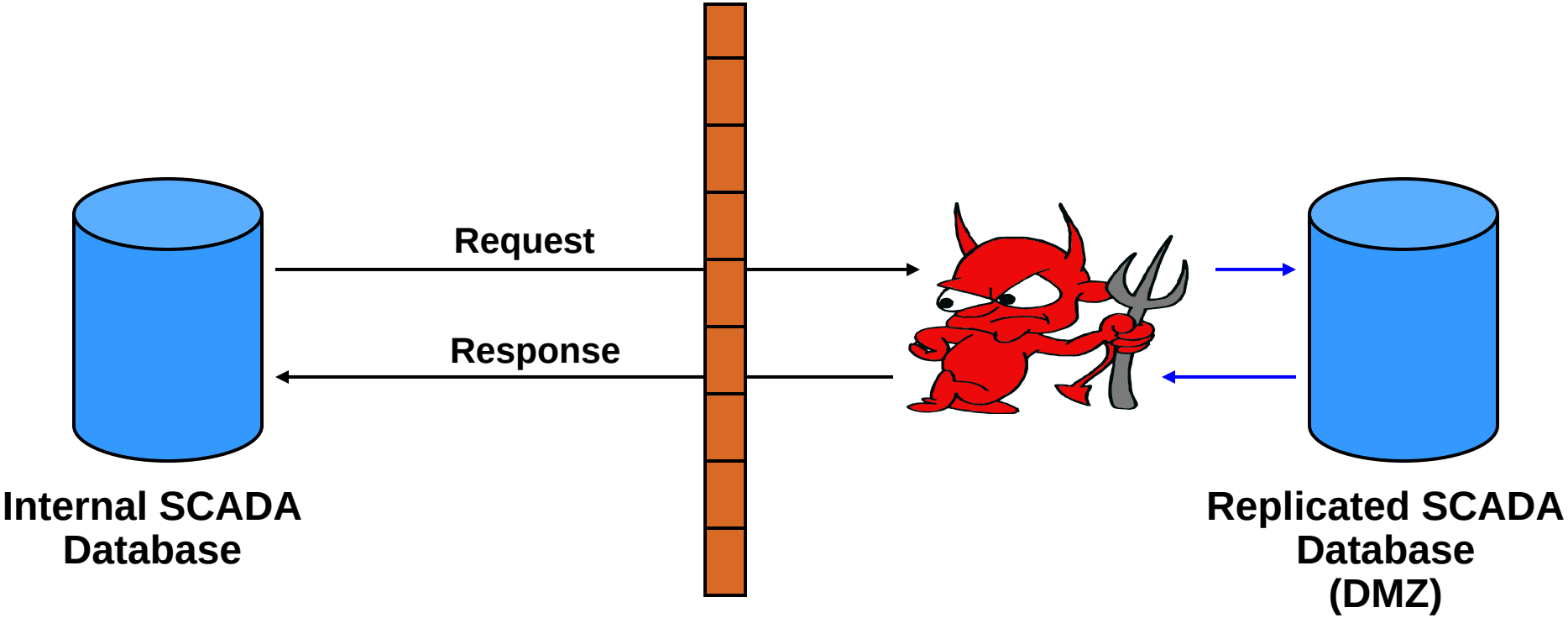
Data Base Attack

- Hijack corporate system
- Listen for conversation sending data to corporate data base
- Hijack the session
- Tell SCADA data base to 'Create Table'
- Insert Shell Kit in new table
- Ask Data base to write table to disk as a .so
- Tell Data base to execute stored procedure
- E.T. Call home

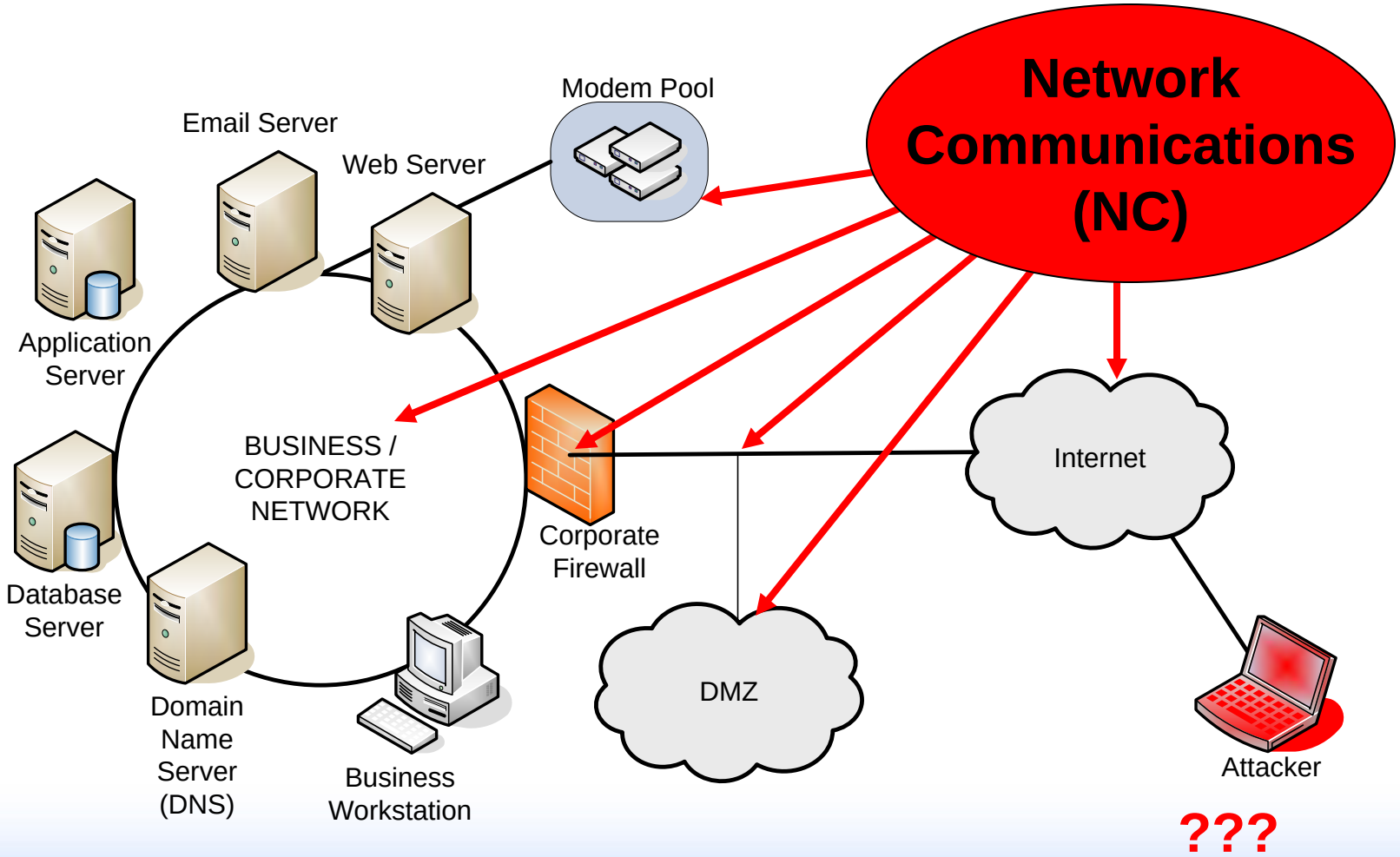
Database / Firewall Example



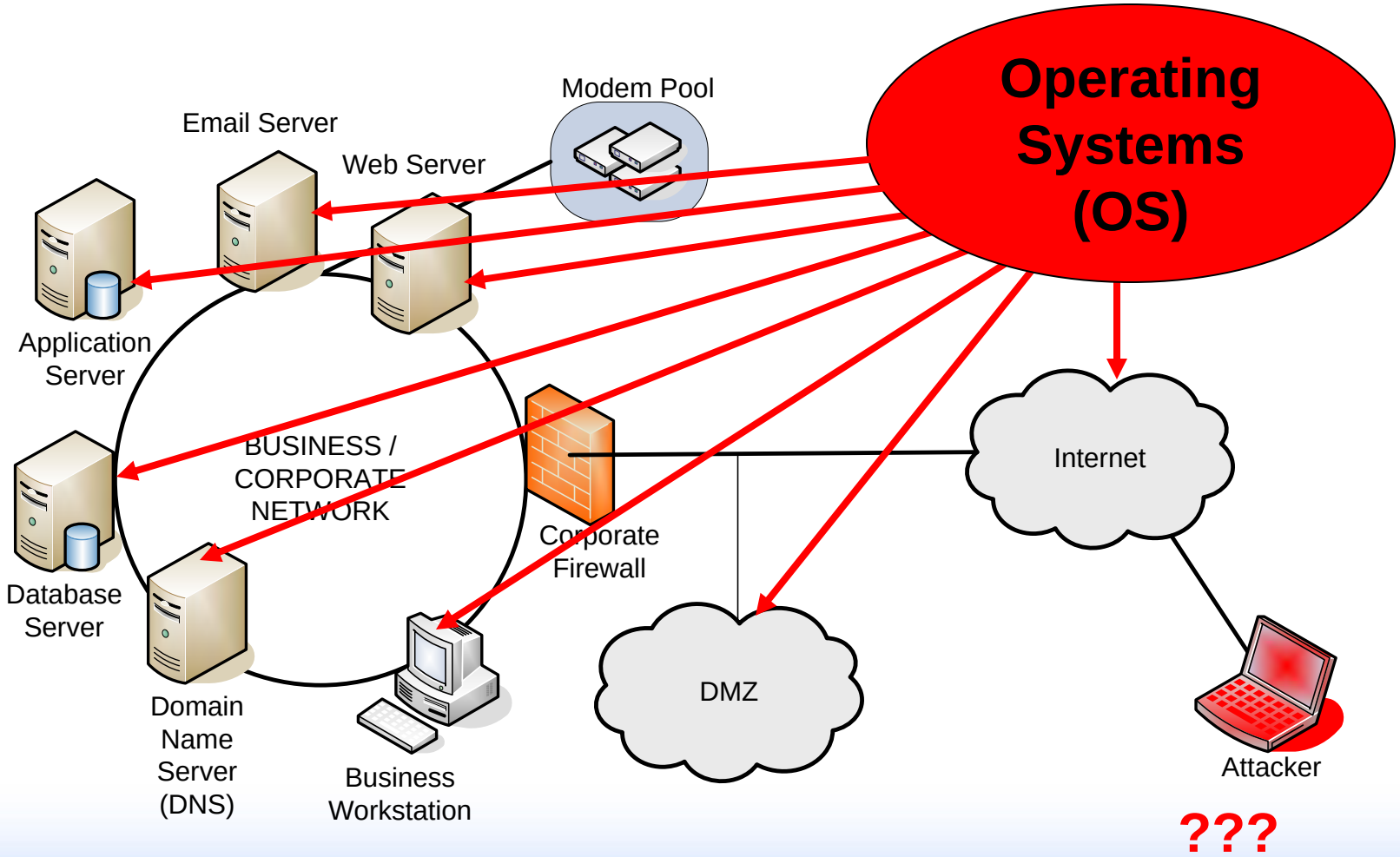
Database / Firewall Example



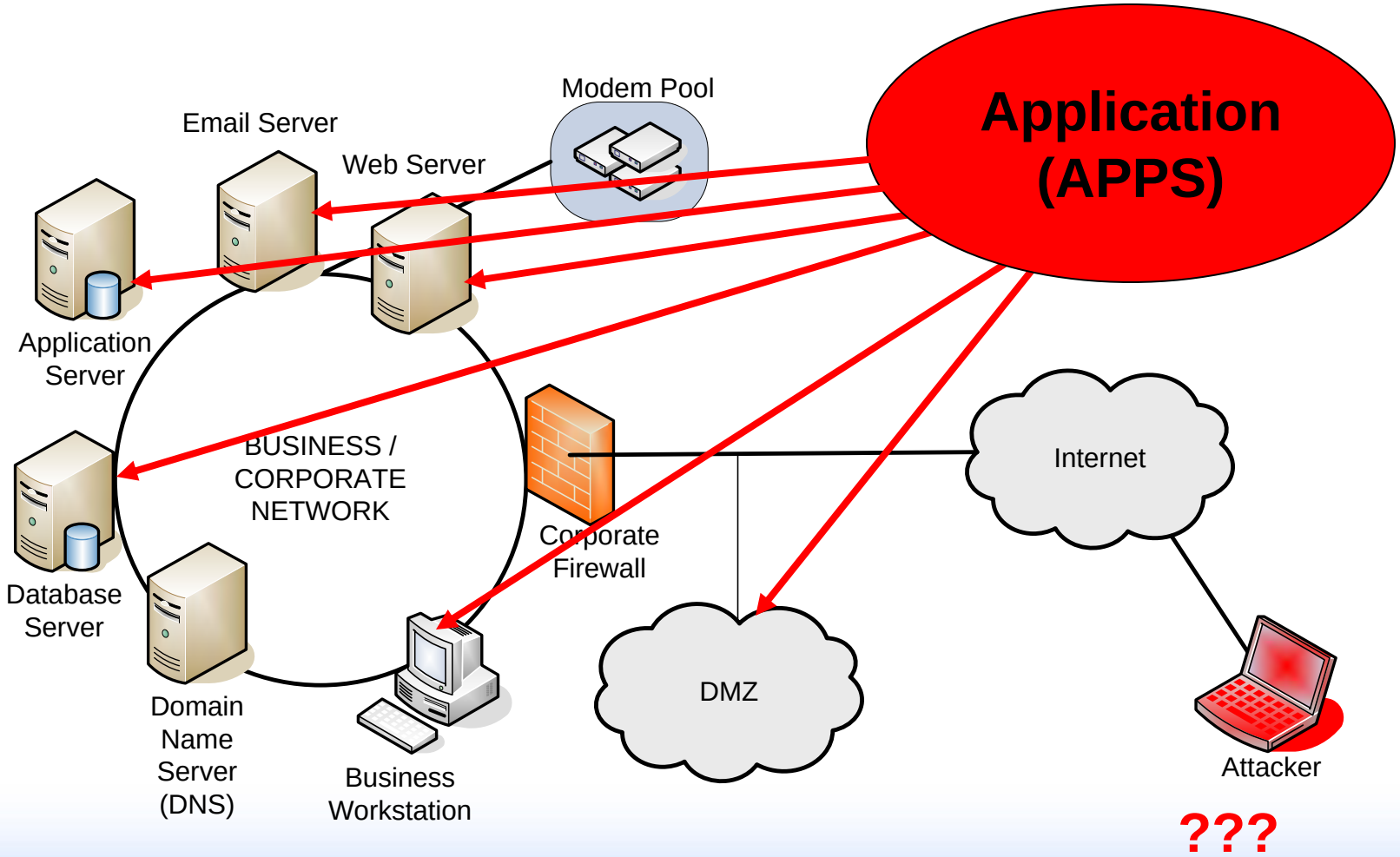
Vulnerability Groupings for COTS



Vulnerability Groupings for COTS

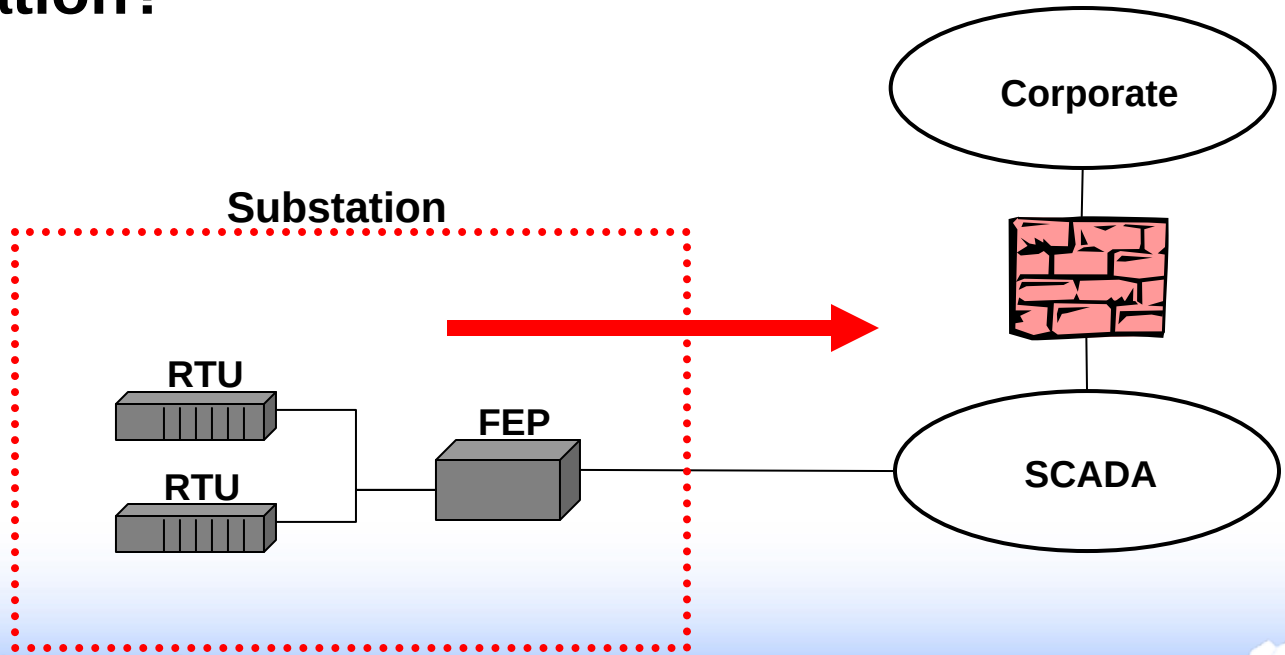


Vulnerability Groupings for COTS



Distributed Nature of SCADA

- Much more complex than typical business networks
- Disparate locations
- Can the SCADA be compromised from a remote location?



Many Back Doors

Bottom Line: There are many routes into systems as complex as a modern SCADA or control system.

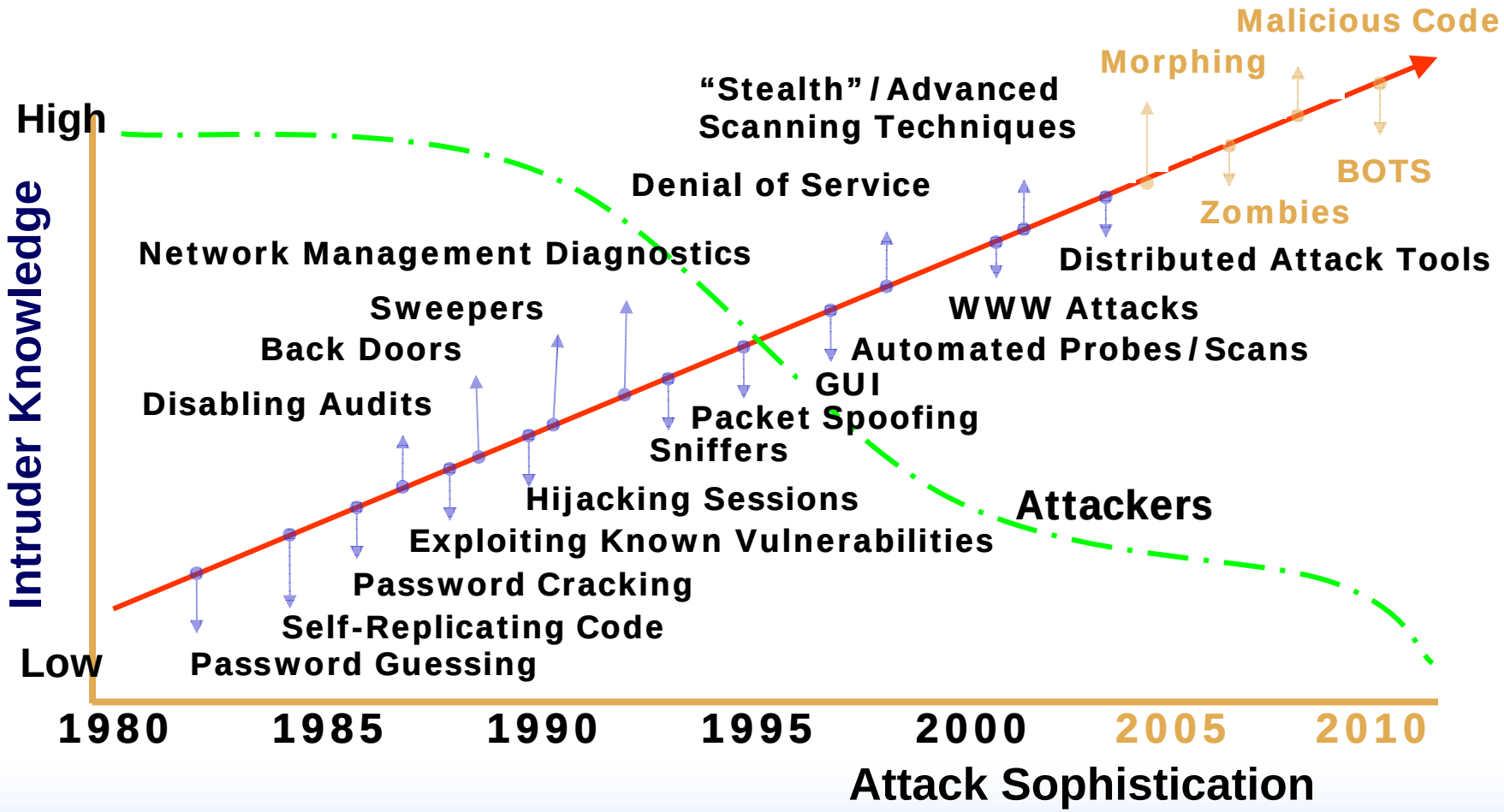
Types of Attackers

- **Script Kiddies – Low hanging fruit**
- **Insider – Disgruntled employee**
- **Terrorists – Shock and awe**
- **Nation States – Plenty of time and money**

Attackers may utilize each others resources…

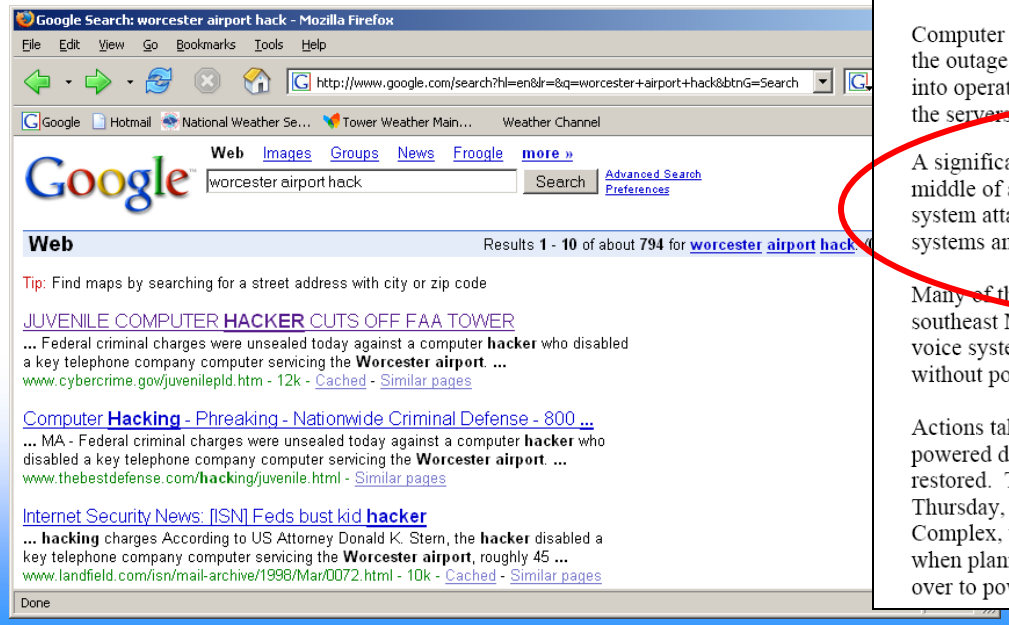
Threat Trends

- Threats More Complex as Attackers Proliferate



Effects of Cyber on Critical Infrastructure

- **Davis-Besse Nuclear Power**
- **Northeast Blackout**
- **Australian Sewage Release**
- **Siberian Pipeline**
- **Worcester Airport**



to avoid errors in software operations. When power is resumed, the servers then reboot, as normal, bringing operation systems back on line. In not all instances will this execute properly and some servers will require a technician to bring the system back on line. In some cases the age of equipment may have been a factor in returning the system to operations.

Computer operations, which run multiple servers, also require cooling in the server room. Since the outage occurred on a hot summer day, it was necessary to get air conditioning systems back into operation, allowing the server room to be cooled to normal operating temperatures before the servers could be returned to service if back up generation was not available.

A significant challenge faced by computer system operators was that the outage occurred in the middle of an effort against the "MSBLASTER" worm virus attack and the "SoBig" virus. The system attacks as a result of these two viruses had already caused some disruptions to computer systems and the power outage compounded the problems and the response.

Many of the State of Michigan's computer operations were affected. Most Lansing and southeast Michigan computer hardware encountered a hard shutdown, with the exception of most voice systems. The Department of Information Technology (DIT) Command Center was without power in the Hannah Building in downtown Lansing.

Actions taken by DIT included a quick response to assure most servers in data centers were powered down prior to exhaustion of UPS battery power to eliminate problems when power was restored. The DIT Emergency Management Coordinator went to SEOC at 7:15 p.m. on Thursday, August 14, and a DIT secondary command center was activated at the State Secondary Complex, which still had power. Additional fuel to power these generators was not available when planned due to the heavy demand on fuel suppliers, and these server operations were cut over to power from the grid at about the time fuel supplies for the generator were exhausted.

Typical Attack Steps

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

Target Identification / Selection

- How visible is your company in the public?
- Is your company/utility desirable?
- How do your defenses compare to your neighbor?

Reconnaissance

- Open Source Intelligence
  - External Web Site
  - Google (Internet) Searches
  - DNS Lookups
- Dumpster Diving
- Social Engineering
- War Dialing / War Driving
- Scanning
- Insider Threat

Reconnaissance Example

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

Project Profile

Pearl Harbor Naval Base

Power Monitoring SCADA System

The United States Navy's shipyard at Pearl Harbor, Hawaii, is one of the most recognized names and facilities in the world. Located on the state capital island of Oahu, Pearl Harbor is one of the largest and most active navy bases in the Pacific. Ships of various sizes, function and electrical need are constantly moving in and out of the facilities, needing external power connection to remain operational during port stays and refitting. Electric loads are constantly changing, requiring up to the minute status and availability information to facilities operations personnel.

Transdyn, acting as a prime contractor, was awarded a contract to upgrade, modernize, and replace the Navy's existing Power Distribution/Substation monitoring and control SCADA system. Transdyn's DYNAC™ System allows operations personnel to look into each of the thirteen major subsections, analyze, modify or control switchgear to numerous docks and facilities within its sphere of influence. Hawaiian Electric Company (HECO) supplies power to several distribution points. This system allows monitoring, control, and record keeping of the power provided by HECO.

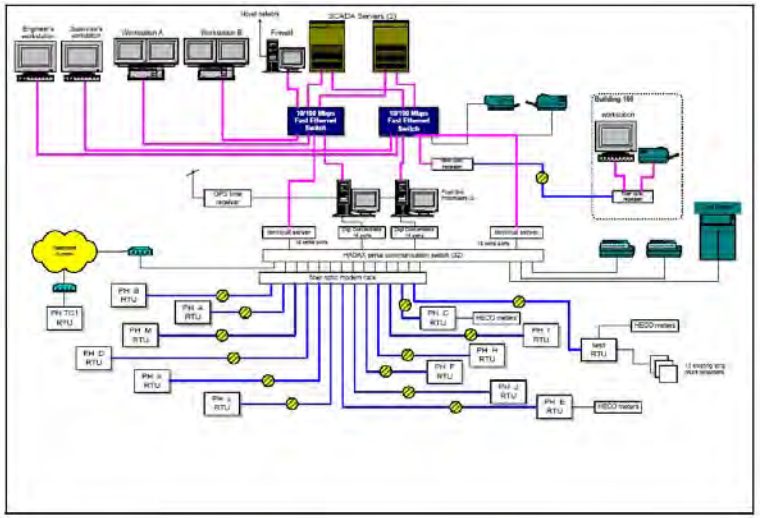
As these substations are geographically distributed over a large area, Transdyn was required to design a system with Remote Telemetry Units (RTUs) that could collect, and send data to the central DYNAC™ system, as well as receive commands and execute the required changes within the substation. This requires a fast, secure and ultra-reliable system configuration.

The DYNAC™ host software runs on a pair of redundant servers with completely redundant fast Ethernet LAN components. Fiber optic communications paths to the RTUs provide the Navy with a secure system for their current, as well as future needs. RTUs are located at 13 substations within the facility and communicate with the central computer using the DNP3 protocol.

Many special features are provided for this project to meet the unique requirements of the US Navy. Two Operator Consoles, with dual 21" CRTs, provide a graphical depiction of the status of the distribution system. In addition, three other remotely-located workstations are provided with full access to the system. A firewall computer provides a secure connection to the US Government's Inter-Service Novell LAN.

Transdyn provided turnkey installation of all new and replacement electrical components (i.e., relays, Flexitest switches and security devices), as well as all new conduit, wiring, and interconnects between switchgear and RTU, RTU-to-host, and host-to-peripherals.

Many unique features are provided for this project to meet the requirements of the US Navy.



- DYNAC™ Software
- Remote Telemetry Units (RTUs)
- Redundant Alpha SCADA Servers
- Ethernet LAN
- Fiber Optic Communications
- Sequence of Events Recording (millisecond resolution)
- Firewall Server
- DNP3 Protocol
- Operator Consoles With Dual 21" CRTs

System Exploits

- Viruses and Worms
- Email
- Hostile Web Pages
- Direct Attacks

Keeping Access

- Attacker may/may not care
- Account creation
- Password cracking
- Backdoors / Trojan Horses
- Rootkits

Covering the Tracks

- Physical damage
- Hiding files
- Log file modification / deletion
- Covert channels (loki, ncovert)

Network Components and Architecture

Security Policy

- Corner stone of your network security!
- Driven by technology!
- Enforceable
- Users need to know the whys!
- Reviewed annually or sooner

Layered Security Model

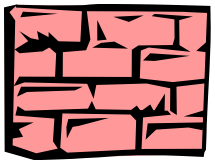
The Five Layer Model

Human

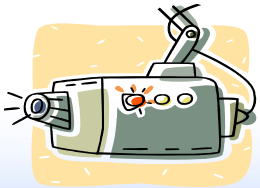
Application

OS

Network



Physical



Switches and Routers

- 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)

Notable Quotes

- **Marty Roesch, speaking at a SANS conference a couple of years ago "Those of you thinking that IDS is only about the sensor, are seeing about 5 percent of the picture!".**
- **Remember Kevin Mitnick? (quoted in 2000), "It's naïve to assume that just installing a firewall is going to protect you from all potential security threats."**
- **SANS Standard "Prevention is ideal, detection is essential."**

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
- Writing rules: best practices
- Data collection
- Monitoring firewalls: Logs, IDS, TESTING

IDS Functions

- Are your firewall(s) doing their job?
- Are your company policies are being followed?
- Are servers affected by malicious traffic?
- Are there mis-configured systems? (data leakage)

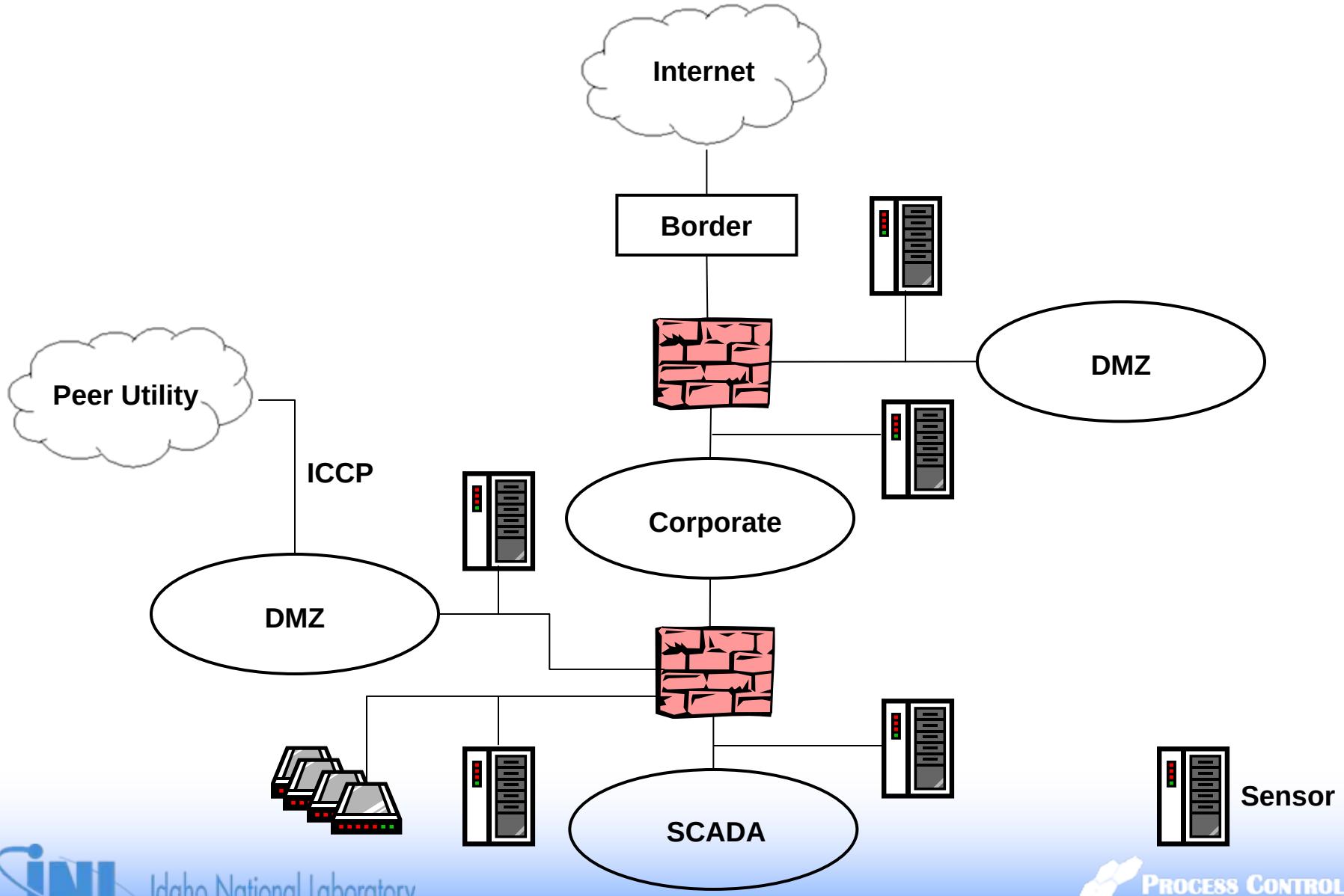
Basic IDS Catagories

- Network Intrusion Detection Systems (NIDS)
- Host-based Intrusion Detection Systems (HIDS)
- Intrusion Prevention Systems (IPS)
- Anti-Virus / *Bot scanners (AVS)

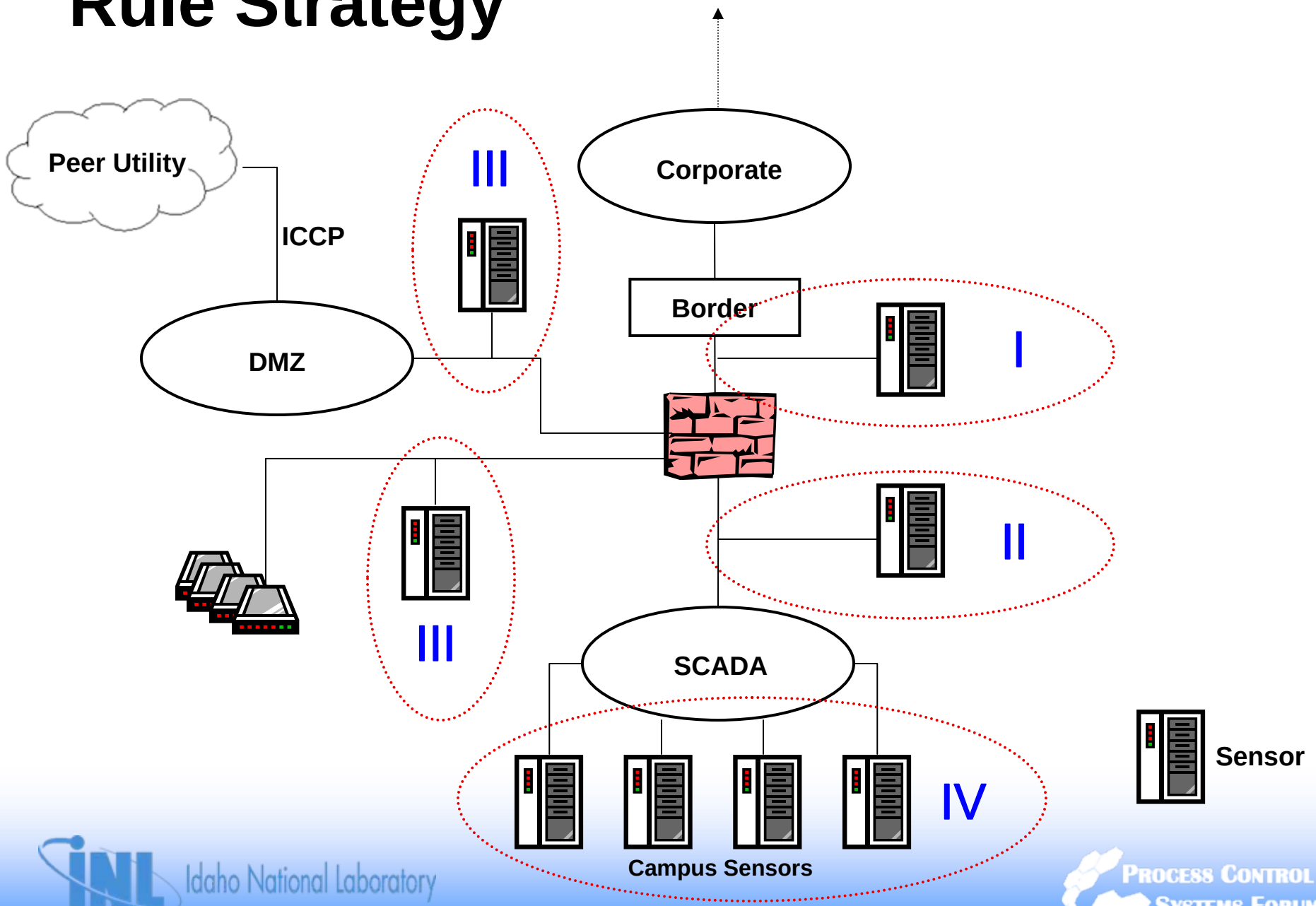
IDS Rules

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

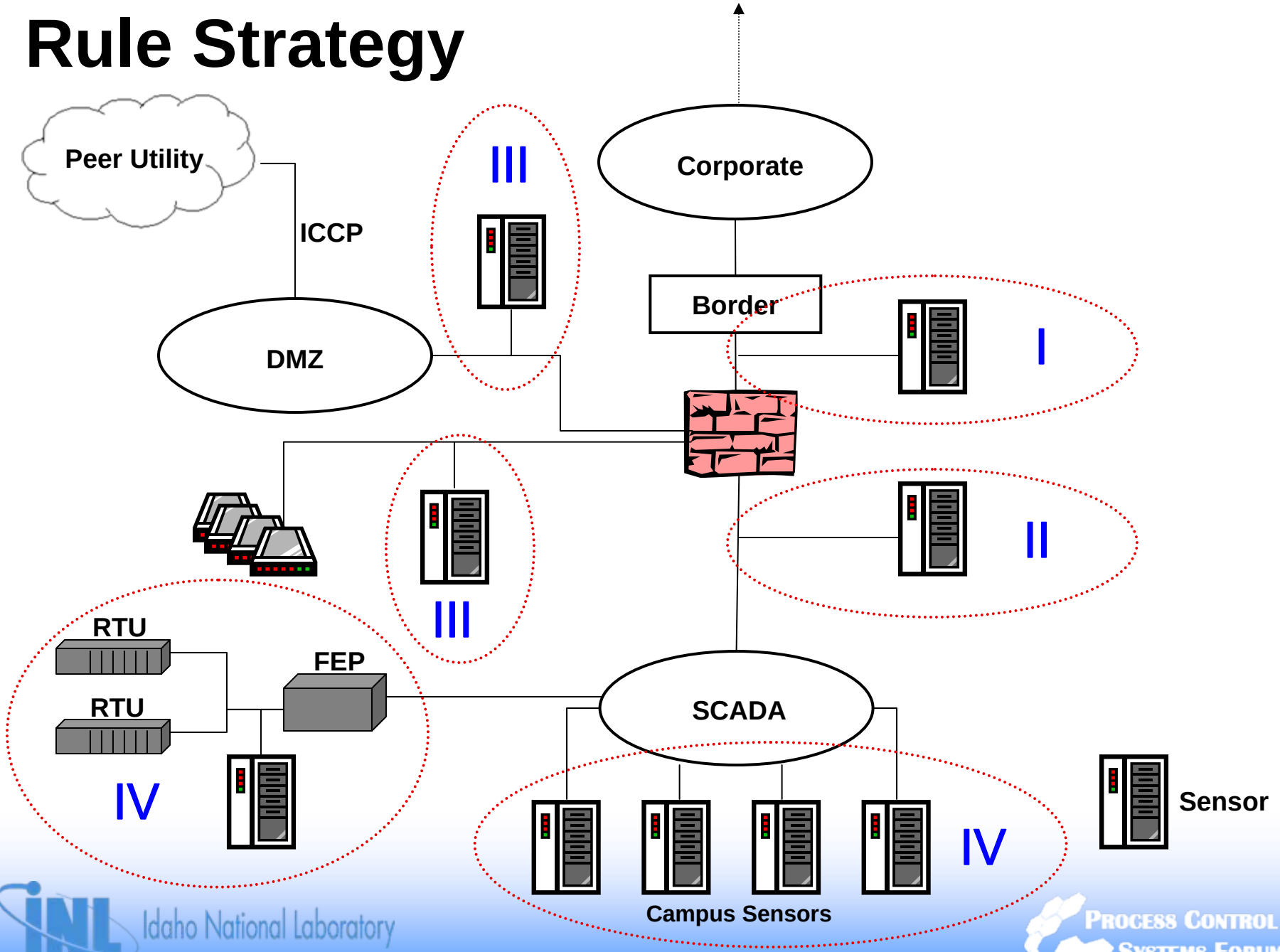
IDS Placement Overview



Rule Strategy



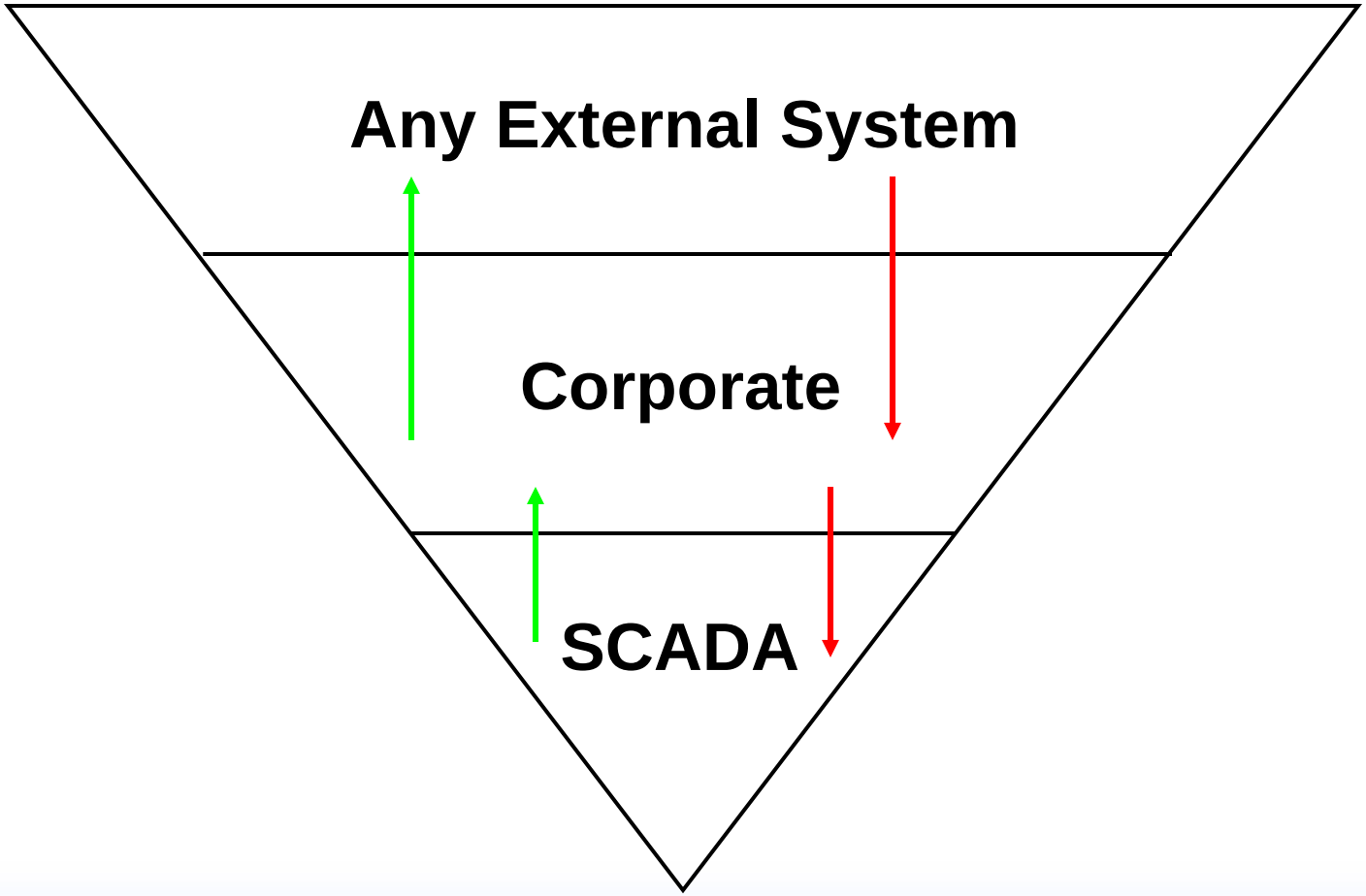
Rule Strategy



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

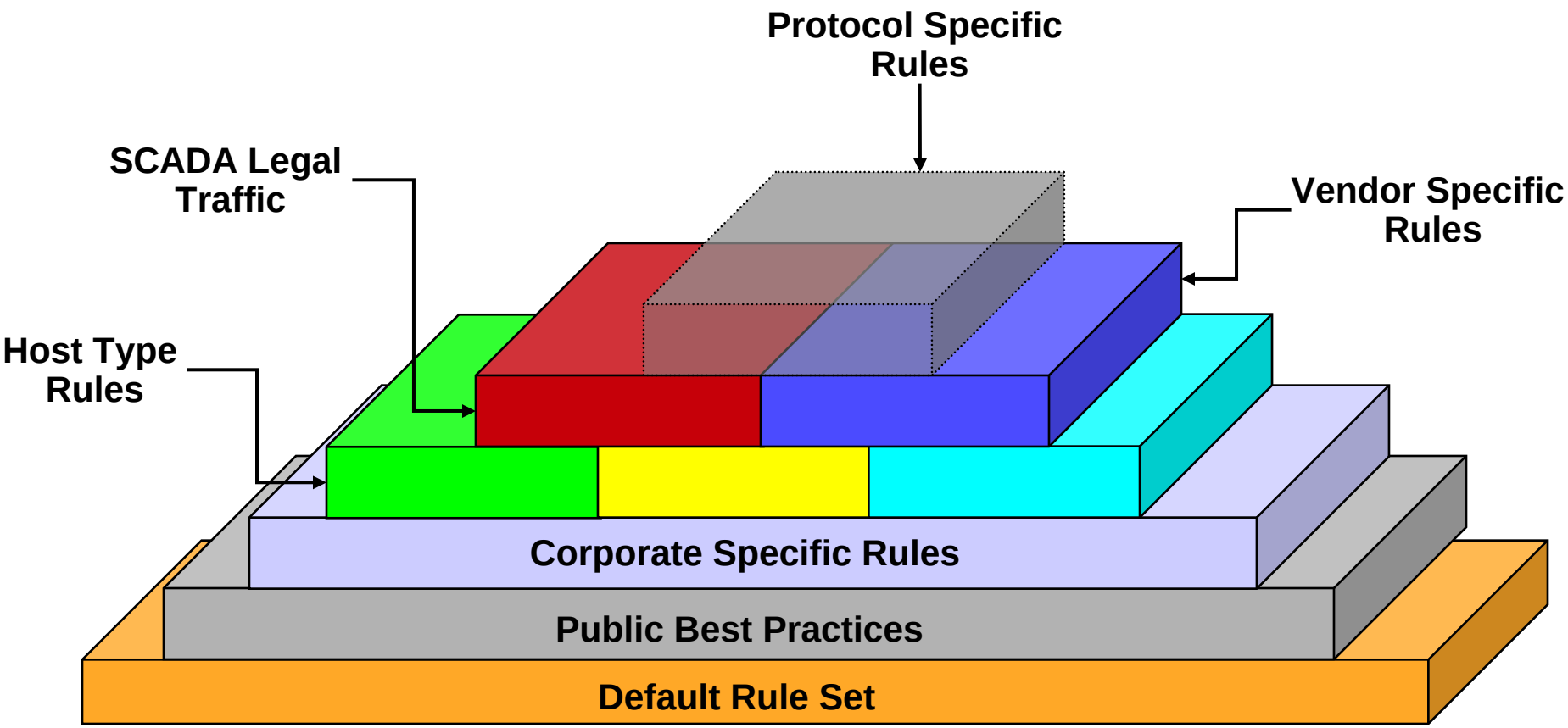
Rule Strategy



Rule Strategy

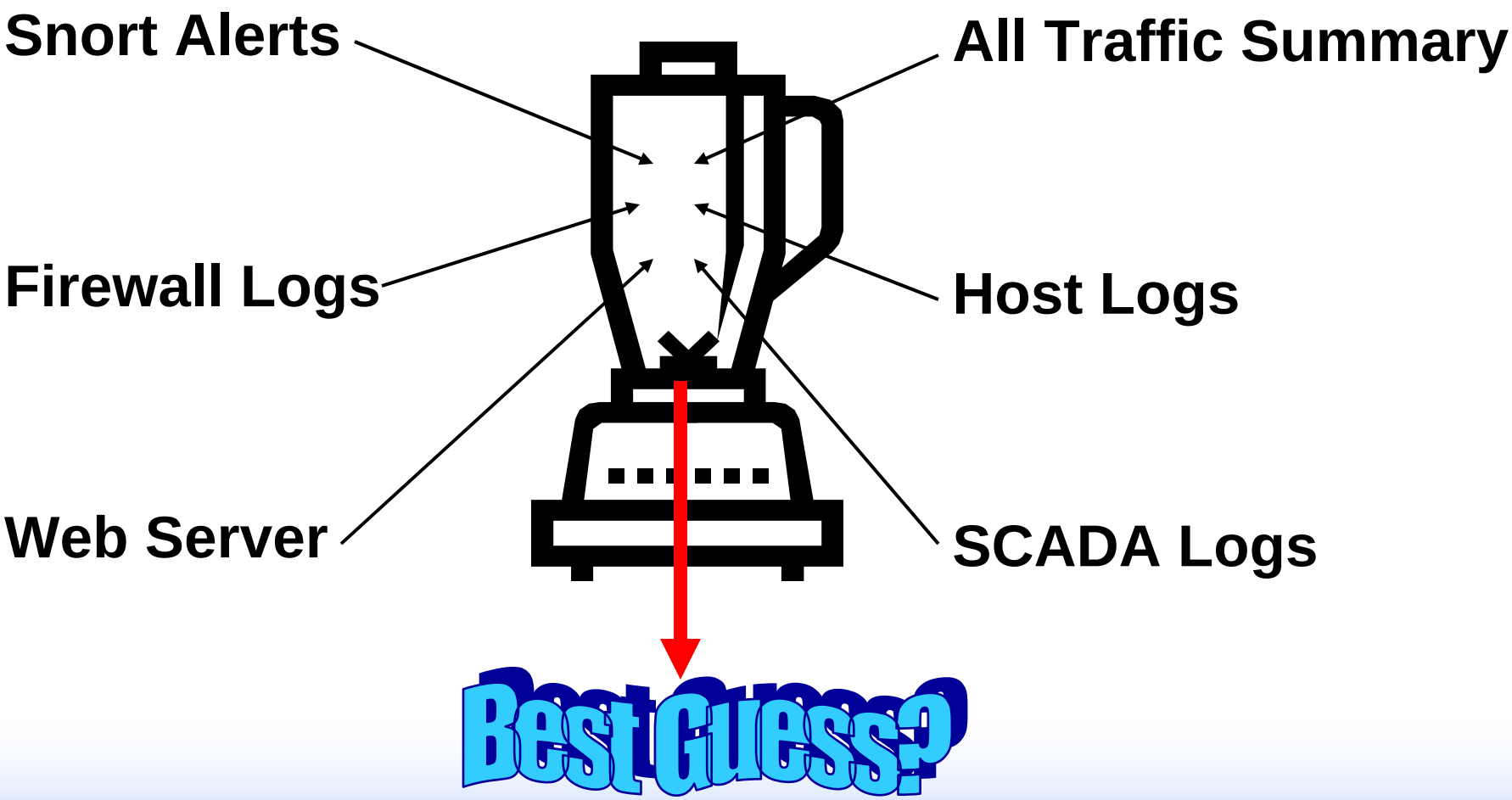
- Rules should follow the pattern currently implemented industry wide
- Legal traffic laws specific to control systems
- Must exploit vendor specific protocols before rules are effectively created
- SCADA specific rules are on and above typical IT rule set

Rule Strategy



SCADA Rule Set Should Build Upon Existing Rules

Disjoint Data Sources



Tools Available

- Firewall, routers, and switches
  - Monitor network flow
- Host Based Intrusion Detection Systems (HIDS)
  - Monitoring host activity
- Log Managers (Syslog, Event Log, etc.)
  - Gathering additional information
- Network Intrusion Detection Systems (NIDS)
  - Network traffic monitoring
- Intrusion Prevention Systems (IPS)
  - Abort attacks in process
- Antivirus Scanners (AVS)
  - Scan and inoculate files
- Passive Vulnerability Scanners
  - Watch and learn from network traffic
- Host Based Firewalls
  - Controlling network traffic to/from host

Vulnerability Testing

Vulnerability Testing – NERC 1300

1306-a-5 **Identification of Vulnerabilities and Responses**

"At a minimum, a vulnerability assessment shall be performed at least annually that includes a diagnostic review (controlled penetration testing) of the access points to the electronic security perimeter, scanning for open ports/services and modems, factory default accounts, and security patch and anti-virus version levels. The responsible entity will implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment."

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.***

The good news / bad news

- Several testing tools available
- Use more than one
- Same tools used by the hackers
- Same tools used by the insiders
- Same tools used by security consultant

Vulnerability Testing Warning

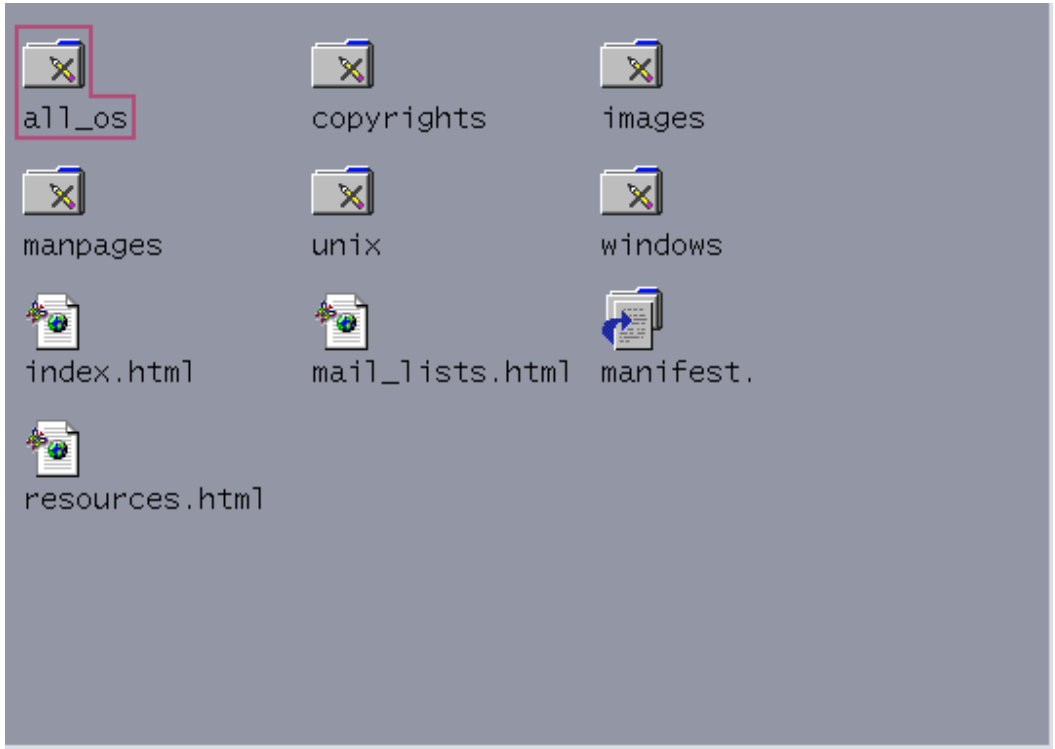
- Only test vulnerabilities they know
- May need more than one tool for complete test
- Only good for that moment in time

Tools and Resources

Tools and Resources Available

- **Open Source tools on CD-rom**
- **Training**
- **Mail lists**

CD Structure



Cyber Security Advisories

- Xforce http://xforce.iss.net
- Insecure.org http://ww.insecure.org
- FIRST http://first.org
- SANS http://www.sans.org
- Incident Storm Center http://isc.sans.org
- US-cert http://www.us-cert.gov

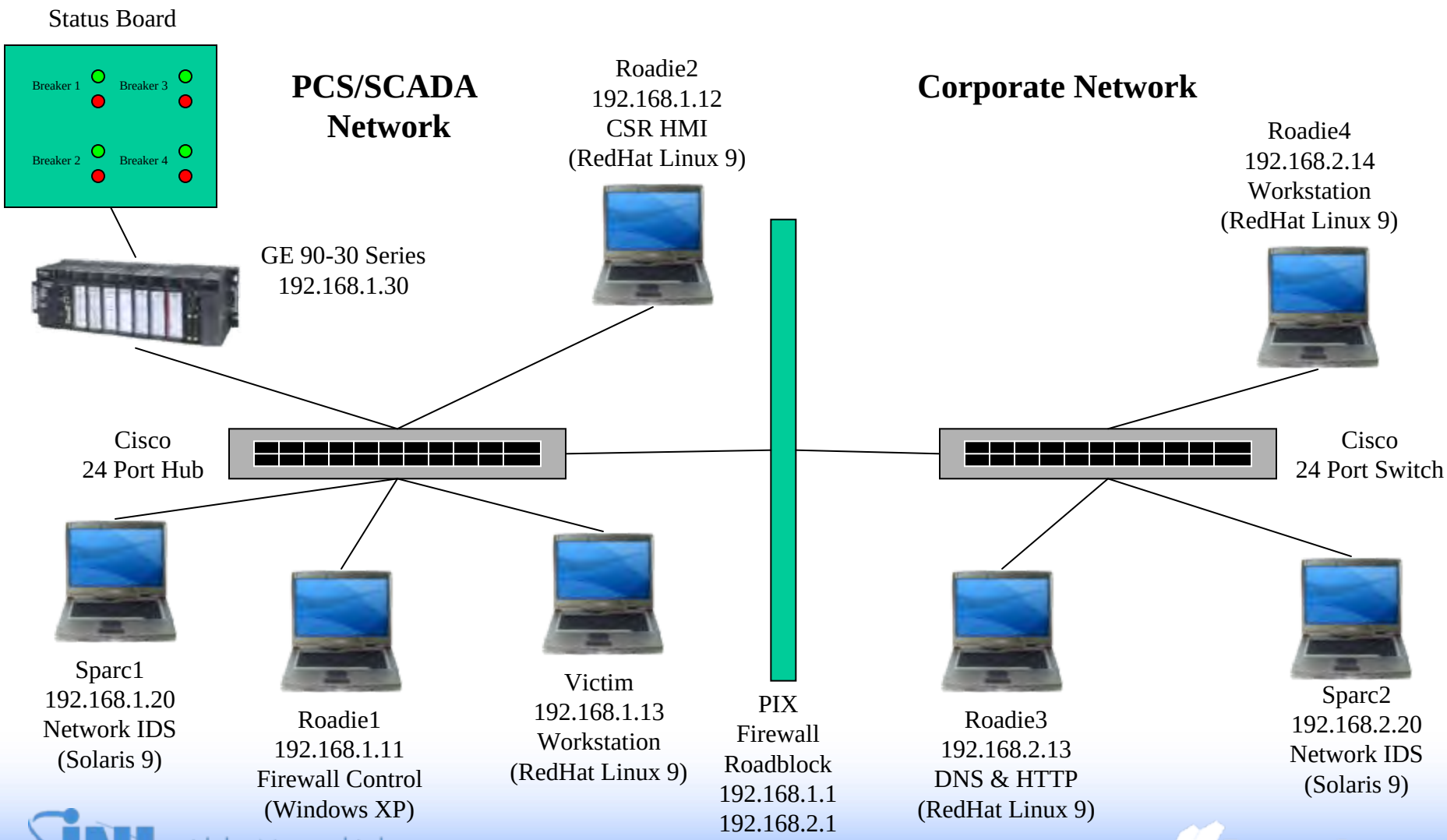
Training – A MUST!!!

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

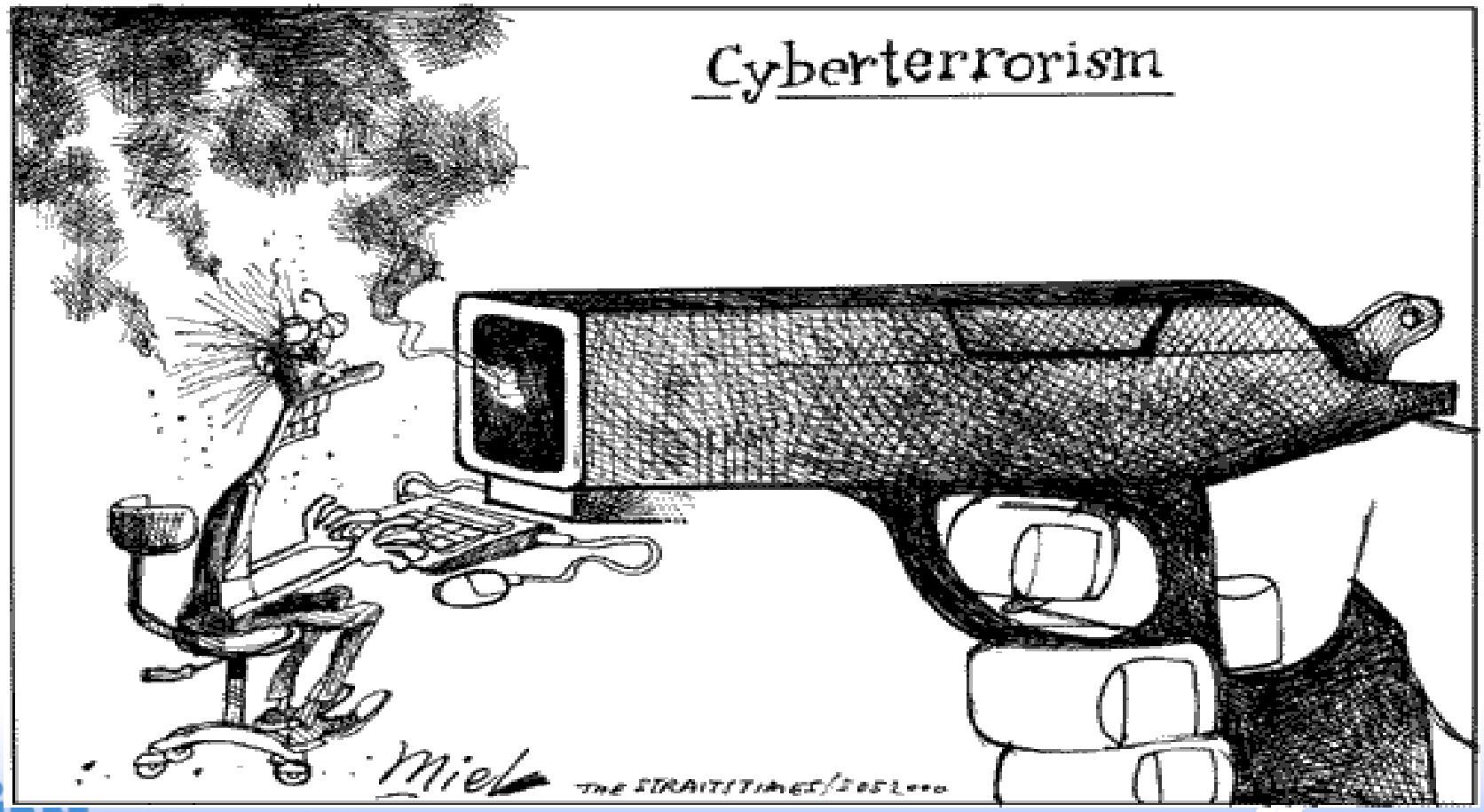
Break Time

Hands-On

Mobile Network Details



The Status of Things



Scenario #1 – Network Scan

- An attacker has gained control of a computer on the corporate network. Using that computer, the attacker scans the corporate network using Nmap.
- The Nmap scan reveals nodes within the address range specified by the attacker. A properly configured scan will result in the discovery of an internal firewall separating the corporate network from the SCADA/PCS network.
- A scan of the PCS/SCADA network was allowed because of the firewall configuration.

Scenario #2 – Using Ethereal and TCPDump

- Nmap may not always detect all hosts on the network. Using tools like Ethereal and TCPDump, the attacker can capture all traffic on the network and may reveal additional IP addressed than what Nmap was able to find.
- The corporate network is on a switch. Ethereal and TCPDump only provide information on traffic that comes across the wire to the host computer.
- The SCADA/PCS network in this demonstration is connected by a hub. Hubs broadcast traffic to all nodes. The end result is that Ethereal will not see much on the corporate network but will see everything on the SCADA/PCS network

Scenario #3 – Vulnerability Scan

- The attacker continues the reconnaissance by launching a vulnerability scan using Nessus. This scan reveals some additional information regarding the hosts that Nmap found. Nessus provides vulnerability information relative to the types of services running on a host.
- Nessus also provides a greater level of detail than Nmap by guessing what services are running on the open ports of a host. This is a very effective tool for watching the network for allowed services.

Scenario #4 – Firewall Configuration

- **Scenarios 1-3 were possible partly due to poor firewall configuration. Review the rules in place on the firewall and modify to still allow required functionality but limit the ability for attacks to take place.**

Scenario #5 – IDS Configuration

- **Basic steps in setting up and configuring Snort. Adding some basic rules to Snort to match the rules in place on the firewall.**

EXTRA CREDIT –Detailed Explanation of the “Blinky-Light” Demonstration

- **Provide a detailed hands-on explanation of how this attack was carried out. Explain the DNS spoofing that was used to direct an internal host to a hostile web server. Discuss how this is a common mis-configuration regarding internal/external DNS and the firewall.**

Supplemental Slides

Pieces and Parts

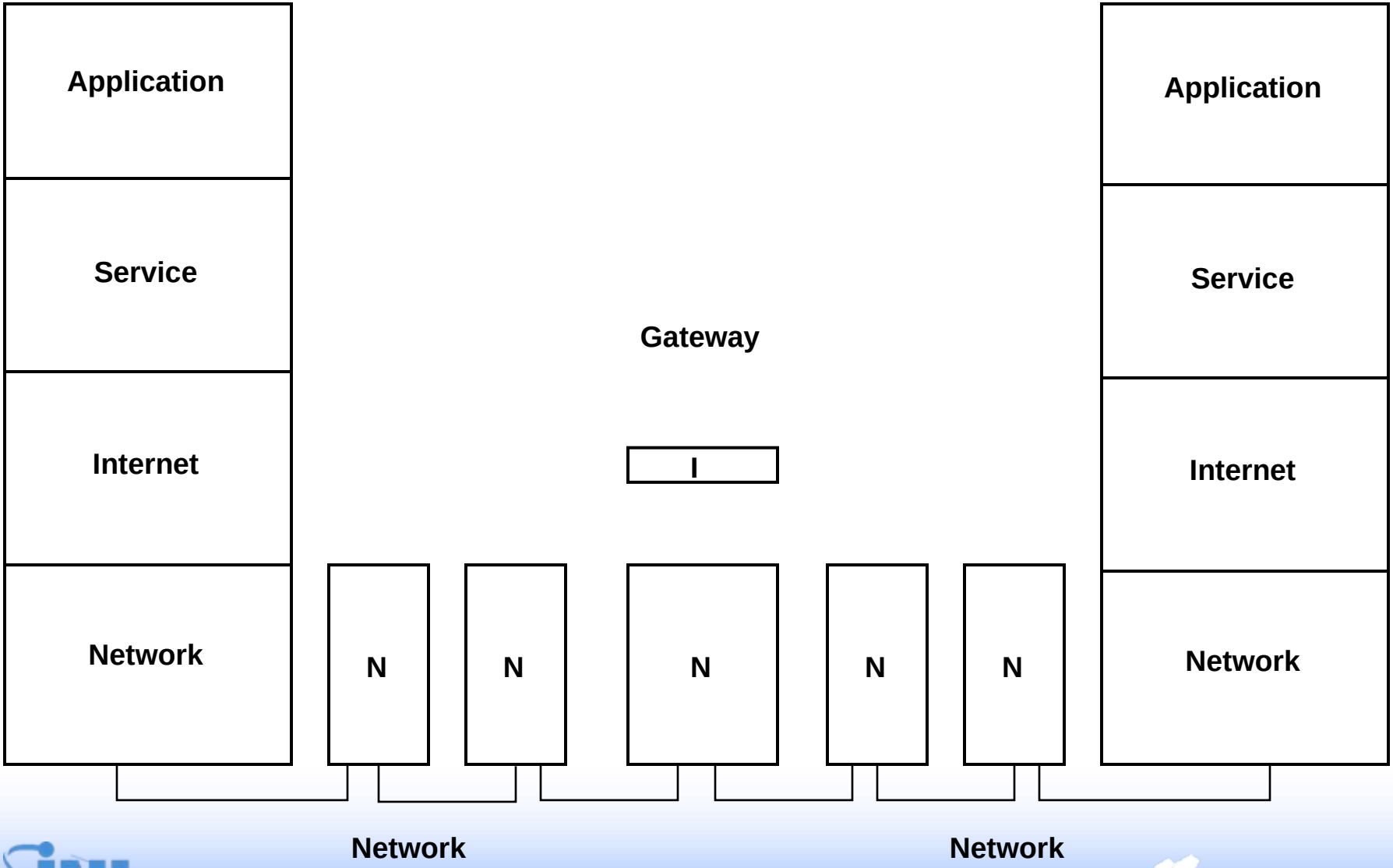
- Network Layers
- Protocols
- IP Addresses
- Ports
- Routers
- Switches
- DNS

Network Layers

The OSI and the ARPA Layered Architecture

OSI	APRA	
Application	Process / Application Layer	← Handling
Presentation		
Session		
Transport	Host-to-Host Layer	← Error Checking
Network	Internet Layer	← Routing
Data Link	Network Interface or Local Network Layer	← Delivery
Physical		
(Theoretical)	(Practical)	

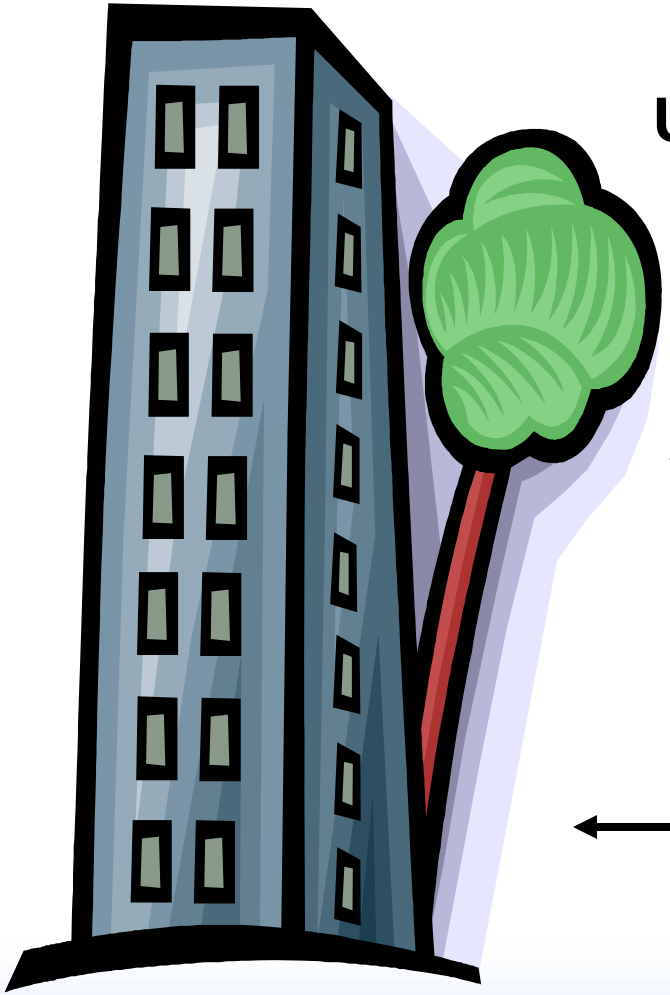
A Packet in Time



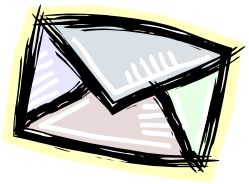
Protocols

Process/ Application	Hypertext Transfer	File Transfer	Electronic Mail	Terminal Emulation	Domain Names	File Transfer	Client/ Server	Network Management	Application
	Hypertext Transfer Protocol (HTTP) RFC 2068	File Transfer Protocol MIL-STD-1781 RFC 959	Simple Mail Transfer Protocol (SMTP) MIL-STD-1781 RFC 2821	TELNET Protocol MIL-STD-1782 RFC 854	Domain Name System (DNS) RFC 1034, 1035	Trivial File Transfer Protocol (TFTP) RFC 783	Sun Microsystems Network File System Protocol (NFS) RFCs 1014,1057, and 1094	Simple Network Management Protocol (SNMP) V1: RFC 1157 V2: RFC 1901-10 V3: RFC 2571-75	
Host-to-Host	Transmission Control Protocol (TCP) MI-STD-1788 RFC 793					User Datagram Protocol (UDP) RFC 768			Presentation Session
Internet	Address Resolution ARP RFC 826 RARP RFC 903	Internet Protocol (IP) MIL-STD-1777 RFC 791				Internet Control Message Protocol (ICMP) RFC 792			Transport Network
Network Interface	Network Interface Cards: Ethernet, Token Ring, ARCNET, MAN and WAN RFC 894, RFC 1042, RFC 1201 and others								Data Link
	Transmission Media: Twisted Pair, Coax, Fiber Optics, Wireless Media, etc.								Physical

IP Addresses



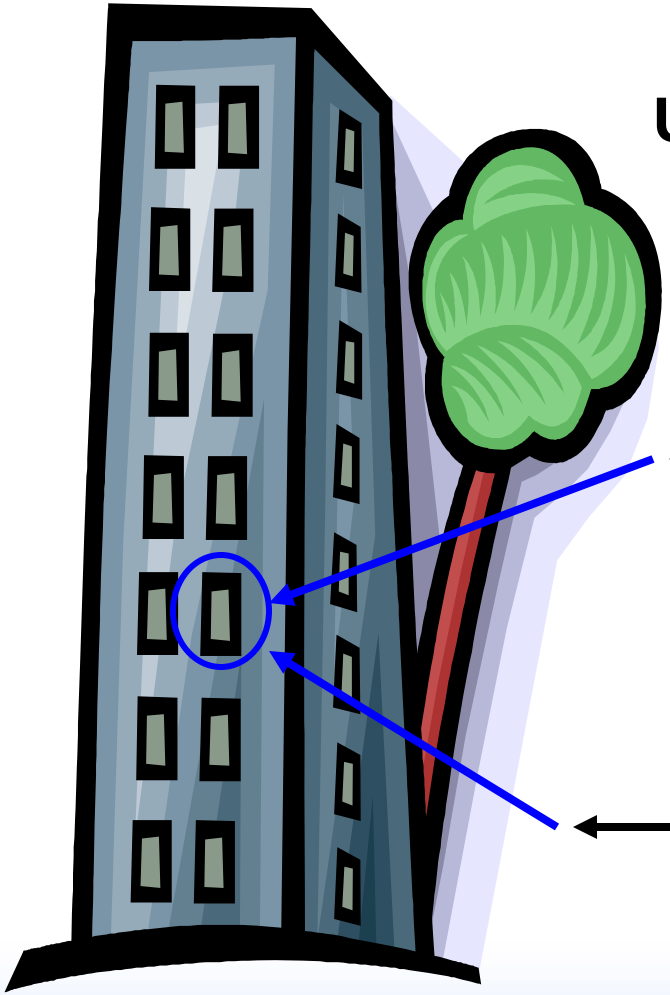
Unique Identification of a Location



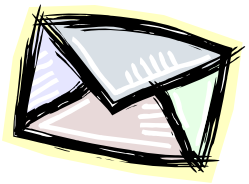
IP Addresses

- Loop Back 127.0.0.1
- Broadcast 255.255.255.255
- Default Network 0.0.0.0
- Class A – 1-126.X.X.X
  - (Very Large Networks, International Companies)
- Class B – 128-191.X.X.X
  - (Medium Sized Networks)
- Class C – 192-223.X.X.X
  - (Small to Mid-size Businesses)

IP Ports

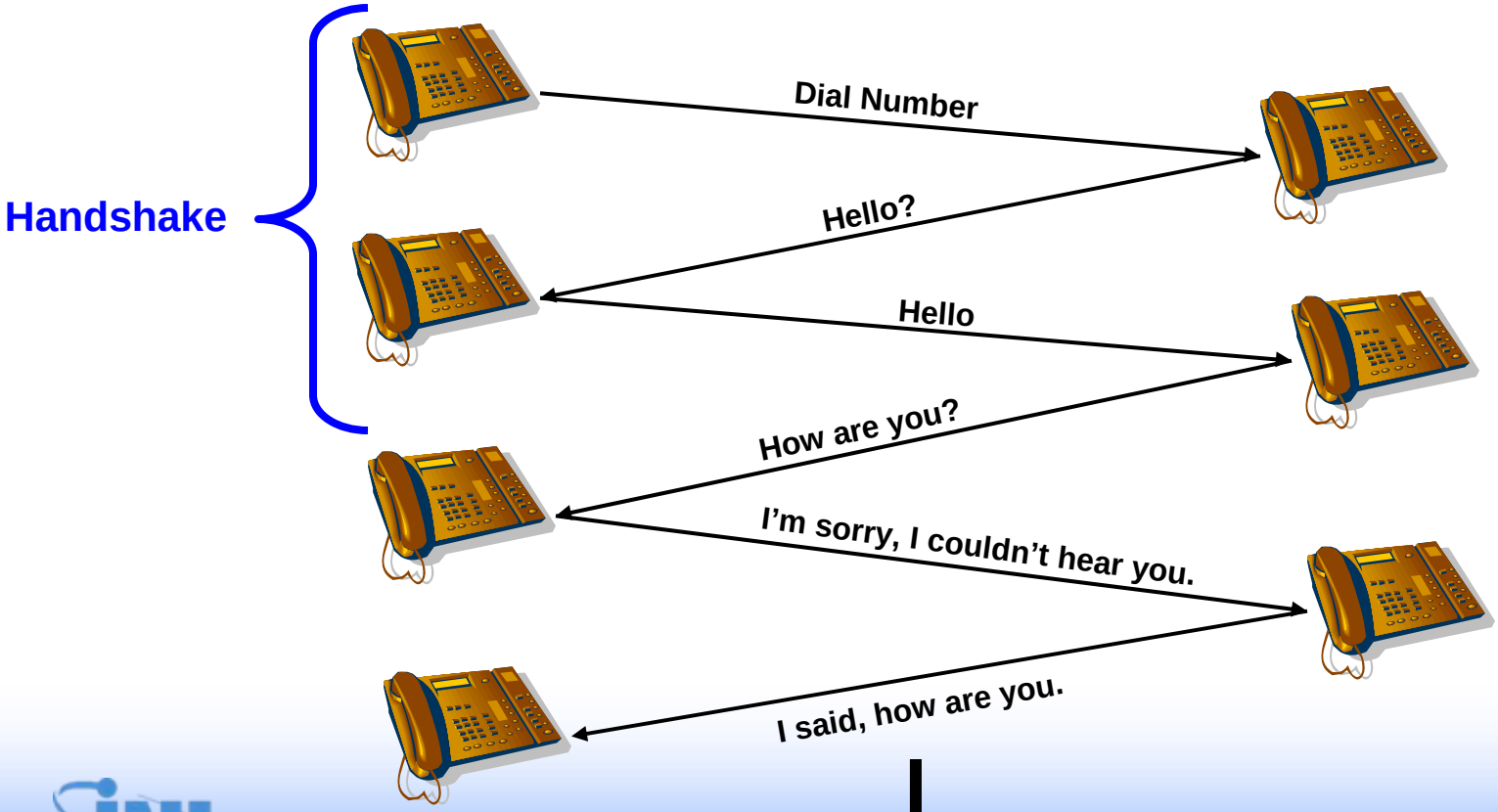


Unique Identification of a Location
and Recipient



Communication Basics

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



Routers

- Layer III Device – is IP address “aware”
- Direct Traffic – where does the request go?
- Transmitting packets
- Protocol Translation
- Physical Address vs. Logical Address

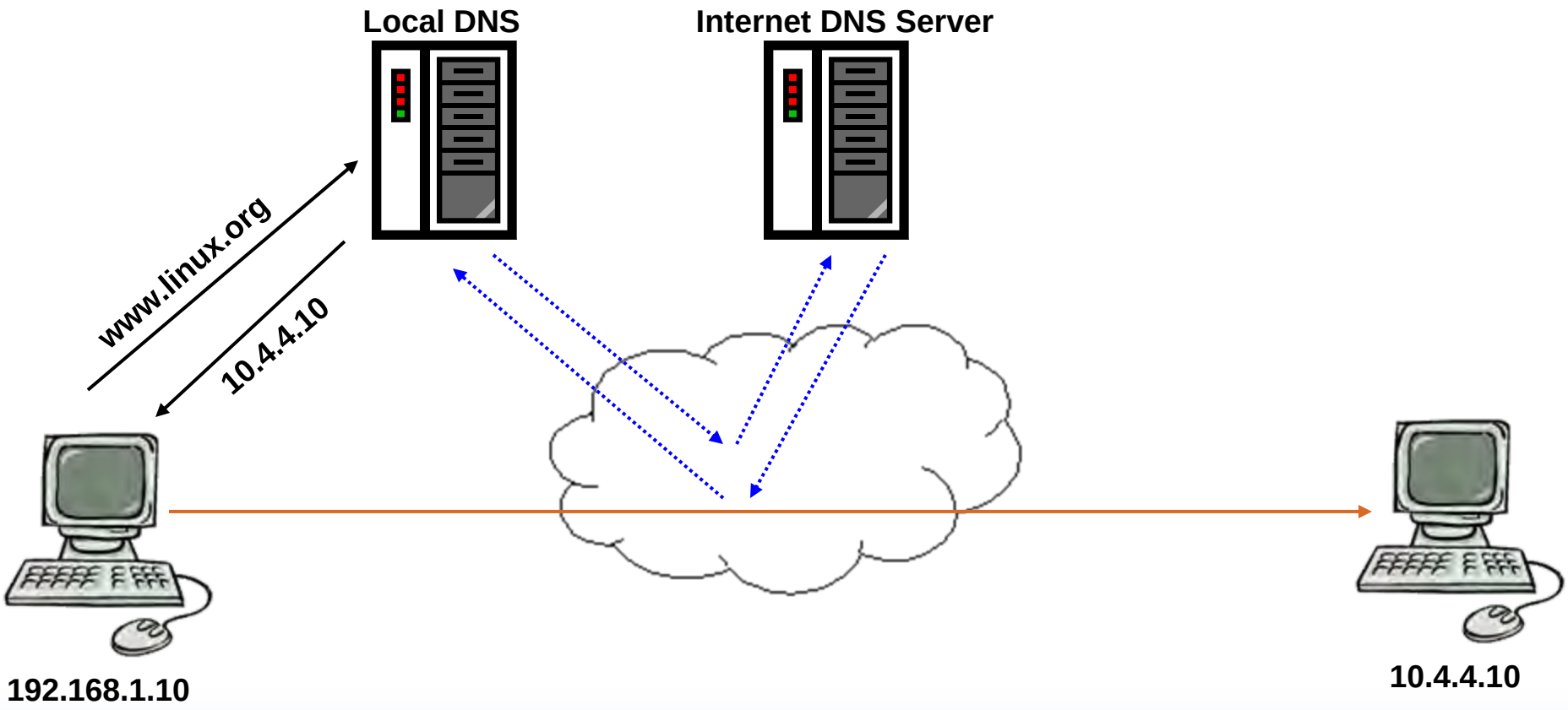
Switches

- Layer II Devices
- Are only aware of Physical Address
- Maps Physical Address to IP Address using ARP Tables
- Traffic is only sent to the intended recipient

Hubs

- Layer II devices
- Have no mapping of IP to MAC
- All traffic is broadcast to all connected hosts

Domain Name Service



Resources

- **SANS.org IPv4 Pocket Guide**
  http://www.sans.org/resources/tcpip.pdf

- **SANS.org IPv4 Pocket Guide**
  http://sans.org/resources/ipv5_tcpip_pocketguide.pdf

- **Securitywizardry.com Packet Diagrams**
  http://www.securitywizardry.com/protpackets.htm

IP Header

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP Version (4 bits)				[illegible]				Type of Service / Differential Service & ECN (8 bits)								[illegible]															
0								1								2								3							
Identification (Fragment ID) (16 bits)																R	DF	MF	Fragment Offset (13 bits)												
4								5								6								7							
Time-To-Live (TTL) (8 bits)								Protocol (8 bits)								Header Checksum (16 bits)															
8								9								10								11							
Source IP Address (32 bits)																															
12								13								14								15							
Destination IP Address (32 bits)																															
16								17								18								19							
Options (If any, variable length, padded with 0 s, 40 bytes max length)																															
20								21								22								23							
Data																															
24								25								26								27							

Format of the Type of Service Field:

Bits 0-2: Precendence
- 111 = Normal Control
- 110 = Internetwork Control
- 101 = CRITIC/ECP
- 100 = Flash Override
- 011 = Flash
- 010 = Immediate
- 001 = Priority
- 000 = Routine

Bit 3: Delay
- 0 = normal delay
- 1 = low delay

Bit 4: Throughput
- 0 = normal throughput
- 1 = high throughput

Bit 5: Reliability
- 0 = normal reliability
- 1 = high reliability

Bit 6-7: Reserved

Flags:

R: Bit 0 is reserved and must be zero

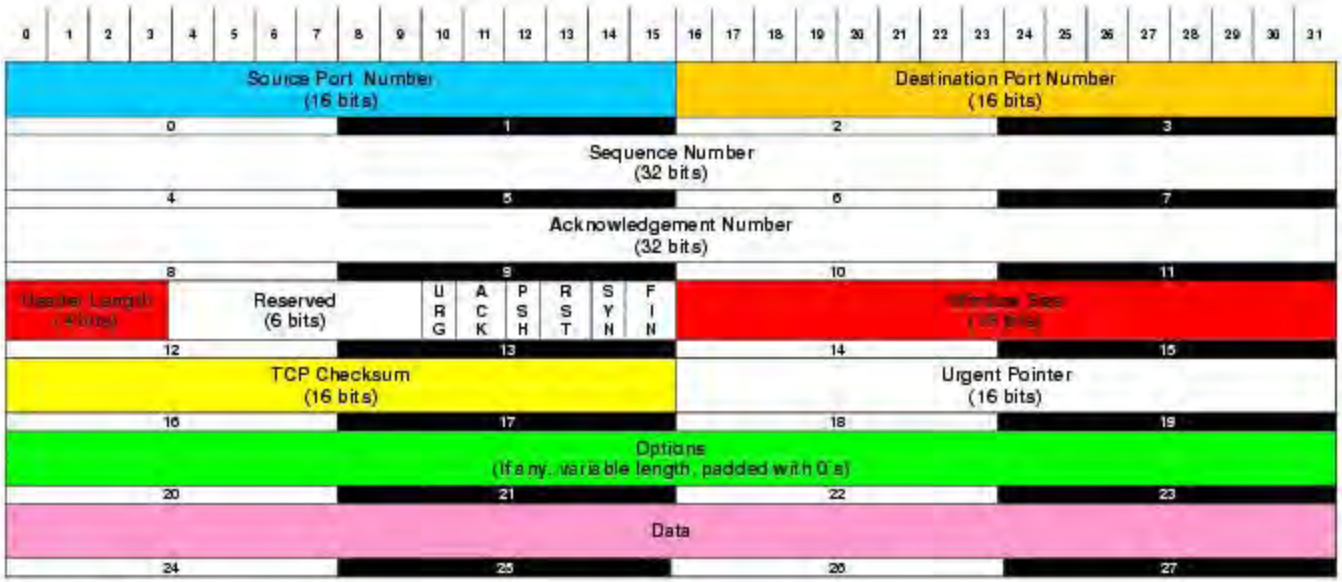
DF: Bit 1: Don't fragment bit:
- 0 May fragment
- 1 Don't fragment

MF: Bit 2: More fragments bit:
- 0 Last fragment
- 1 More fragments

Type of Service Field

0	1	2	3	4	5	6	7
Precedence			Delay	Through put	Reliability	Reserved	

TCP Header



Example TCP Applications

- TELNET
- FTP
- SMTP
- HTTP

UDP Header

Common UDP Well-Known Server Ports

Port	Description
7	Echo
19	Chargen
37	Time
53	Domain
67	Bootps (DHCP)
68	Bootpc (DHCP)
69	Tftp
137	Netbios-ns

Port	Description
138	Netbios-dgm
161	Snmp
162	Snmp-trap
500	Isakmp
514	Syslog
520	Rip
33434	Traceroute

Length
The number of bytes in the entire datagram, including the header: minimum value = 8

Checksum
Covers pseudo-header and entire UDP datagram

ICMP Message Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								Checksum															
0								1								2								3							
Content Dependant on Type and Code																															
4								5								6								7							

Type	Code	Meaning
8	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Information Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

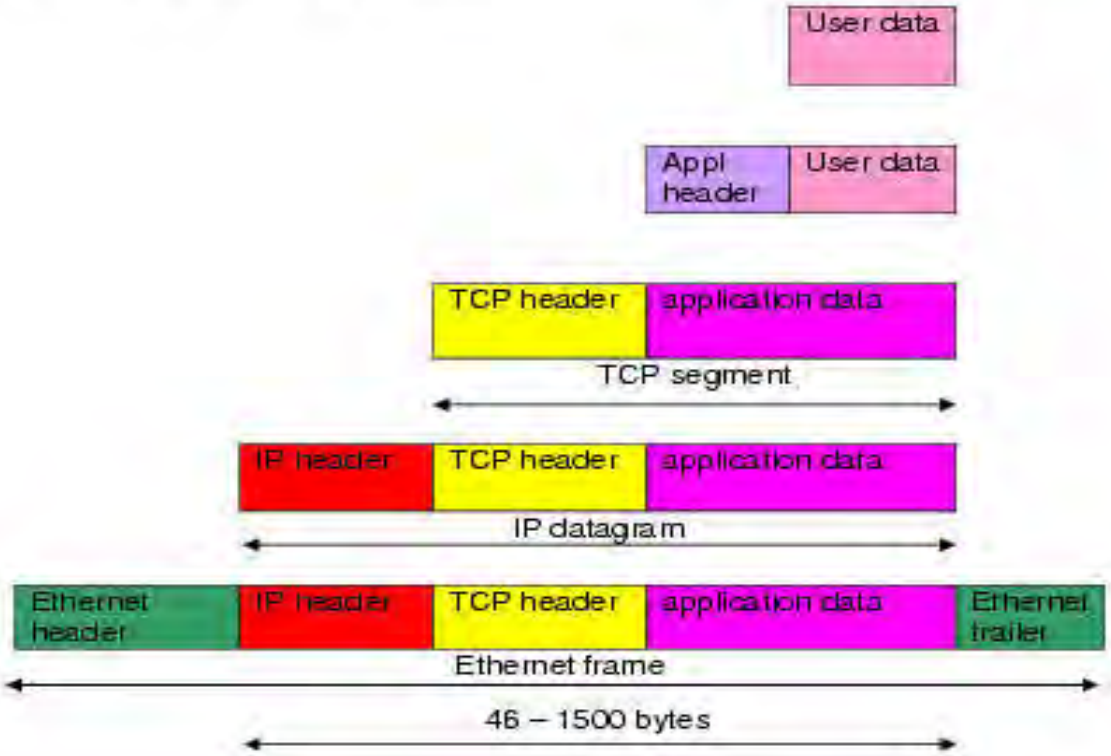
ICMP Parameter Message Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								Checksum															
0								1								2								3							
Pointer								Unused																							
4								5								6								7							
Internet Header + 8 bytes of Original Data Datagram																															
8																															

Type	Code	Meaning
8	0	Echo Reqs
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Informaiton Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

Encapsulation of data



ARP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Hardware Address Type																Protocol Address Type															
0								1								2								3							
Hardware Address Length								Protocol Address Length								Operation															
4								5								6								7							
Source Hardware Address																															
8								9								10								11							
Source Hardware Address cont.																Source Protocol Address															
12								13								14								15							
Source Protocol Address cont.																Target Hardware Address															
16								17								18								19							
Target Hardware Address cont.																															
20								21								22								23							
Target Protocol Address																															
24								25								26								27							

ARP Parameters for Ethernet and IPv4

Hardware Address Type		
	1	Ethernet
	6	IEEE 802 LAN
Protocol Address Type		
	2048	IPv4 (0x0800)
Hardware Address Length		
	6	for Ethernet / IEEE 802

Protocol Address Length		
	4	For IPv4
Operation		
	1	Request
	2	Reply

DNS

DNS Parameters

Query / Response

0	Query
1	Response

Opcode

0	Standard Query (QUERY)
1	Inverse Query (IQUERY)
2	Server Status Request (STATUS)

AA	1 = Authoritative Answer
TC	1 = TrunCation
RD	1 = Recursion Desired
RA	1 = Recursion Available
Z	Reserved; set to 0 (The DNS Evil bit)

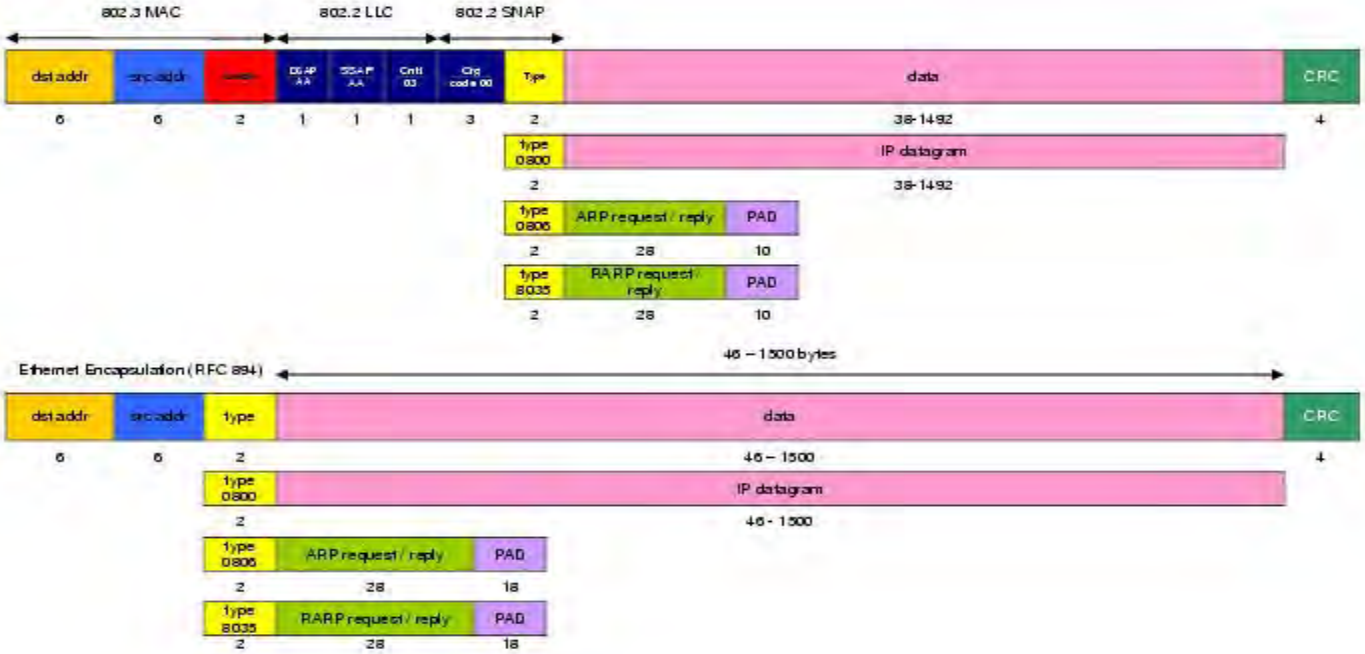
Response Code

0	No error
1	Format error
2	Server failure
3	Non-existent domain (NXDOMAIN)
4	Query type not implemented
5	Query refused

QDCOUNT	No. of entries in the Question Section
ANCOUNT	No. of resource records in Answer Section
NSCOUNT	No. of name server resource records in Authority Section
ARCOUNT	No. of resource records in Additional Information Section.

Link Layer Headers

IEEE 802.2 / 802.3 Encapsulation (RFC 1042)



IPv6 Header

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				Traffic Class								Flow Label (20 bits)																			
0								1								2								3							
Payload Length																Next Header								Hop Limit							
4								5								6								7							
Source Address (128 bits)																															
8								9								10								11							
Source Address																															
12								13								14								15							
Source Address																															
16								17								18								19							
Source Address																															
20								21								22								23							
Destination Address (128 bits)																															
24								25								26								27							
Destination Address																															
28								29								30								31							
Destination Address																															
32								33								34								35							
Destination Address																															
36								37								38								39							

Note: the standard IPv6 is 40 bytes long as opposed to 20 bytes for a v4 header (without options) also the v6 header is a lot simpler than is older brother and thus easier to understand. There are however, IPv6 extension headers that fit between the IPv6 header and next header, these include routing headers and fragment headers.

IPv6 Extension Headers

(RFC2460 IPv6 Spec)

An IPv6 packet can carry as many extension headers as it needs (Obviously within reason)
Example are below:-

IPv6 Header Next Header = TCP	TCP Header + data

IPv6 Header Next Header = Routing	Routing Header Next Header = TCP	TCP Header + data

IPv6 Header Next Header = Routing	Routing Header Next Header = Fragment	Fragment Header Next Header = TCP	TCP Header + data

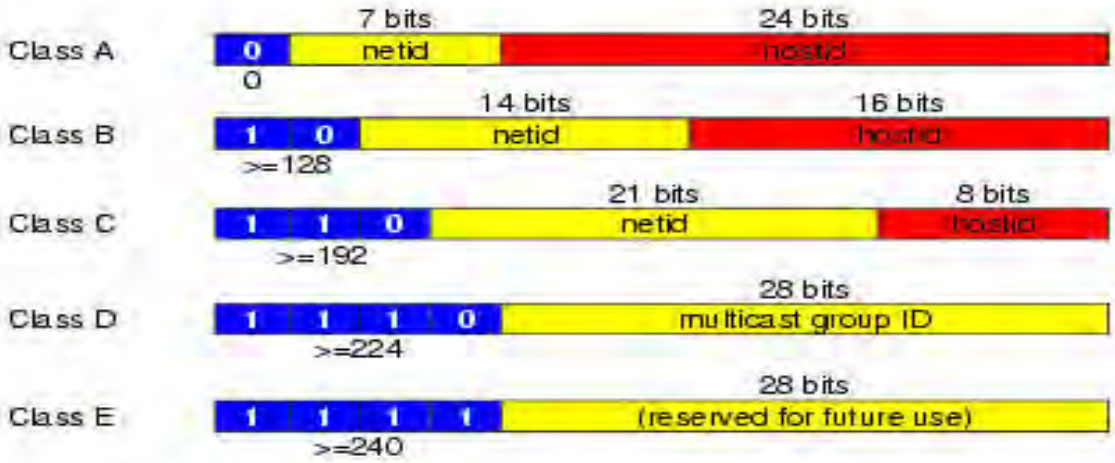
Extension Header Order

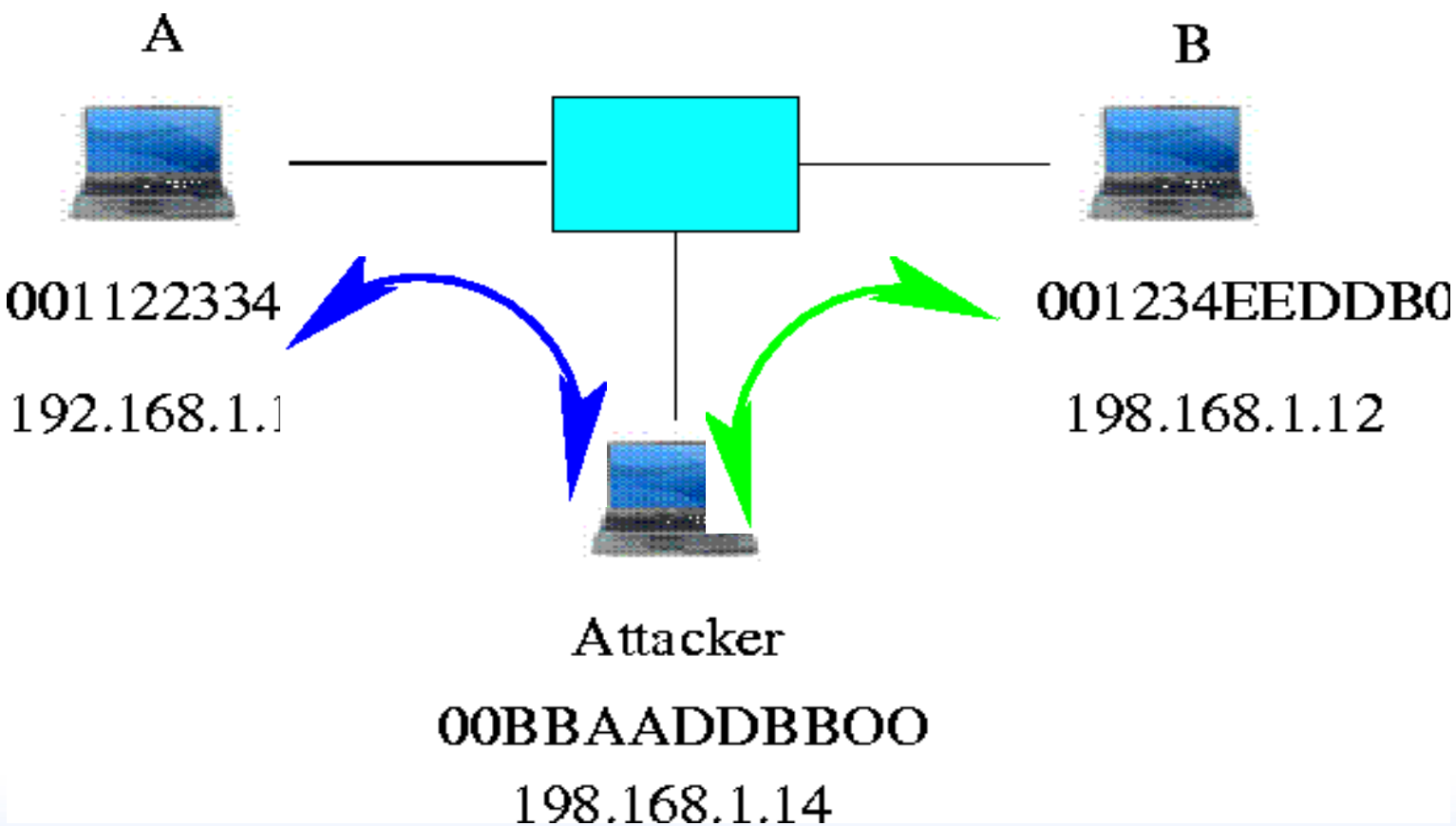
The extension headers are not checked until it the destination identified. The following order is recommended in RFC 2460 and that they feature no more than once except for the destination options which can occur at most twice (once before a Routing header and once before the upper-layer header):

IPv6 header, Hop-by-Hop Options header, Destination Options header (note 1), Routing header, Fragment header
then
Authentication header (note 2), Encapsulating Security Payload header (note 2), Destination Options header (note 3) and then upper-layer header

note 1: for options to be processed by the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the Routing header.	**note 2**: additional recommendations regarding the relative order of the Authentication and Encapsulating Security Payload headers are given in [RFC-2406].	**note 3**: for options to be processed only by the final destination of the packet.

Network Classes



Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255

ARP Poisoning