

State of the State of Control System Cyber Security

Joe Weiss, PE, CISM

IEEE PES San Francisco Section
October 15, 2007

What Are the Goals

- Maintain reliability and availability
- Minimize intentional and unintentional cyber events
- Promote better understanding and communication between IT security and Operations personnel
- Encourage vendors to provide secure instrumentation, control, and monitoring hardware and software
- Address myths and issues stemming from recent DHS disclosures

Definition

- Cyber Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional. (FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System*, March 2006.)
 - What is important about this definition
 - Intentional or unintentional
 - Actual or potential compromise of CIA
 - Violation or imminent threat to CIA

Myths

- Using Windows and TCP/IP makes it IT
- External, malicious threats are the biggest concerns
- Firewalls make you secure
- VPNs make you secure
- Encryption makes you secure
- IDSs can identify control system attacks
- Messaging can be one-way
- Field devices can't be hacked
- You are secure if hackers can't get in
- More and better widgets can solve security problems
- NERC CIPs have been approved by industry and FERC
- ...

NERC and FERC

- NERC has issued the NERC CIPs that industry has accepted
- FERC has proposed accepting the NERC CIPs with MODIFICATIONS and has issued a NOPR which will have significant industry impact (even beyond electric)
- Potential impacts include:
 - Classification of critical cyber assets
 - Systems and threats to be considered
 - Other technical issues

PG&E FERC NOPR Submittal

- These standards may not prevent the most far-flung scenario imaginable, but standards that address any scenario, no matter how unlikely, would be neither desirable nor feasible.
 - The NERC CIPs don't address events that have occurred
- More extreme or aggressive measure could in fact detract from reliability
 - The CIPs don't address recommendations from the Northeast Outage Report
- The proposed CIP standards are the result of concerted, open, and honest debate by industry participants with decades of technical expertise in protecting and managing the reliability of the electric system.
 - ISA comments rejected as well as drafting team member comments
 - Doesn't mention anyone with control system cyber security experience
- PG&E disagrees with the Commission's proposal to direct NERC to modify Requirement R1.2 of CIP-002-1 to include a requirement that a Responsible Entity "show why specific assets were or were not chosen as critical assets, and to require the consideration of misuse of control systems." The Responsible Entity's asset identification methodology will adequately document how critical assets and critical cyber assets were selected.
 - These are cyber, not reliability standards which PG&E doesn't address

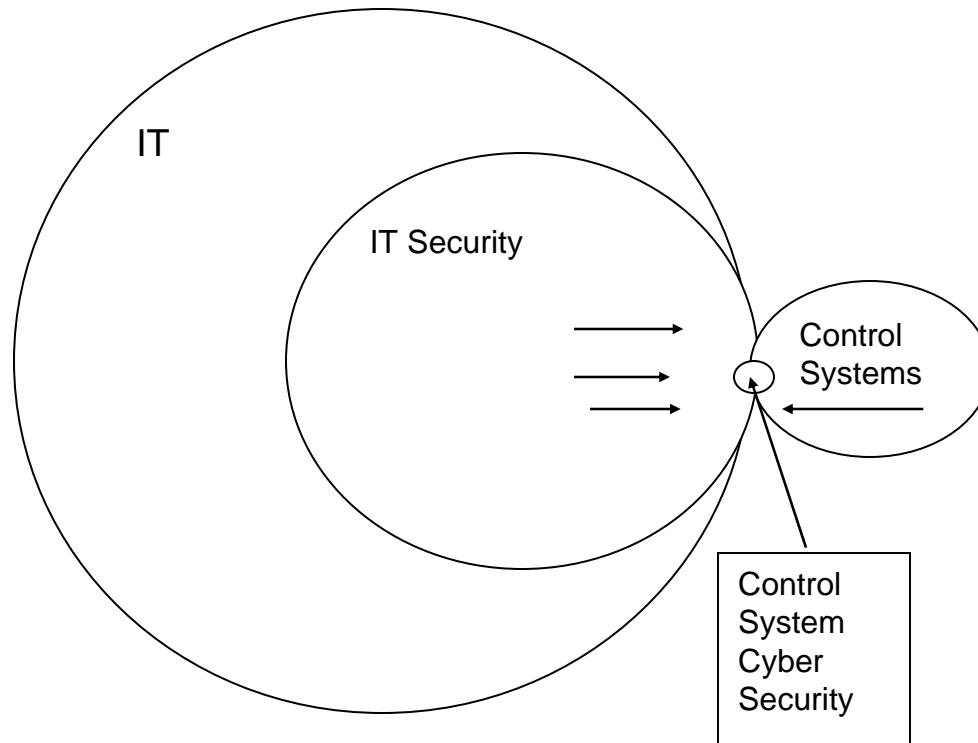
Selected Case Histories NERC CIPs Would Not Have Addressed

- February-April 2000 wireless hack of Australian sewage system
Issues: The Final Report of the Northeast Blackout recommends the development of capability to detect wireless and remote wireline intrusion and surveillance. The NERC CIP excludes telecom and non-routable protocols and does not explicitly address wireless. NIST SP800-53 does not have these exclusions for telecom or non-routable protocols and directly addresses wireless communications.
- June 20, 2003 “SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector”.
Issues: The slammer worm affected the frame relay communications to the substations. The Final Report of the Northeast Blackout recommends the development of capability to detect wireless and remote wireline intrusion and surveillance. The NERC CIP excludes telecom. NIST SP800-53 does not have the exclusion for telecom.
- NRC Information Notice: 2007-15 from August 2006 broadcast storm
Issues: Nuclear plants represent approximately 20% of the US electric generation. Shutdown of nuclear facilities would have a significant impact on the reliability of the bulk electric grid. The NRC is responsible for the safety of nuclear plants, that is, safe shutdown. NRC does not “regulate” the continued operation of nuclear plants to provide grid reliability as can be seen from the NRC Information Notice. However, the NERC CIP excludes nuclear power facilities. NIST SP800-53 does not have these exclusions for nuclear plants.
- June 2007 Southwest outage
Issues: Intentional, though not malicious, software change in distribution SCADA. The NERC CIP excludes Distribution. NIST SP800-53 does not have the exclusion for distribution systems.

Cultural Change is Needed

- Productivity considerations are pushing the use of vulnerable systems and connections
 - Eliminating “Islands of Automation” can have unexpected consequences
 - Interoperability can create cyber vulnerabilities
- Operations and IT view the other as the risk
 - Operations views O&M as their driver; security is an impediment
- Operations and IT have different goals
 - Operations wants reliability; IT wants security
- Engineers like “toys” ; IT likes COTS
 - Both can be vulnerable
- Need to reduce “Paperwork Maximization Act”
 - “Paperwork” doesn’t necessarily make you more secure

Why Are There So Few Experts



Cyber Security is a Process

- System vulnerabilities and threats are constantly changing
 - Any modification, integration, upgrade, or test can affect cyber vulnerability
 - Vulnerability assessments are a snap-shot in time
- There is NO silver bullet
 - No single technology is sufficient to protect control systems
 - Relevant control system security policies and procedures are closest
 - Without appropriate policies, any technology can be defeated

Pipeline Rupture with Fatalities

June 10, 1999 SCADA failure resulted in a pipeline rupture

- Gasoline leaked into two creeks in the City of Bellingham, Washington and ignited
- Fireball killed three persons, injured eight other persons
- Caused significant property damage
- Released approximately ¼ million gallons of gasoline causing substantial environmental damage



Browns Ferry Unit 3 Shutdown

NRC Information Notice 2007-15, issued
April 17, 2007

Both reactor recirculation pumps 3A and 3B tripped after the pump's Variable Frequency Drives (VFDs) became inoperable

The condensate demineralizer's PLC controller also failed simultaneously

All 3 failures attributed to the controller's Ethernet connections to the plant's "integrated computer system" (ICS) network, and excessive traffic on this network

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

April 17, 2007

NRC INFORMATION NOTICE: 2007-15: EFFECTS OF ETHERNET-BASED, NON-SAFETY RELATED CONTROLS ON THE SAFE AND CONTINUED OPERATION OF NUCLEAR POWER STATIONS

ADDRESSEES

All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice (IN) to alert licensees about recent operating experience related to the effects of potential interactions and unanticipated failures of ethernet connected non-safety equipment on the safety and performance capability of nuclear power stations. NRC expects that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this IN are not NRC requirements; therefore, no specific action or written response is required.

DESCRIPTION OF CIRCUMSTANCES

On August 19, 2006, operators at Browns Ferry, Unit 3, manually scrammed the unit following a loss of both the 3A and 3B reactor recirculation pumps. Plant procedures following the loss of recirculation flow required the manual scram. Immediate loss of the recirculation flow placed the plant in a high power, low flow condition where core thermal hydraulic stability problems may exist at boiling-water reactors (BWRs). Generally, intentional operation in this condition, of high power and low flow, is not permitted. Although some BWRs are authorized for single loop operation, sudden loss of even one pump could present the plant with the same stability problems and could result in the reactor protection system initiating a shutdown of the plant.

The initial investigation into the dual pump trip found that the recirculation pump variable frequency drive (VFD) controllers were nonresponsive. The operators cycled the control power off and on, reset the controllers, and restarted the VFDs. The licensee also determined that the Unit 3 condensate demineralizer controller had failed simultaneously with the Unit 3 VFD controllers. The condensate demineralizer primary controller is a dual redundant programmable logic control (PLC) system connected to the ethernet-based plant integrated computer system (ICS) network. The VFD controllers are also connected to this same plant

ML071010303

INL Cyber Test



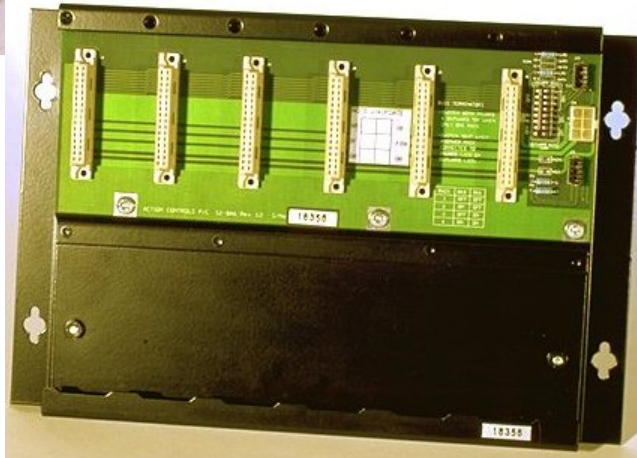
Need to Understand the Differences Between IT and ICS

- ISO 17799 was not developed for control systems
- Many IT security technologies designed to focus on confidentiality rather than integrity or availability issues
- Passive and active penetration testing approaches developed for IT systems with full IP stacks may be harmful to legacy control systems
- Some industry standards such as NERC CIPs and NEI-0404 not focused on legacy field devices
- Some control system vulnerabilities are different
 - First few cases to be addressed were neither Microsoft nor the Internet

Typical Operator Interface



Typical PLC Hardware



Comparison of Control Systems to IT

Attribute	Office IT	Control Systems
Confidentiality	High	Low
Message Integrity	Low-moderate	Very High
Availability	Low-Moderate	Very High
Time Criticality	Delays tolerated	Critical
Security skills/awareness	Good	Usually poor
Patching	Frequent	Slow or impossible
System Life Cycle	3-5 years	15-25 years/multiple year replacement cycle
Software changes	Frequent, formal, and documented	Rare, informal, not always coordinated
Automated tools	Widely used	Limited, used with care
Interoperability	Not critical	Critical, security often not a consideration

Comparison of Control Systems to IT

Attribute	Office IT	Control Systems
Communication protocols	IP	DNP, ICCP, Modbus
Communications	Telco, wi-fi	Telco, radio, satellite, power line carrier, wi-fi
Computing resources	High	Very limited
Bandwidth	High	Limited
Security standards	ISO-17799	ISA SP99, etc
Administration	Centralized	Localized
Operating systems	COTS (Windows)	COTS for HMI, proprietary real time for field devices
Security impacts	Business	Business, equipment, personnel safety, and environment

Comparison of Control Systems to IT

Attribute	Office IT	Control Systems
Information Assurance	Yes	No
Software development standards	Usually	Usually not available
Interoperability	Not important	Very important
Software changes	Frequent, formal, and documented	Rare, informal, not always coordinated
Automated tools	Widely used	Limited, used with care

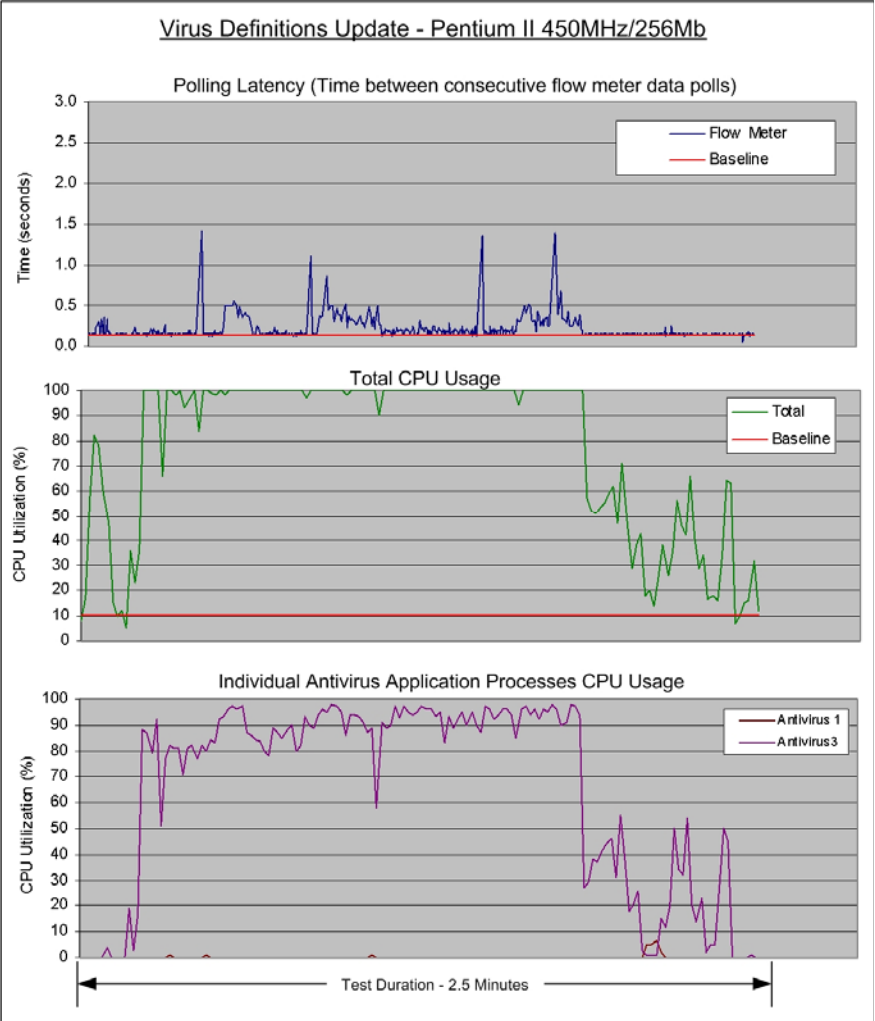
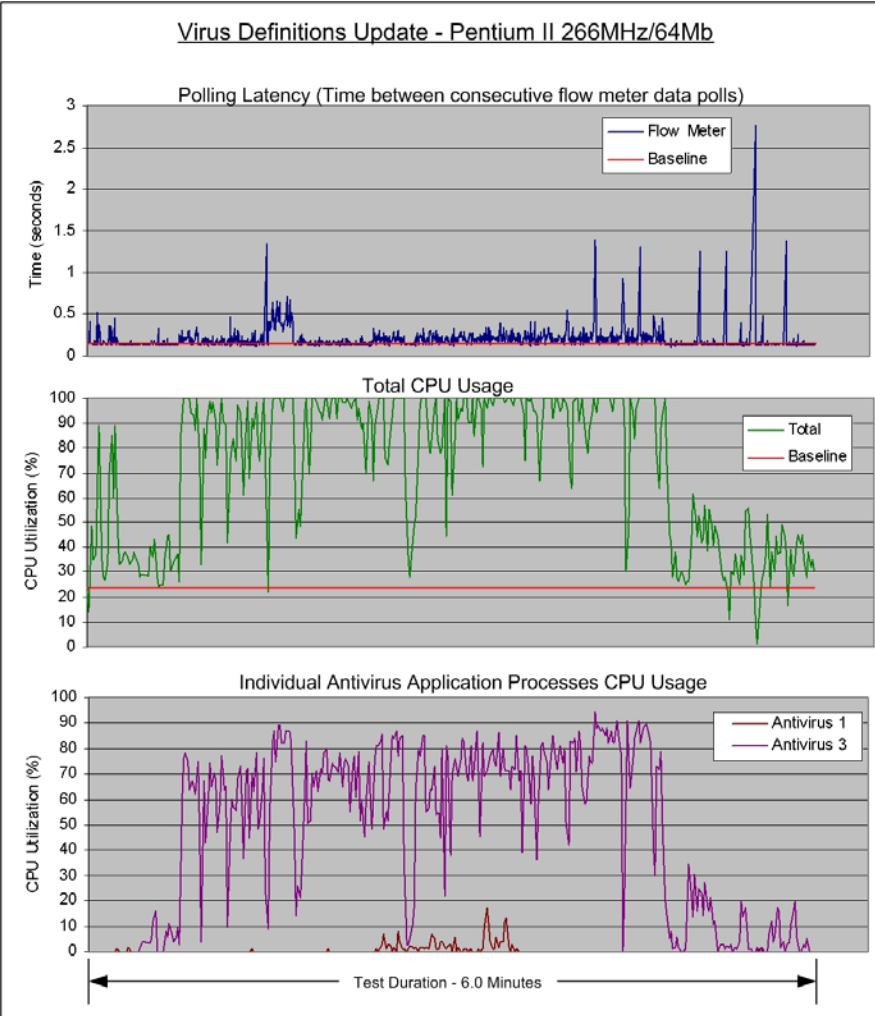
Generational Issues with Control Systems

- Legacy equipment
 - Security agnostic
 - Vulnerabilities backfit and security often turned off
 - Will be around for at least another 5 years
- New equipment
 - Vulnerabilities designed in
 - Will become pervasive in about 5 years for the next 15-20 years
- Future equipment
 - Security and performance part of initial design criteria
 - Probably about 20 years away before pervasive

Other Vulnerabilities

- Dial-ups still being used with new equipment
 - Many dial-up connections are not even owned by the end-user
 - War-dialing may not be possible if telephone line installed by vendor
- Use of wireless modems, bluetooth, web services, Telnet, SNMP, DCOM, ActiveX, and other vulnerable applications in new equipment
- Use of vulnerable versions of remote access including PCAnywhere, Hummingbird, etc
- Connections between plant and corporate networks
- Backdoors designed in (“Onstar” for control systems)

Test Case Data - *Virus Definition Update*



UNIT SUBSTATIONS NOW WEB-ENABLED TO SIMPLIFY ACCESS TO POWER TRANSFORMER DATA

Aug. 29, 2005 – Equipped with an Ethernet interface and Web server, Vendor A Unit Substations now provide simple, affordable access to power system information – including transformer coil temperatures – using a standard Web browser. The pre-engineered equipment ships in standard lead-times and connects to a customer's existing Ethernet Local Area Network much like adding a PC or printer.

Unit substations include a Temperature Controller, which provides remote access to transformer data, in addition to its primary role in controlling cooling fans. With a simple click of a mouse, it is easy to monitor transformer coil temperatures per phase, and verify cooling fan status at a glance. Among the many potential benefits, these new capabilities make it possible to correlate circuit loading with transformer temperatures to extend equipment life.

The typical unit substation incorporates Medium Voltage Metal-Enclosed Switchgear on the primary side and Low Voltage Switchgear or Low Voltage Switchboard on the secondary.

Vendor A was the first manufacturer in the world to embed an Ethernet interface and Web server into its power distribution equipment, allowing customers easier access to power system information. The family of power distribution equipment includes medium and low voltage switchgear, unit substations, motor control centers, switchboards and panelboards.



Other New Technologies

Powerful Mobile PDA Based HMI



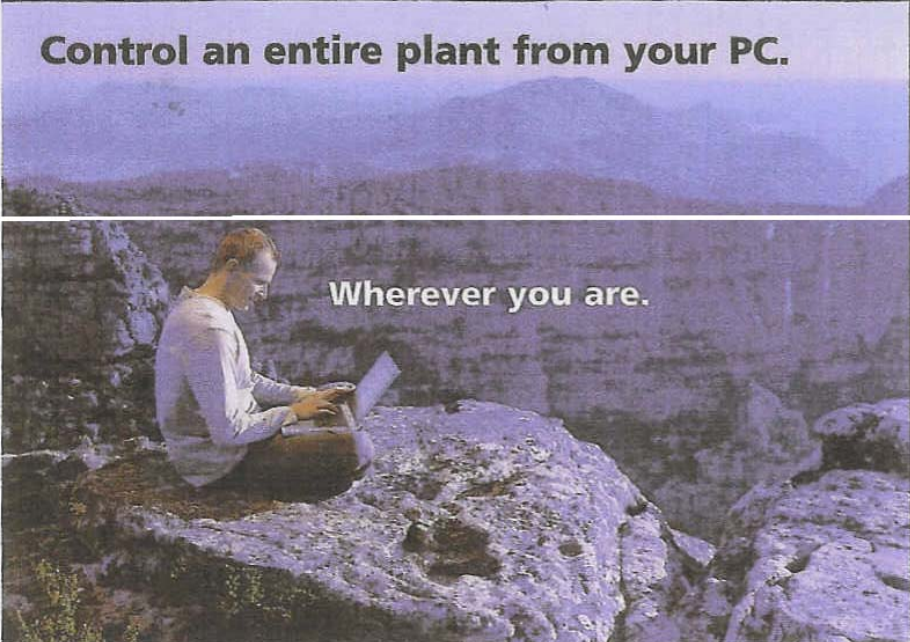
- Periodic Independent System Validation
- HMI/SCADA System Installation Checkout
- Diagnostic Troubleshooting
- Datalogging w/GPS Location
- Clipboard Replacement

Controller Interfaces
Modbus - TCP/IP
Ethernet/IP - OPC
Many More...

Communications
WiFi (802.11) - Bluetooth
Ethernet - Serial
Infrared (IrDA)

SOFTWARE
11/02/05
001 Copyright © 2005 Software Resources Inc.
HMI/SCADA and Software Features are registered Trademarks of Software Resources Inc.
All other Trademarks belong to their respective owners.

Control an entire plant from your PC.



Wherever you are.

Disclosure Issues (White Hat)

- Minimal disclosures to “White Hat” community
 - Very few public cases
 - Reticence to disclose
 - Myths (examples)
 - Salt River Project – Roosevelt Dam
 - CA ISO hack
 - FUD
- Other public disclosures
 - Hole Found in Protocol Handling Vital National Infrastructure
<http://www.eweek.com/article2/0,1895,2107265,00.asp>

Disclosure Issues (Black Hat)

- Technical disclosures to “Black Hat” community (2005)
 - Step-by-step instructions on how to hack Modbus, DNP3, UCA, GOOSE
<http://toorcon.org/2005/slides/mgrimes/mgrimes-scadaexposed.pdf>
- Hacker shows flaw in software that controls key infrastructure (2007)
 - “After the basics I will be getting into the finer details of the protocols as to what function code, internal indication flags does what and how that can be used to attack or take down the SCADA system. I shall as well discuss and demonstrate the current level of security implementation that these sites have.”
<http://dvlabs.tippingpoint.com/appearances/>

What can the Government do

- Establish baselines for what are acceptable vulnerability and risk assessments
- Establish minimum security requirements – metrics
 - How much security is enough
- Evaluate technology on actual systems
 - Assure that security does not affect performance
- Support industry organizations such as ISA SP99 and SP100, IEC, and IEEE
- Mandate NIST standards efforts – 800-53, 800-82, FIPS99/100

Summary

- Leaping from mid-80's to mainstream networking technologies has advantages and disadvantages
 - We need to understand them enough to make prudent decisions or we will become less secure
- We need to be able to specify security in products and employ relevant practices
 - This requires an understanding of security and system performance