EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

NERCOMP SIG

Security Architectures

Christopher Misra
University of Massachusetts

September 2007

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Outline

- What is security architecture
- Example: Network Access Control (NAC)
  - Network Topology
  - Wired and Wireless
  - Automating Policy Enforcement
  - Registration and Endpoint Intergrity
- Diagnostics (How do we know it all works)
  - Logging, Monitoring, Netflow,
- Support
  - Integrating security

Why Architecture?

- Network security is composed of a variety of components
  - Policies
  - Procedures
  - Technologies/Tools
- But what provides a coherent plan to ensure that we meet our IT security goals?

Why Architecture?

- IT Security Policy:
  - Formally state rules
  - Support Ethical use
  - Assign responsibility
  - Set strategic goals
- Procedures:
  - Sequence of tasks and decisions
  - Ensure consistency
  - Implement tactical goals

Why Architecture?

- IT Security tools:
  - Perform technical actions
  - Require technical skill
- Architecture
  - "*Art and discipline of creating or inferring an implied or apparent plan of any complex object or system*"

http://en.wikipedia.org/wiki/Architecture

Security Architecture

- Security systems are complex
- The interrelation between components is not obvious
- The technical details of security systems can obscure perspective with respect to other critical systems
- Tools are not always completely compatible with the desired outcome

Security Architectures

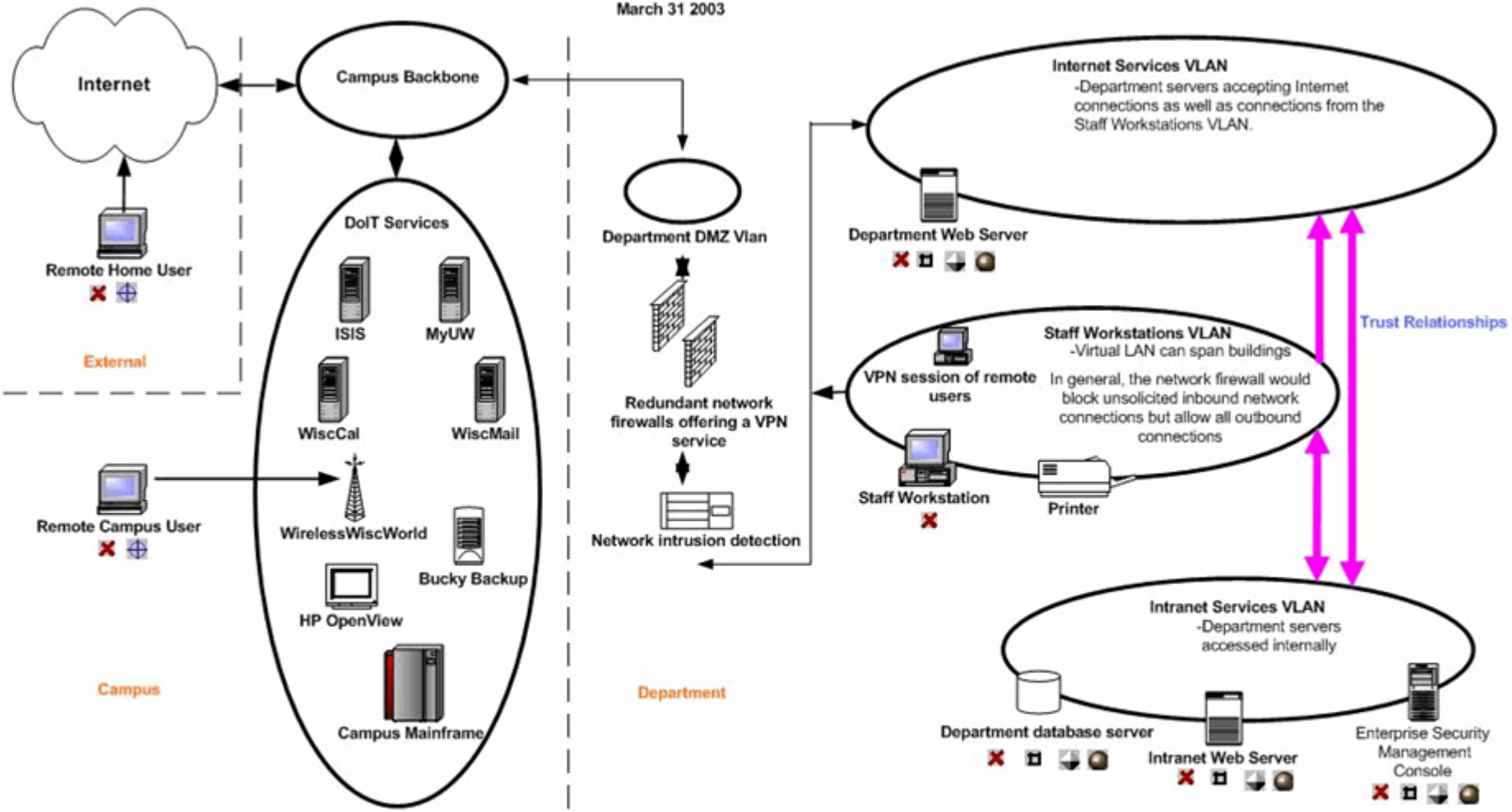
What do we mean by network security architecture?

Architecture: n. Orderly arrangement of parts; structure

Creating organized structures, using tools, techniques, and procedures, to cohesively mitigate information security risk consistent with policy.

Example Secure Network Architecture

March 31 2003



Design Notes:

This example network is a high level logical diagram design to illustrate a number of security standards, eg defense in depth, and security controls, eg network firewall, virus protection, etc and how they might be implemented together to lower risk.

Example Implementation:
Network firewalls -> NetScreen, Cisco PIX
Network intrusion detection -> Cisco 4235 appliance
Enterprise Virus Protection -> Symantec AntiVirus Corporate Edition
Enterprise File Integrity -> Enterprise version of Tripwire
Host based firewall -> Kerio (Windows), SunScreen (Solaris)
Host Based Intrusion Detection -> Cisco Host Sensor

Security Controls Key

- VPN Client
- Enterprise Virus Protection
- Host Based Intrusion Detection
- Enterprise File Integrity
- Host based firewall

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Security Architecture and Models

- “Rather than grafting security onto existing systems, it is more effective to redesign systems to make security an integral part of them. However, developing a security architecture for colleges and universities is complex because of the needs of different groups sharing the network (for example, academic, administrative, clinical, and residential). Many college and university networks must be able to accommodate unknown devices, including handheld devices and being connected by visitors, students, and other members of the community.”

https://wiki.internet2.edu/confluence/display/secguide/Security+Architecture+and+Models

Network Topology

- Many network design decisions impact security
  - Providing capabilities
  - Constraining available tools
- Different networks behave differently
  - Wired vs Wireless
  - Consistency of use experience

Network Segmentation Drivers

- Wide availability of 802.1q
  - Ability to deploy multiple security domains with limited overhead
  - Effective use of existing wiring
  - Cost savings
- Layer 2 isolation
  - Perceived vs. actual security
- Unmanaged systems
- Wireless

Network Segmentation

- Network quarantines
  - Automated policy enforcement (NetAuth)
- SCADA devices
  - **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
- VPN
  - User-based and LAN-to-LAN
- VoIP
  - Device and application

Other Network Segmentation

- Additional security perimeters
  - Residential and Academic
  - Campus Surveillance
  - Life Safety
  - Wireless
  - Parking meters
  - Vending machines
  - Door Swipes

Firewalls and VPN

- Firewalls are traditional segment boundaries
  - Now, often implemented with vLANs, ACLs, VPNs, etc.
- Segmentation paradigm is not intrinsically dependent on the firewalling capabilities
- VPN often serve this role for remote sites
  - Unique set of challenges

Network Segmentation Benefits

- Smaller perimeters mitigate some risks
- Inability to properly secure some endpoints
  - SCADA devices
- Perform endpoint policy compliance
  - Posture assessment
- Limit spread of ‘bad things’
  - Reactive or automated

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Network Segmentation Challenges

- Network edge is now contingent on switch port configuration
  - What is the system of record?
  - Configuration management
- Limited end user visibility
  - How do I know what network I am in?
- Who can use what?
  - Sounds like middleware

EDUCAUSE INTERNET2 | COMPUTER AND NETWORK SECURITY TASK FORCE

Network Segmentation Challenges

- Adding complexity to mitigate risk
  - Difficulty in problem diagnosis
- Does not improve basic service
- May constrict or preclude 'good things'
  - Apparent non-deterministic behavior to end users
  - What *works* here, doesn't *work there*
- Reduces network transpency
  - So much for end-to-end connectivity

Policy enforcement

- Preventative policy enforcement often implemented by segmentation
- Automated remediation systems frequently rely on segmentation
  - positive security impact on a large number of hosts
  - relatively small time investment from computing staff.

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Policy compliance: Posture assessment

- Proper patch level
- Up-to-date antivirus software
- Other administratively defined conditions.
- Commercial software
  - Cisco Network Admission Control (**NAC**)
  - Microsoft Network Access Protection (**NAP**)
  - Countless others (at least 35)

Policy compliance: Posture assessment

- Open-source software
  - Southwestern NetReg,CMU NetReg, Packetfence, RINGS
- Standards
  - IETF Network Endpoint Assessment (**NEA**)
    - https://www1.ietf.org/mailman/listinfo/nea
  - Trusted Network Connect (**TNC**)
    - https://www.trustedcomputinggroup.org/groups/network/

Network Quarantines

- Isolation is enforced by changing network devices (or state)
  - to limit the access of non-compliant hosts
- Protects other hosts from isolated host
- Protect isolated host from additional compromise
- May provide a conduit for notifying the responsible individual/department

EDUCAUSE INTERNET2 | COMPUTER AND NETWORK SECURITY TASK FORCE

Network Quarantines

- May be result of initial or periodic host assessment
- Possibly event driven
  - IDS result
  - abuse@ mail
  - Other security or forensic result
- Communication with end user
  - Non-user endpoint device?

Fine-grained Policy Enforcement

- Proliferation of different classes of devices
  - VoIP phones
  - SCADA devices
- Allocation of device privileges may depend on class of device
  - Per device network segment assignment
  - Potential additional security risks

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Fine-grained Policy Enforcement

- Meta-data about devices is increasingly rich
  - Relationship to the enterprise directory
- Network privilege assignment is complex
  - Posture assessment
  - Device class
  - User-centric or Device-centric
- *eduDevice*?

Fine-grained Policy Enforcement

- How are devices authenticated?
- Devices that can't speak EAP?
- Can you handle fall-through authentication?
  - If (can 802.1x)
    elsif (web-redirect)
    elsif (MAC address filter)
    else (deny access)

Fine-grained Policy Enforcement

- VPN
  - Per-user privilege allocation
  - Transport security and security perimeter in one
  - Application-centric proxies
- Tight IdM integration
  - This isn't a new problem, just an application of middleware to a different medium

Fine-grained Policy Enforcement

- Non IdM data sources
- Applying security perimeters based on non-network centric characteristics
  - Certain devices in certain buildings
  - Some devices in no buildings
  - Time of day limitation
- Generic network device authorizations

Fine-grained Policy Enforcement

- We still need a limited set of resultant policy classes
  - Policy is a continuum (real number)
  - vLANs are not (hopefully small integer)
- How are policy class communicated to the user
  - What are the challenges of dynamic policy class assignment

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Managing Complexity

- How do new technologies impact current and future segmentation capabilities
  - Optical
  - Federated network access
- Does segmentation map directly to security perimeters
  - Linearly or non-linearly
- How do we understand these changes

Wired vs Wireless

- Wired and wireless network equipment each have distinct capabilities
  - Users do not see it this way
- Same security capabilites
  - 802.1x
  - Endpoint integrity
- Different security capabilites
  - Wireless: WEP/WPA/WPA2

Wired vs Wireless

- Open edge
  - Open DHCP (“free love”)
  - DHCP with MAC registration (“netreg”)
  - VPN-only access (“vpn”)
  - Web middlebox (“portal”)
    - Cisco Clean Access, Bluesocket, AP portals, etc…
- *Static WEP (“doesn’t scale”)*
- 802.1x w/ Dynamic WEP, WPA, WPA2

Open Wired Edge

- No client authentication
  - Application encryption encouraged
- Often depends on physical security
  - Jacks are usually in locked offices
- Lowest Common Denominator
  - Nearly any device/user can connect

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Open Wireless Edge : Common Features

- No encryption between client and AP
  - Application encryption encouraged, naturally
  - But – can’t guarantee this for all sites
  - Some information disclosure anyway (src, dest IP)
- Lowest Common Denominator – Nearly any device/user can connect

Unrestricted WiFi : Challenges

- Isolating systems requires DHCP configuration changes or AP MAC filters
- Difficult to notify isolated users if you can't identify them
  - Notifying help desk/support also a challenge
- Legal, security, and resource usage implications
  - Of course, wireless authn should not be the sole factor in granting application privileges
  - YMMV…

DHCP/MAC Registration : Common Features

- Can limit access to valid users
  - Via authenticated registration interface
  - Web browser not necessarily required
- Infrequent registration
  - e.g. once per semester
- Users are identified
  - e.g. for isolation, notification, etc

DHCP/MAC Registration: Challenges

- *Devices* (not users) are identified
  - Associated to a given user at time of registration
- Subject to MAC address spoofing
- NetAuth: active/passive scanning required

Mandatory VPN : Common Features

- Provides network-layer encryption and authentication
- Can use ACLs to require VPN for access outside of wireless network
- Not necessary to track/filter MAC address
  - Each session is authenticated
- Limited to authorized users

Mandatory VPN : Challenges

- Client software install often required
- Not all systems supported
  - Linux/MacOS clients may be limited
- Client support = Help Desk Hell
  - If you think email was difficult…
- Increased overhead
- No easy access for guests
- NetAuth: active/passive scanning required

EDUCAUSE INTERNET2 | COMPUTER AND NETWORK SECURITY TASK FORCE

Web Middlebox (portal): Common Features

- Middlebox often required to be inline
  - Many support 802.1q termination
- Web-based authentication interface
  - Per-session authentication
- MAC address filter bypass
  - Devices may be *registered* to bypass authentication
- NetAuth scans may be triggered from reg page (assuming portal support)

Web Middlebox (portal): Challenges

- Physical infrastructure constraints
  - Parallel backbone or distributed middleboxes
- Requires web browser on client
- Possible spoofing
  - More complicated to attack than DHCP/MAC registration
- 802.1x migration challenges

Static WEP

- Not worth much consideration, as it simply doesn’t scale
- Adds encryption between client and AP
- But..
  - One key shared by everyone
  - Key can be easily recovered given time

802.1x Edge Authentication

- Authn required prior to network access
- Client software ("supplicant") required
  - Windows XP/2K: framework built-in, some supplicants built-in
  - Mac OS X: framework and most supplicants built-in
  - Linux: Add-on software provides supplicants
  - Windows Mobile: Add-on software

802.1x ~ Encryption

- 802.1x authn provides keys for edge encryption
- Several levels of encryption:
  - Dynamic WEP: 40/104-bit RC4
    - Proprietary extension, widely supported
  - WPA/TKIP: 104-bit RC4
    - Standard, good client & AP support
  - WPA2/802.11i: 128-bit AES
    - Standard, limited client & AP support

802.1x ~ Authentication Types

- Multiple authentication types possible with 802.1x. This modularity comes from the Extensible Authentication Protocol (EAP)
- Some EAP supplicants builtin to OSs, others as third party
  - Microsoft Windows EAP framework [builtin to XP, 2K]
  - Apple OS X EAP framework [builtin to Mac OS X 10.3+]
  - SecureW2
  - Funk Odyssey
  - Meetinghouse AEGIS
  - wpa_supplicant
  - Xsupplicant
  - Wire1x

802.1x ~ EAP Deployment

- Each site should choose one (one+ possible) EAP method for authentication
- Most popular EAP methods:
  - TLS: X.509 client certificate authn
  - TTLS: Tunneled TLS; no client cert required. Can transport plaintext password (TTLS:PAP)
  - PEAP: Protected EAP; often used w/ MS AD (PEAP:MS-CHAPv2, PEAP:GTC)
- Other EAP methods
  - LEAP: Proprietary; cracked.
  - FAST: Proprietary; not widely supported.
  - SIM: Authentication for mobile phones.

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

802.1x ~ EAP Compatibility

Client	98/ ME	XP/ 2K	OS X	Li nux	Pckt PC	TLS	PEAP	TTLS	License
Win Builtin	✗	✓	✗	✗	✗	✓	CHAP v2	✗	Builtin
OSX Builtin	✗	✗	✓	✗	✗	✓	✓	✓	Builtin
SecureW2	✗	✓	✗	✗	✓	✗	✗	✓	Free
Odyssey	✓	✓	✗	✗	✓	✓	✓	✓	$$
AEGIS	✓	✓	✓	✓	✓	✓	✓	✓	$$
wpa_supp	✓	✓	✗	✓	✗	✓	✓	✓	Free
Xsupplicant	✗	✗	✗	✓	✗	✓	✓	✓	Free

Reference: LIN 802.1x factsheet

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

802.1x ~ Encryption Compatibility

Client	WEP	WPA	WPA2	License
Win Builtin	✓	✓	✓	Builtin
OSX Builtin	✓	✓	✓	Builtin
SecureW2	✓	✓	✗	Free
Odyssey	✓	✓	✓	$$
AEGIS	✓	✓	✗	$$
wpa_supp	✓	✓	✓	Free
Xsupplicant	✓	✓	✓	Free

Note: Some hardware & operating system restrictions may apply to support.

Reference: LIN 802.1x factsheet

802.1x ~ EAP, what's missing?

- Current practical authn types:
  - X.509 Certs (TLS)
  - Plaintext password (TTLS:PAP, PEAP:GTC)
    - e.g. for LDAP, Kerberos, OTP
  - Windows hashed password (PEAP:MSCHAPv2, TTLS:MSCHAPv2)
- Many sites use Kerberos; EAP-Kerb/EAP-GSSAPI would be ideal
  - Somewhat tricky, as recall there is no network connectivity pre-auth
  - Some work on this by Shumon Huque @ UPenn

802.1x ~ RADIUS

- RADIUS authn required for EAP
- Server must support chosen type
- Multiple servers provide redundancy (but accounting becomes trickier)
- Servers:
  - Cisco ACS
  - FreeRADIUS
  - Radiator
  - Infoblox
  - Funk Steel-belted
  - Many others…

802.1x ~ NetAuth

- Edge authentication provides no easy opportunity for pre-connection scanning
- Instead:
  - Active, periodic scans can be used
  - Passive detection
  - Could monitor RADIUS Acctng to launch scan
- Common issue: handling insecure boxes
  - Could use dynamic vlan support to drop users into a walled garden (AP support required)

802.1x ~ Putting it Together

- Access Points
  - Must support EAP type (**should** just pass-through all types)
  - Must support 802.1x auth and encryption mechanism
- Encryption Type (WEP/WPA/WPA2)
  - Must be supported by APs
  - Must be supported by client hardware, OS drivers, and supplicant
- Authentication Type (EAP Method: TLS, TTLS, etc..)
  - Must be supported by client hardware, OS drivers, and supplicant
  - Must be supported by RADIUS server
- RADIUS Server(s)
  - Must support backend authn using EAP credentials

802.1x ~ Deploying

- Client config / software may be required
  - Can't provide instructions over 802.1x net, due to pre-auth requirement
- Common solution: a limited-access open SSID to provide instructions
- Debate over SSID broadcast
  - Windows tends to ignore "hidden" SSIDs when preferred broadcast SSIDs are present
  - But broadcasts can create confusion, and..
  - Some APs can only broadcast a single SSID (a waning issue)

Example Deployment: 802.1x

- Deployment at a “well-known” University
- Pilot deployment began Aug 2005 in one building
- Encryption: WPA
  - Believed the number of older machines would be very small
  - But WPA2 has only limited client support currently (APs are capable)
- Authentication: EAP-TTLS:PAP
  - Backend auth against central Kerberos database
  - All users login as “userid@example.edu”
- RADIUS Server: FreeRADIUS
- Instructions are provided via an open SSID, which doubles as a web login portal for guests
  - Any University user can generate one time use “tokens” granting a guest up to 2 weeks of access

Diagnostics

- ***Diagnosis*** *(from the Greek words dia = by and gnosis = knowledge) is the process of identifying a disease by its signs, symptoms and results of various diagnostic procedures. The conclusion reached through that process is also called a diagnosis.*
  - http://en.wikipedia.org/wiki/Diagnosis
- ***Diagnostic***
  - A symptom or a distinguishing feature serving as supporting evidence in a diagnosis.

Network Diagnostics

- Provide effective exchange, management, and correlation of log and event information
  - between dependent layers
  - among interdependent components
- A data orchestration function

http://www.cmu.edu/computing/eddy/introduction.htm

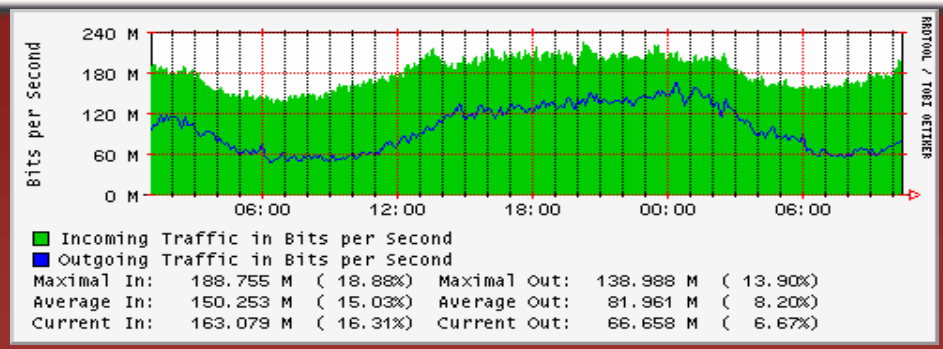
Network Diagnostics

- Enable system managers to pinpoint problems as they occur
- Allow autonomic processes to assist in prediction, management, and maintenance.

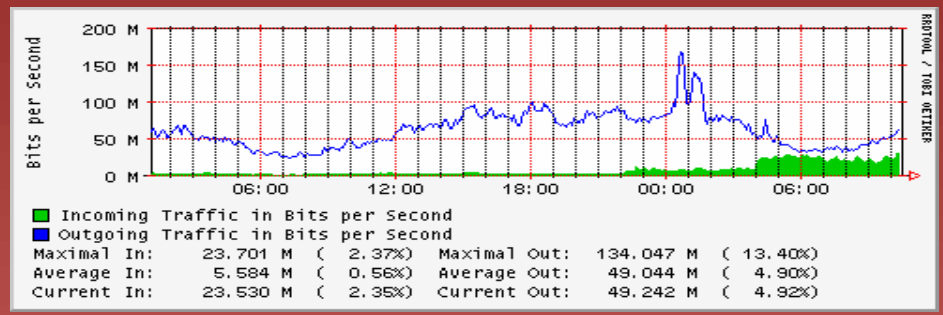
http://www.cmu.edu/computing/eddy/introduction.htm

Local Network Bandwidth

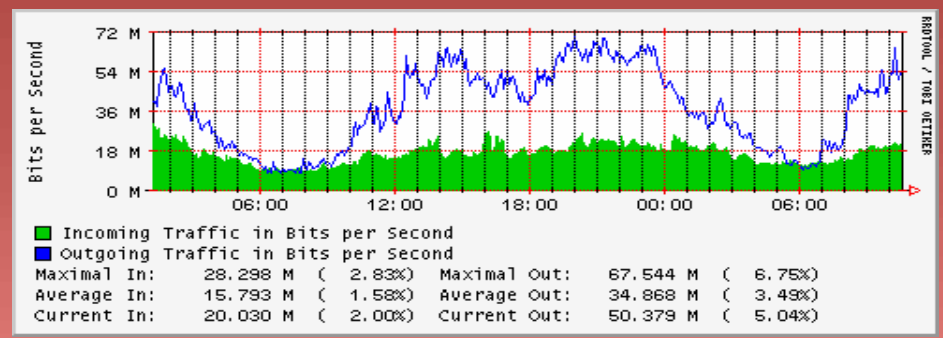
- Edge1 <-> Border



- Edge2 <-> Border

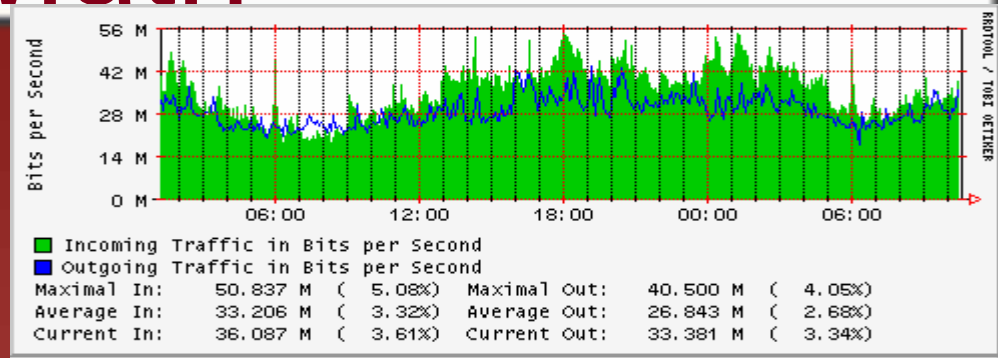


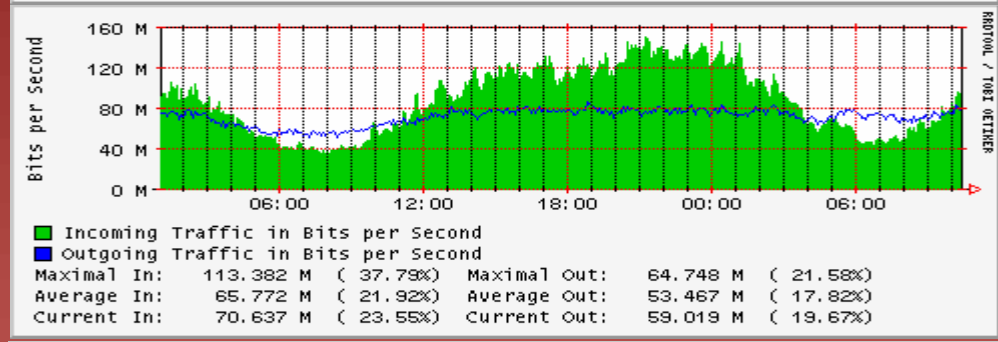
- Local Peers

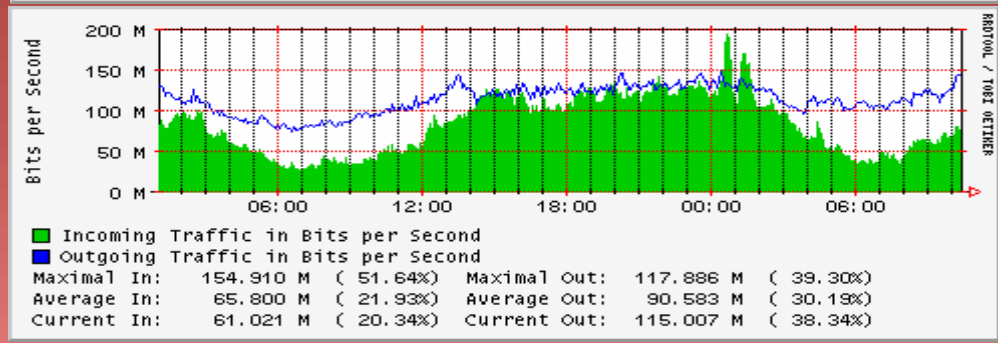


Peering Network Bandwidth

- Internet2
- Commodity ISP1
- Commodity ISP2

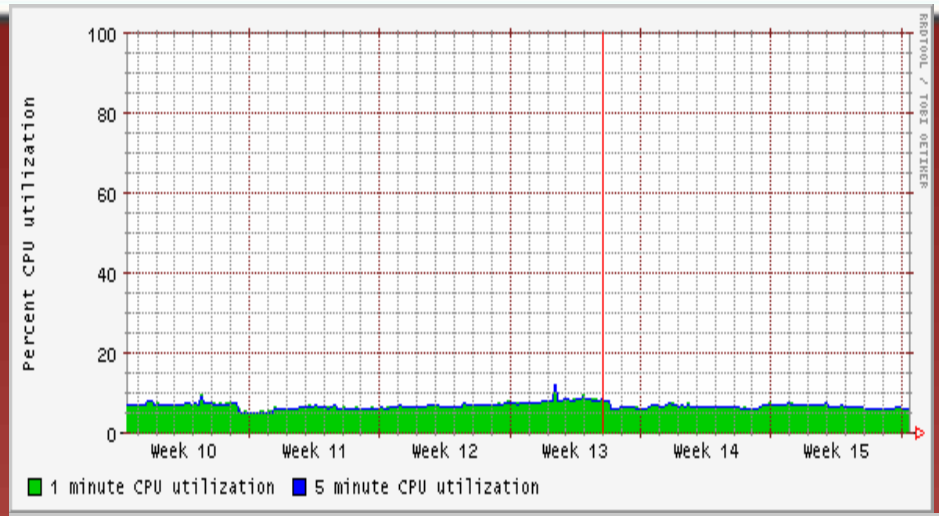


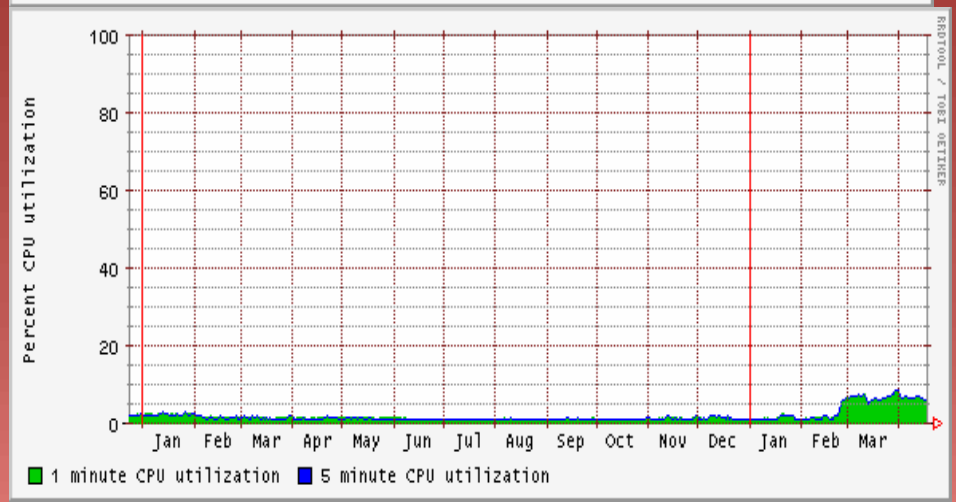




CPU Utilization

- Monthly
- Yearly

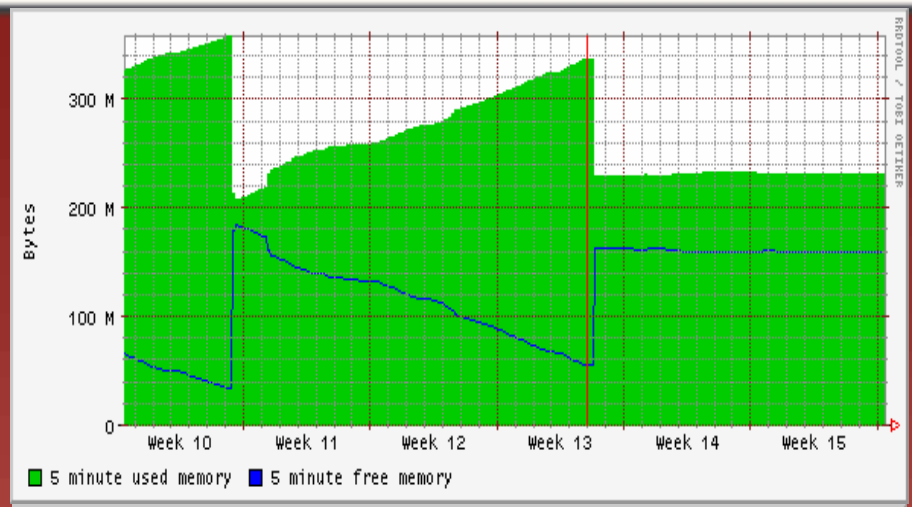


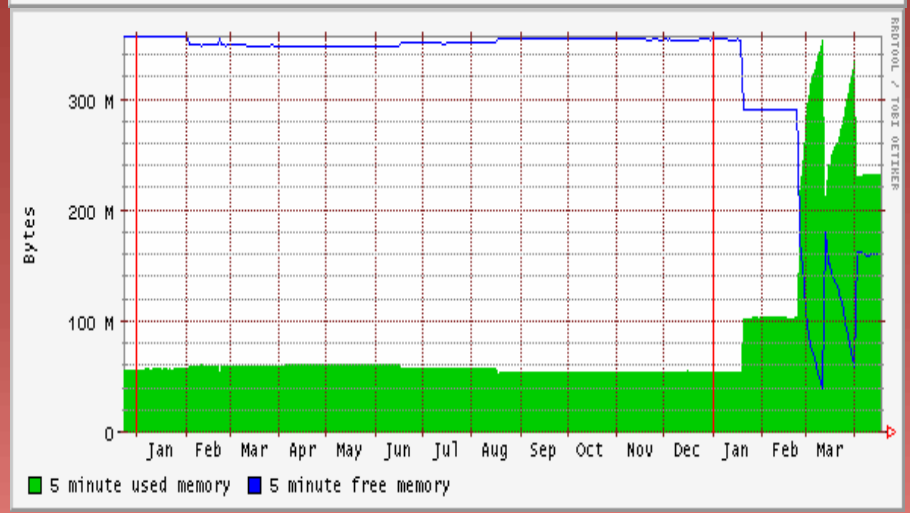


COMPUTER AND NETWORK SECURITY TASK FORCE

Memory Utilization

- Monthly
  - 5 minute polling
  - Used vs Free
- Yearly
  - 5 minute polling
  - Used vs Free

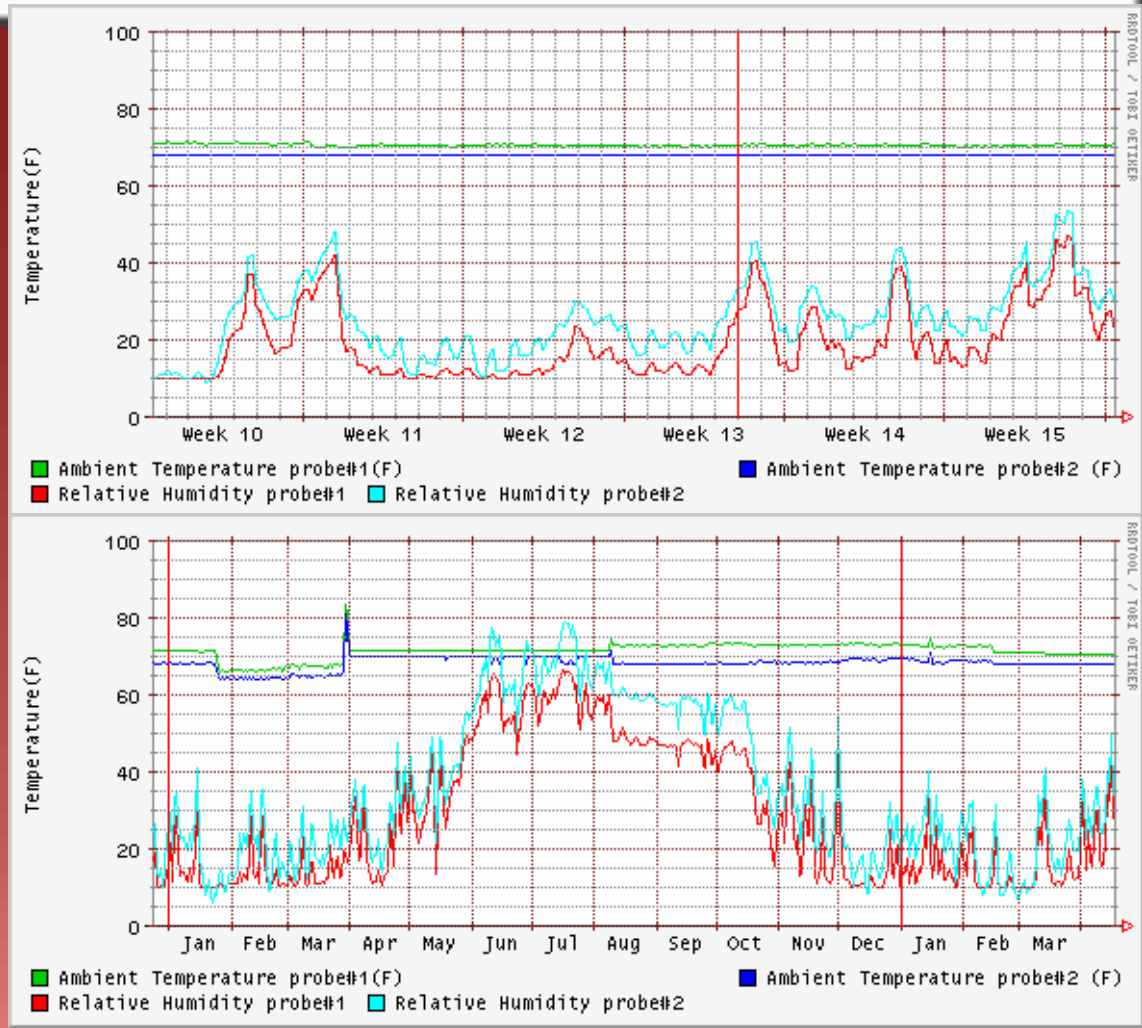




COMPUTER AND NETWORK SECURITY TASK FORCE

Environmental

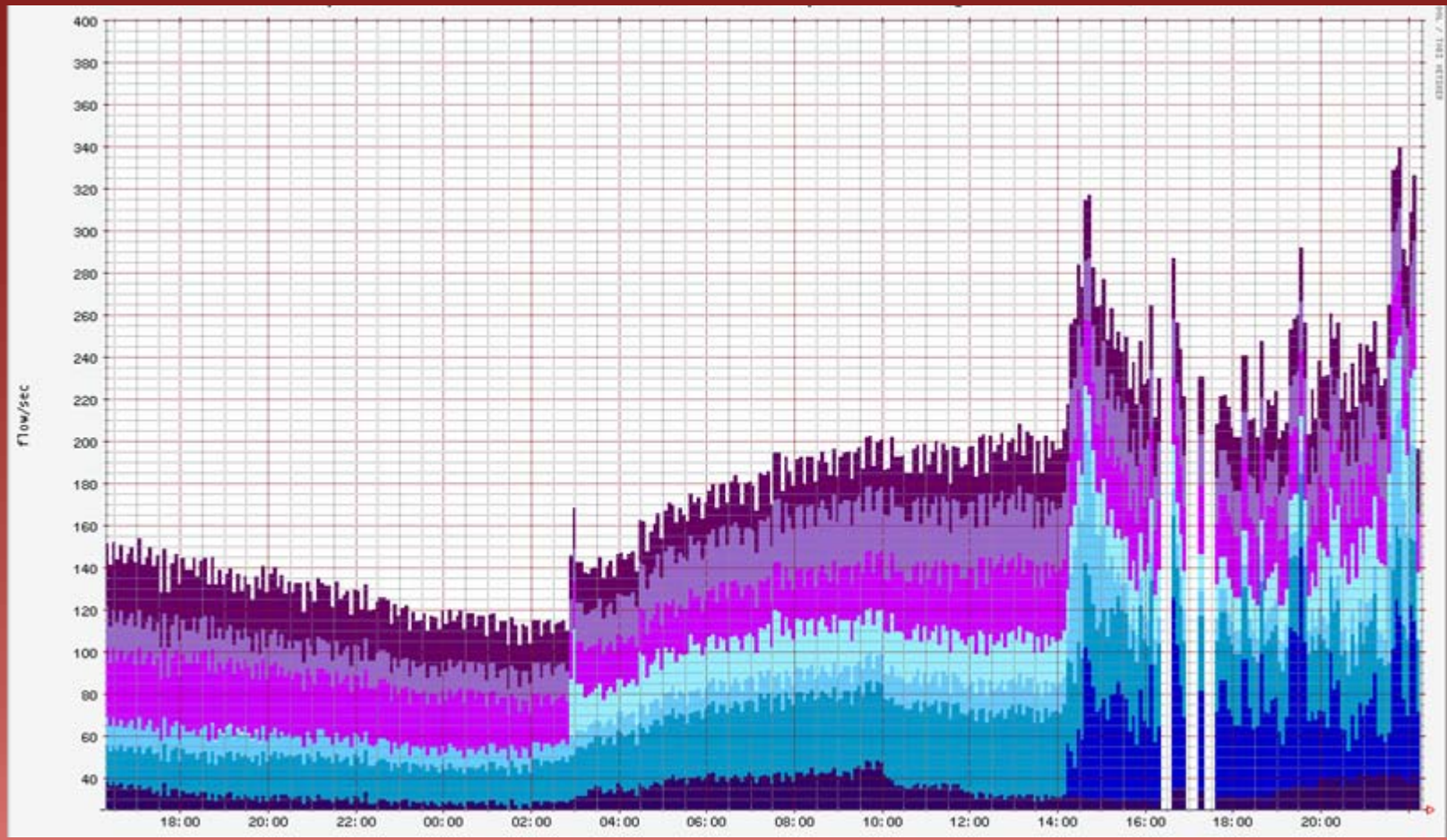
- Monthly
  - Temperature
  - Humidity
- Yearly
  - Temperature
  - Humidity



EDUCAUSE INTERNET2

COMPUTER AND NETWORK SECURITY TASK FORCE

Netflow



Netflow

"NetFlow technology efficiently provides the metering base for a key set of applications including network traffic accounting, …"

- Data export mechanism that records information about router flows.
  - Src/dst IP, port, etc
  - Bytes
  - No packet content is logged

Unified logging

- Given the number and variety of systems that generate logs, it is intractable to manually parse them
  - Syslog helps, but doesn't reduce the data
  - Databases help, but add complexity
- Given sufficient unification, registration may not be necessary
  - GULP from Columbia

Config Management

- Given the large number of infrastructure devices, automated management is required
  - Device availability
  - Scheduled outages
- Configurations need to be centrally stored
  - And retrievable
- Accountability and audit capability
  - To allow efficient restoration of service

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Help Desk and security

- Are security incidents different from traditional trouble ticketing?
  - Not always
- Many schools have support incidents through existing help desk services.
- Involved some training and awareness for help desk staff
- Also been significant work done in facilitating interactions between the information security team and the help desk.

Conclusions

- These tools can form an architecture
  - Often site local
- However the tools in and of themselves are insufficient
  - We need an architecture to tie together these components
- Security should be part of the infrastructure, not retofit

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Conclusions

- We need a coherent plan to ensure that we meet our IT security goals
- Security and IdM share aligned goals
  - But not always aligned implentations
- We need to develop this area
  - Staff that are fluent across layers
  - Policies, Procedures,Technologies/Tools
- This requires more than just technical managers…

EDUCAUSE INTERNET2 COMPUTER AND NETWORK SECURITY TASK FORCE

Resources

- CAMP: Bridging Security and Identity Management
  - http://www.educause.edu/camp081

References

- EDUCAUSE ‘Security Architecture’
  - Jack Suess, UMBC

  http://www.educause.edu/ir/library/pdf/pub7008j.pdf

- Windows Security Architecture Blueprint

http://www.microsoft.com/technet/itsolutions/wssra/raguide/ArchitectureBlueprints/rbabsa.mspx?mfr=true

This Presentation

http://people.umass.edu/crispy/conf/