Network Security Overview

by Clifford Collins

Thursday, May 31st, 2001
What We Are Going To Cover

The Importance of Policy
Event Logging
Firewalls
Intrusion Detection Systems
Administrative Computing
Departmental Connections
You Really Need Policy
Office Modems
Modem Scanners
Modem Pools
Dormitory Connections
Internet Scanners
Your Policy Needs to be Written Down
Public Key Infrastructure
Directory Services
Certificate Authorities
Routers
Wireless
Let’s Begin At The Beginning
Your users don’t care how good your security may be

People want utility-grade service, now!

Performance and ease-of-use cannot be significantly impacted by security

You have limited resources to protect finite assets

And, if something goes sour, you’re responsible!
Primary Threats
Both Accidental and Deliberate

Unauthorized Access
Unauthorized Modification
Unauthorized Destruction
Unauthorized Disclosure
A Walking Tour Of Network Security
Event Logging
The Ideal Campus Network

- **PKI, DS, and CA**
- **PBX**
- **Telco**
- **Modem Pool**
- **Policy**
- **Internal Network Scanner**
- **Event Logger**
- **Dept. Connections**
- **Office Workstation**
- **Modem Scanner**
- **PKI, DS, and CA**
- **Policy**
- **Internal Network Scanner**
- **Policy**
- **Policy**
- **Policy**
- **External Network Scanner**
- **Policy**
- **Admin Computing**
- **Policy**
- **IDS**
- **Policy**
- **Policy**
- **DMZ**
- **Policy**
- **DSL & Cable Modems**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Office Workstation**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
- **Policy**
Characteristics of an Event Logger

Protected record of events
Originates from every sensor on net
Allows for the reconstruction of an incident
Basis for pattern analysis and Intrusion Detection Systems
Only effective if fed from all strategic devices
All unusual events should be logged
All attempts to authenticate should be logged
All system transitions should be logged
All session terminations should be logged
All mail events should be logged
All administrative transactions should be logged
All certificates issued should be logged
All logs are privileged (restricted access)
Firewalls and Intrusion Detection Systems
Intrusion Detection System (IDS) Policy

Firewalls and IDS

Firewall

Policy

Internet

External Network Scanner

Policy

DSL & Cable Modems

Admin Computing

Policy

DMZ

Intrusion Detection System (IDS)

Policy

Firewall

E-mail Web FTP
Firewall and IDS Policy

- All firewalls should be registered
- Firewalls must log events centrally
- Firewalls are to be tested periodically
- Firewalls are to be monitored
- IDS should not be left on autopilot
- IDS should be tested periodically
- Penalties for attempts to bypass or penetrate without authorization
Policy drives everything

Even if it isn’t written down, something is implied

Subject to institution rules and regulations

Subject to state and federal laws

Ignore creating policy and it will bite you!
Administrative Computing
Traffic From Administrative Offices

- Admin Computing
- Policy
- Firewall
- Intrusion Detection System (IDS)
Traffic From The Dorms Or A Public Lab

Admin Computing

Firewall

Policy

To Event Logger

Firewall
Unauthorized access and attempts are considered hostile

All transactions are logged

No access from off campus (except via approved VPNs)

Authentication - password length, characters, change frequency, lockout, reset, notification

Strict, detailed, access controls
Departmental Connections
Department With No Servers

Departmental Connections

Office Workstations

To Event Logger

Traffic From Off Campus

Policy

Policy
Department With Modems

Departmental Connections

Policy

Office Workstations

Modem

Policy
All hosts must be registered centrally
Use DHCP? Register MAC addresses?
No NATs?
Maintain current revisions of software
Respond to central notifications and incidents
Wireless?
No dial-in modems
Modem Scanners
The campus phones will be scanned periodically to detect modems
Scans will be unannounced
Penalties for unauthorized modems
Modem Pools
Modem Pool

Policy

To Event Logger

Dial-in Modem Pool

A legitimate user logs in

Telco
An unauthorized person attempts to log in, perhaps several times.
How many failed attempts before lockout?
How do they get it reset?
How many concurrent connections?
Account sharing?
How long can they stay connected?
Is there a maximum connect time per month?
What characterizes legitimate use?
What penalties for violations?
Dormitory Connections
Dormitory Connections

Policy

Dormitories
Dormitory Policy

Are they allowed to run servers?
Are they allowed to attach to both the phone and the network (run a dial-in service)?
Outbound traffic only?
On campus only?
Academic use only?
Bandwidth restrictions?
Penalties for violations?
Internet Scanners
Internet Scanners

Internal Network Scanner

Policy
External Scanner

Scanning the Backbone

External Network Scanner

To DMZ

To Backbone

To Event Logger

E-mail
Web
FTP
Scanning

Inventory what’s REALLY on your network

ID O/S, active ports, & active services

Determine brand and version of services

Flag known vulnerabilities

In some cases, do penetration testing (firewalls, IDS, critical services on DMZ)
Scanning Policy

The entire campus address space will be scanned periodically.

Results will be delivered to DNA and high risk systems WILL BE FIXED IN A TIMELY MANNER.

Teeth: failure to fix such systems will lead to blocking of its traffic.

All scanning that traverses the backbone must be centrally authorized (IDS triggered).
Public Key Infrastructure
Public Key Infrastructure

PKI, DS, and CA

Policy
Sensitive data is protected through encryption

Asymmetric keys: public and private

Messages are encrypted with recipient’s public key and signed with sender’s digital signature

Recipient decrypts messages with their private key and confirm digital signature
With PKI!
User asks registration authority for digital certificate

The registration authority verifies user’s ID and asks the CA to issue certificate

The CA stores the certificate in the directory and copies the user when needed
User accesses a secure server, providing a personal certificate

Server provides user with a server certificate

User and server validate received certificates by lookup in a directory. Once authentication is completed, the user is allowed access.
Routers
Route Updates

Your ISP

Internet

Joe Hacker

Policy

Dept. of Psycho-botany
ALL routers are to be managed centrally

Only static routes to departmental firewalls

Route updates are only to be accepted from your ISP (named routers)
Wireless
Wireless Issues

You can’t avoid dealing with wireless
Set policy before the “factory default”
sets it for you
Authenticate (RADIUS and soon PKI)
Roaming won’t work unless centrally
administered
All access points are to be registered
Avoid NAT and DHCP on access points
All departmental access points should use authentication
Unless encrypted all sessions are vulnerable – buyer beware
Log, log, log
Virtual Private Networks
The Ideal Campus Network
External Network Scanner

Admin Computing

Policy

DSL & Cable Modems

Intrusion Detection System (IDS)

E-mail

Web

FTP

Firewall

Virtual Private Network
Benefits of a VPN

- It safely extends your network to the remote or mobile user
- Supports individual access privileges
- It is proven and standards based
- Available off the shelf
- Removes the excuse for using “barefoot” access (POP, telnet, etc.)
VPN Policy

*It should be the only way to access your internal network from the outside (SSH a possible exception)*

*It must be authenticated*

*All sessions are logged (but not monitored)*

*Must be centrally managed*
Wrap Up
In Review

Understand the need for policy
Understand the need for logging of events
Understand the proper use of firewalls
Use packet filters on your departments
Modems in offices should be prohibited (or at least regulated)
Scan regularly for unauthorized modems
Scan regularly for vulnerabilities and unnecessary services

Plan on implementing or outsourcing PKI

Keep a tight grip on all routers

Be proactive on wireless or you’ll give away the store!

VPNs are the next logical step for telecommuters and conference attendees
Any Questions?
E-mail: ccollins@enss.net
E-mail: ccollins@oar.net
Phone: (800) 627-8101 x352
Web: security.internet2.edu
Web: www.enss.net
Web: www.oar.net