



Campus Network Design and Deployment@SANOG 17

Security Cookbook



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Tools and Topics

Some other Security Tools and Topics and how they relate to what we've been doing...

Topic Areas

- Access control
- Antivirus
- Authentication
- Detection
- Encryption

But, not necessarily in that order 😊

Covered so far...

- Basic cryptography
 - public/private keys
 - hashes
 - ciphers
- SSH and SSH Agent
- Kerberos
- LDAP
- Authentication

Authentication

How to verify you are who you say you are...

- **OPIE:** *One time Passwords In Everything*, implements a one-time password (OTP) scheme based on S/key, which will require a secret passphrase (not echoed) to generate a password for the current session, or a list of passwords you can print and carry on your person.
- **RADIUS:** *Remote Authentication Dial In User Service*, is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.



*free***RADIUS** The world's most popular RADIUS Server.

Authentication

How to verify you are who you say you are...

- **token based authentication:** one-time id per session to offer additional layer of security. Similar to OPIE. Many products and variations:
http://en.wikipedia.org/wiki/Security_token



Encryption

TLS: *Transport Layer Security:*

How TLS Works*

A TLS client and server negotiate a stateful connection by using a handshaking procedure:

1. The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported CipherSuites (ciphers and hash functions).
2. From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.
3. The server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA) and the server's public encryption key.
4. The client may contact the server that issued the certificate (the trusted CA as above) and confirm that the certificate is valid before proceeding.
5. In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key and sends the result to the server. Only the server should be able to decrypt it, with its private key.
6. From the random number, both parties generate key material for encryption and decryption.

*http://en.wikipedia.org/wiki/Transport_Layer_Security

Encryption

IPSec: Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

- Protects any application traffic across an IP network.
- An end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite.
- Uses SHA1 for integrity protection and authenticity and 3DES or AES for confidentiality.
- Available for most operating systems built in to the kernel stack:
 - ✓ Linux, AIX, OpenBSD, FreeBSD, Mac OS X
 - ✓ Windows (since 2000)
 - ✓ Cisco IOS
 - ✓ Android, z/OS, Solaris
 - ✓ Many more...

Encryption

- **PSK:** Pre-Shared Key. Used with deprecated Wi-Fi protection scheme known as WPA or “Home Mode”. Key is created on the AP and passphrase is used on the client to regenerate the key. Excellent details available here:

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- **PEAP:** The **Protected Extensible Authentication Protocol**, also known as **Protected EAP** or simply **PEAP**, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
 - **EAP:** http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
 - **EAP-TLS:** <http://en.wikipedia.org/wiki/EAP-TLS#EAP-TL>
 - **PEAP-TLS:** http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

Access Control

Gaining proper access to resources:

- **WPA-2 (802.11i): Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)** are the names of security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WPA using TKIP is largely deprecated
- **WEP: Wired Equivalent Privacy** (deprecated) security algorithm for IEEE 802.11 wireless networks. Is susceptible to eavesdropping. A WEP connection can be cracked with readily available software within minutes.

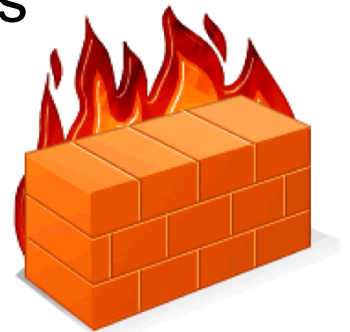
A nice primer on TLS, Wi-Fi and the use of the Extensible Authentication Protocol, or EAP:

<http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+9.+Upper-Layer+Authentication/Transport+Layer+Security+TLS/>

Access Control

Firewalls: Where to place them?

- Between VLANs and VRFs (Virtual Firewalls)
 - 3COM, Cisco, Juniper, etc. have solutions
- On individual servers
- On some clients
- Near the border? This is hard. Why?
 - Consider minimal key ACLs (NetBIOS, antispoofing, RFC 1918 leakage or ingress, etc.)
 - Do you need firewalls on all servers?



Access Control

Firewalls:

A few Open Source software-based options

- **IPTables** (iptables): Linux
- **IPFW**: FreeBSD
- **IPF**: FreeBSD, NetBSD, OpenBSD, SunOS, HP/UX, and Solaris
- **PF** (with ALTQ for QoS): FreeBSD and OpenBSD

Under Windows

- **Windows Firewall**: XP and above
- ZoneAlarm Pro, Comodo Firewall Pro, Outpost Firewall Free, PC Tools Firewall Plus, Privatefirewall, Tall Emu's Online-Armor, Ashampoo, Jetico, Lavasoft, Look'n'Stop, Net, Preventon, Sphinx [Software], Sunbelt, Bullguard, Computer Associates, F-Secure, Kaspersky, McAfee, MicroWorld, Norton, Panda & Trend Micro, Webroot.

And, there's always what comes on your wireless router...

Access Control

BCP38: *Best Current Practices 38*, or
“Ingress Filtering” as defined by RFC 2827:

<http://tools.ietf.org/html/bcp38>

Egress Filtering: Don't let your
compromised clients harm others. Keep
Your organization off blacklists.

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

Access Control

Egress Filtering

- Watch for viruses (part of Network Scanning)
- Block outgoing SMTP from unauthorized IPs
- Look for typical attack signatures and block
- What else?

Other Types of Access

- Rate limit users if necessary (PF w/ALT-Q or in HW)
- Transparent Proxies (Cisco's WCCP [Web Cache Control Protocol] and, possibly, the use of Squid)

Detection

Detect bad stuff on your network using
Network Intrusion Detection Systems (NIDS)

Open Source

- SNORT: <http://www.snort.org/>
 - ✓ sguil: <http://sguil.sourceforge.net/>



Commercial

- Cisco Intrusion Detection in hardware:
<http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz>
- VCC/Tripwire, F5, Big Iron, Juniper, etc.

Detection

Detect unexpected changes on servers:

Open Source

- Tripwire: <http://sourceforge.net/projects/tripwire/>
- Samhain: <http://www.la-samhna.de/samhain/>
- fcheck: `apt-get install fcheck ...`

Scan Servers for Vulnerabilities

- Nessus: <http://www.nessus.org/>
- nmap: <http://nmap.org/>
- Nikto: <http://cirt.net/nikto2>

```
# nmap -A -T4 -F <HOST>
```



Detection

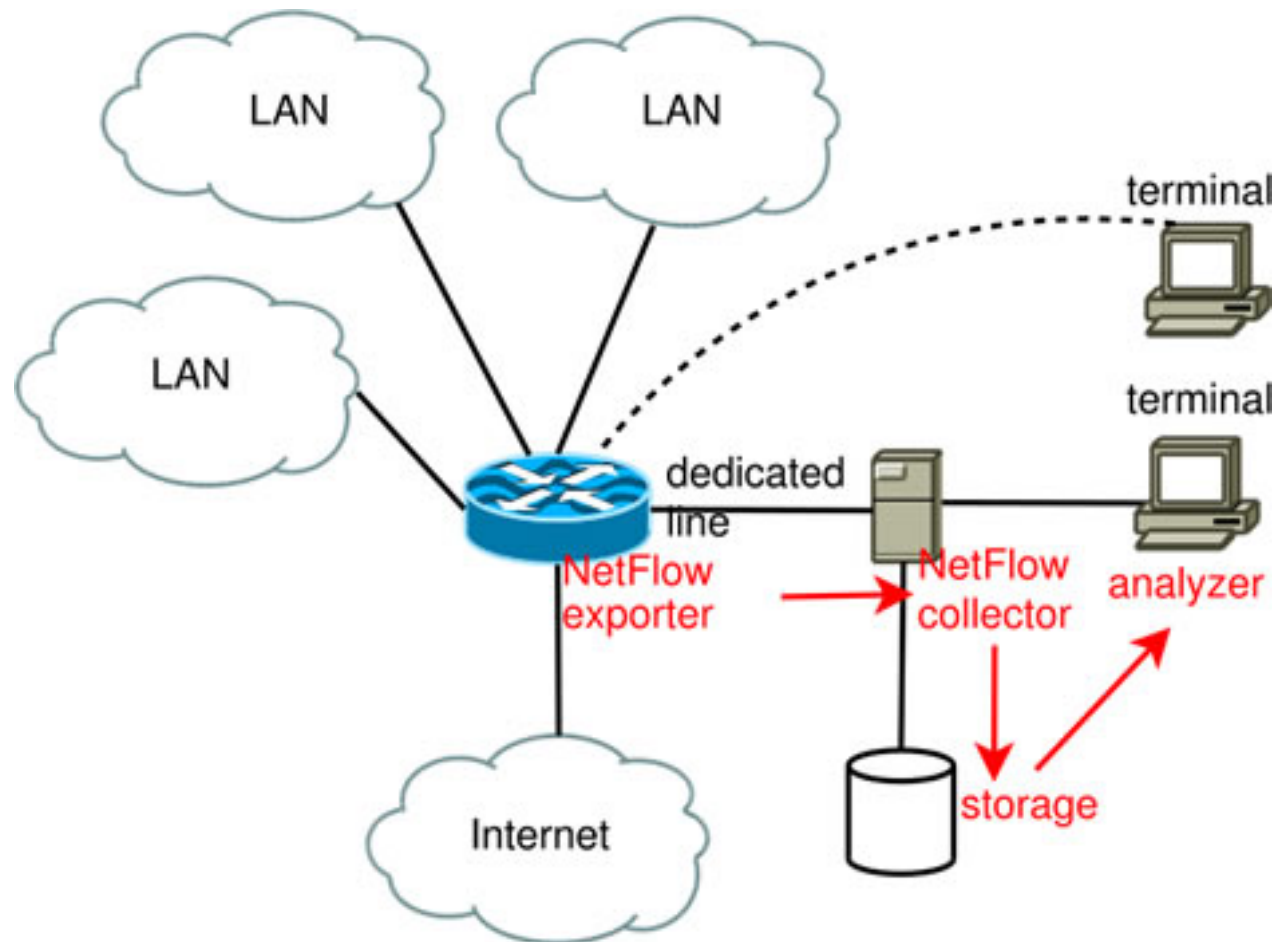
The NetFlow standard is available on Cisco, Juniper, HP, etc. hardware.

Use tools to view flows to detect DDoS attacks and common other network attacks:

Tools

- **nfdump** (collector): <http://nfdump.sourceforge.net/>
- **NfSen** (GUI): <http://nfsen.sourceforge.net/>
- **pmacct** (collector): <http://www.pmacct.net/>
- **pmGraph** (GUI): <http://www.aptnivate.org/pmgraph>

Detection: Netflow



Antivirus

From the server side. Scanning incoming and outgoing emails for viruses:

Open Source Tools

- Amavis Next Generation: <http://sourceforge.net/projects/amavis/>
- Clam Antivirus: <http://www.clamav.net/>
- exiscan (for Exim): <http://www.exim.org/>
- Mailscanner: <http://www.mailscanner.info/>
- Sanitizer: <http://mailtools.anomy.net/>



Graphing and Baselining

A core Network Monitoring and Management concept. We will discuss this tomorrow.

- Start to monitor your network
- Gain insight in to what is “normal” activity
- Graph this information



Now you will more easily detect abnormal conditions and be able to present this graphically.

A few references

- *Enterprise MPLS VPN – Howto*
http://brokenpipes.blogspot.com/2006_06_01_archive.html
- *FreeBSD Security*
<http://www.freebsd.org/doc/handbook/security.html>
- *Real Security For a Virtual Network*
<http://3comsblog.wordpress.com/tag/vrf/>
- *Securing Debian Manual*
<http://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-tools.en.html>
- *Top 100 Security Tools (2006)*
<http://sectools.org/>
- *Ubuntu Security Forums*
<http://ubuntuforums.org/showthread.php?t=510812>