Design Principles for Secure Enterprise Campus Networks

Mike Peeters

Security Specialist SE

Cisco Canada

CISSP, CCIE, CCSP, CCDA

Disclaimer

“This presentation provides a tit for tat description of a fictional electronic war between a disgruntled and determined employee and an overworked, but well funded, IT staff. Any similarities to your current environment is purely coincidental.

Cisco does not recommend such reactionary security design. Rather we suggest you pay close attention to the later half of this presentation and take a systematic approach to the network security problem.”

“Finally, sorry for all the acronyms.”

The Authors at Cisco Systems

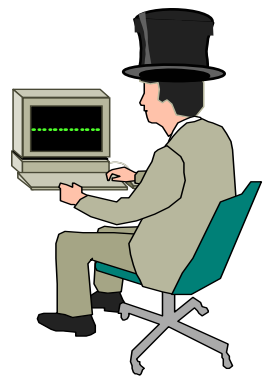
Let’s Get Started!

- **Welcome to HackFest (Campus) 2003!**

The Aggressor

- **Milton**
  - **Middle aged, mid-life crisis**
  - **Just bought a Miata**
  - **Former computer science major**
  - **Passed up for promotion by a witty go-getter named Chet**
  - **Wants revenge**

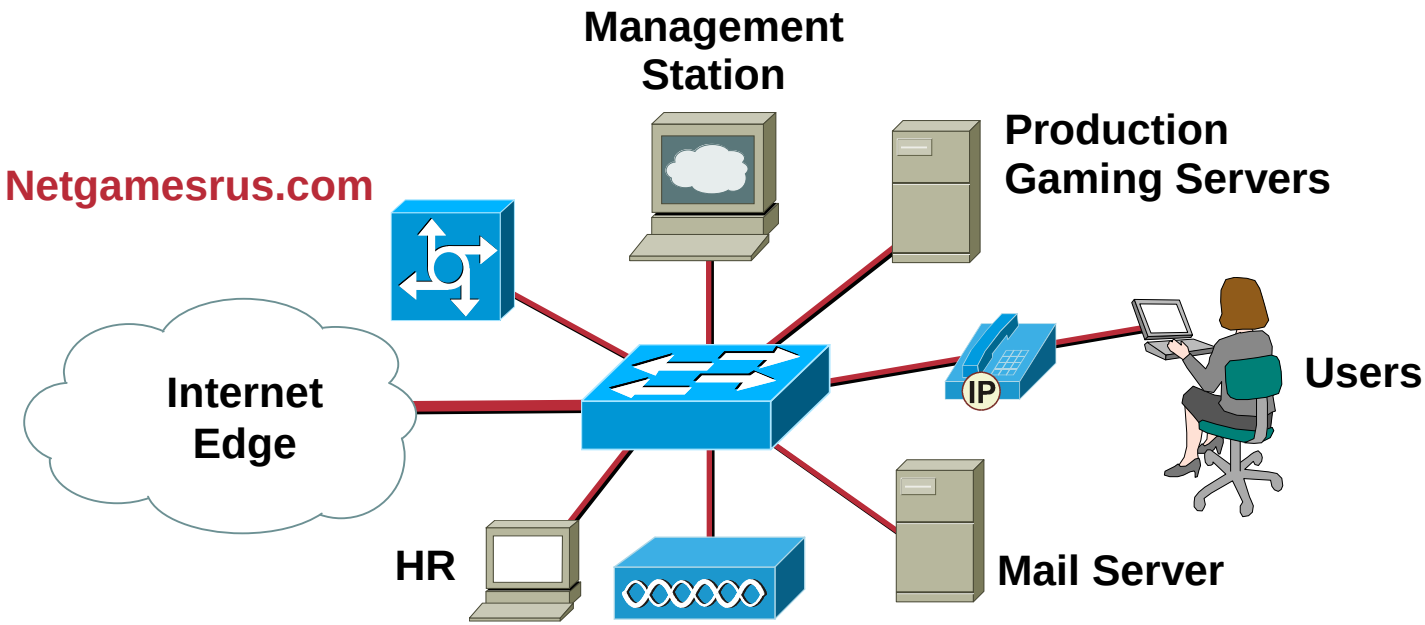
Milton



The Defenders

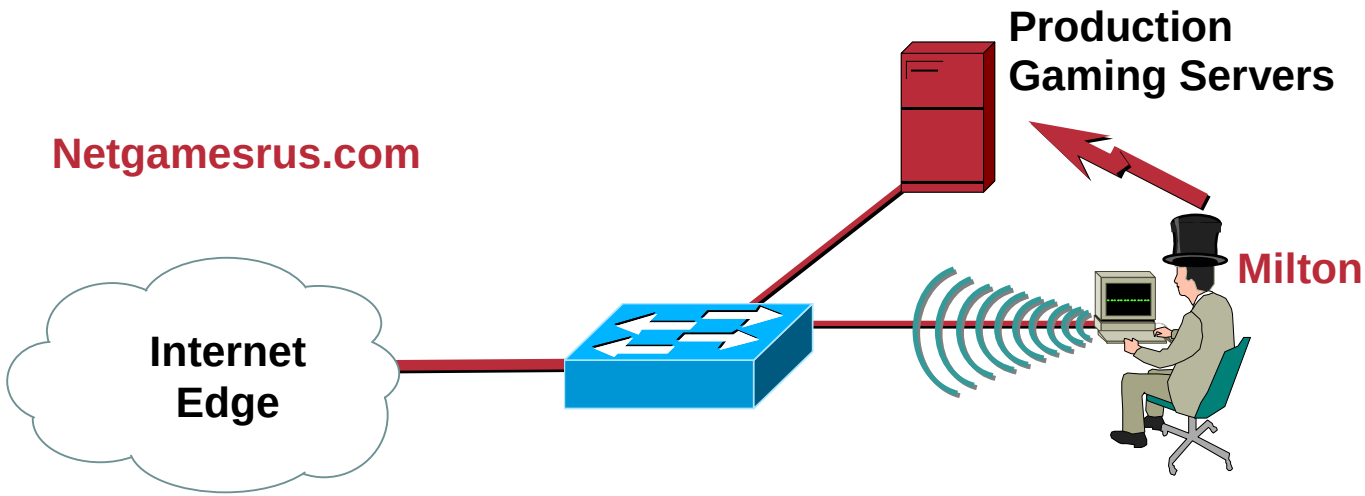
- **Netgamesrus.com**
  - **Web-based gaming company**
  - **Experienced explosive growth and hasn't had much time to think about security**
  - **IT staff is minimal, and most have occupied their time play-testing their newest creation**
  - **Just went through a second round of funding that hasn't been spent yet**

Initial Solution



- Campus is one flat network
- Management is done in-band (over the company's user network) and in the clear (telnet, tftp, syslog, SNMP)
- Dial-in access available (reusable passwords)
- WLAN access available via rogue AP (default SSID, static WEP)
- A single router in the edge provides reachibility to the outside world

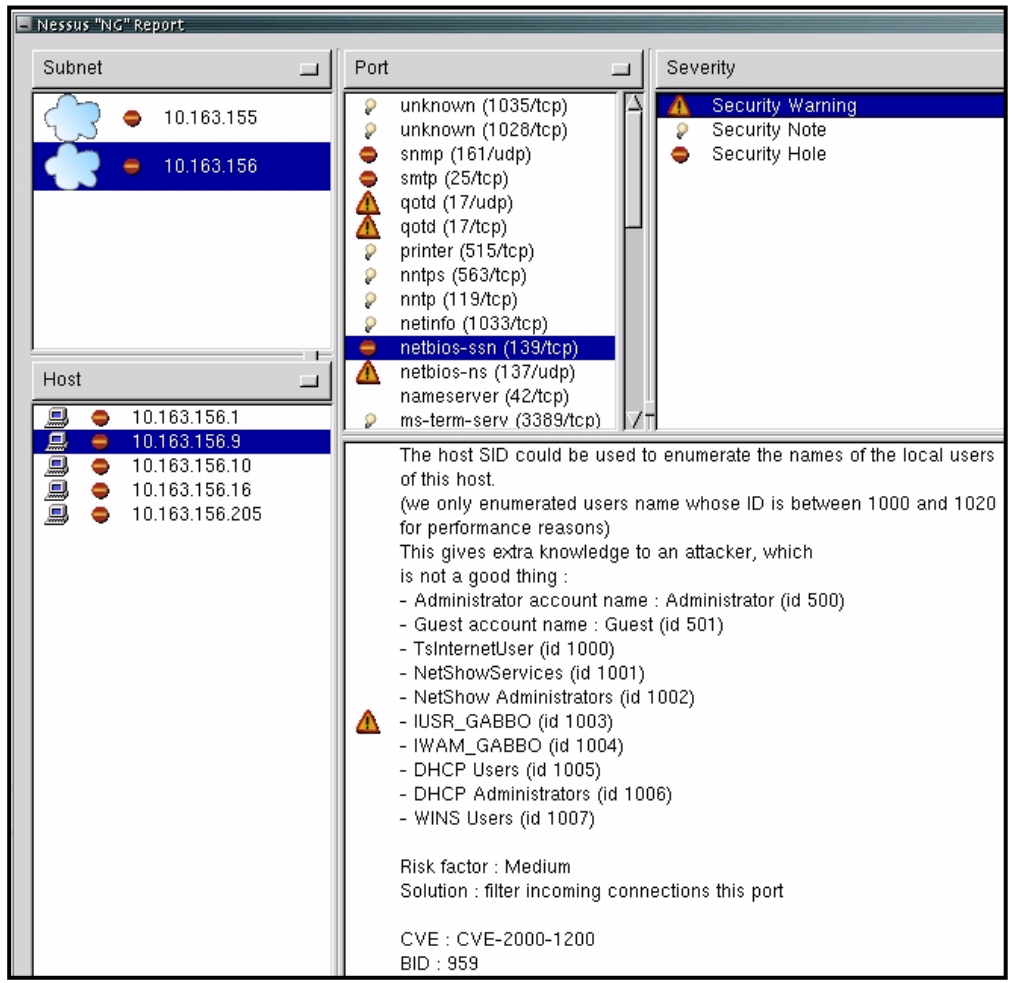
During My Coffee Break



- Use sniffers to map network and addressing schemes
- Selectively scans network for exploitable services
- Finds unauthenticated network share on gaming server
- Next logon causes root kit and Secure Shell (SSH) server installation
- With hidden remote access, on occasion Milton logs in and changes the gameplay
- “That will teach you!”

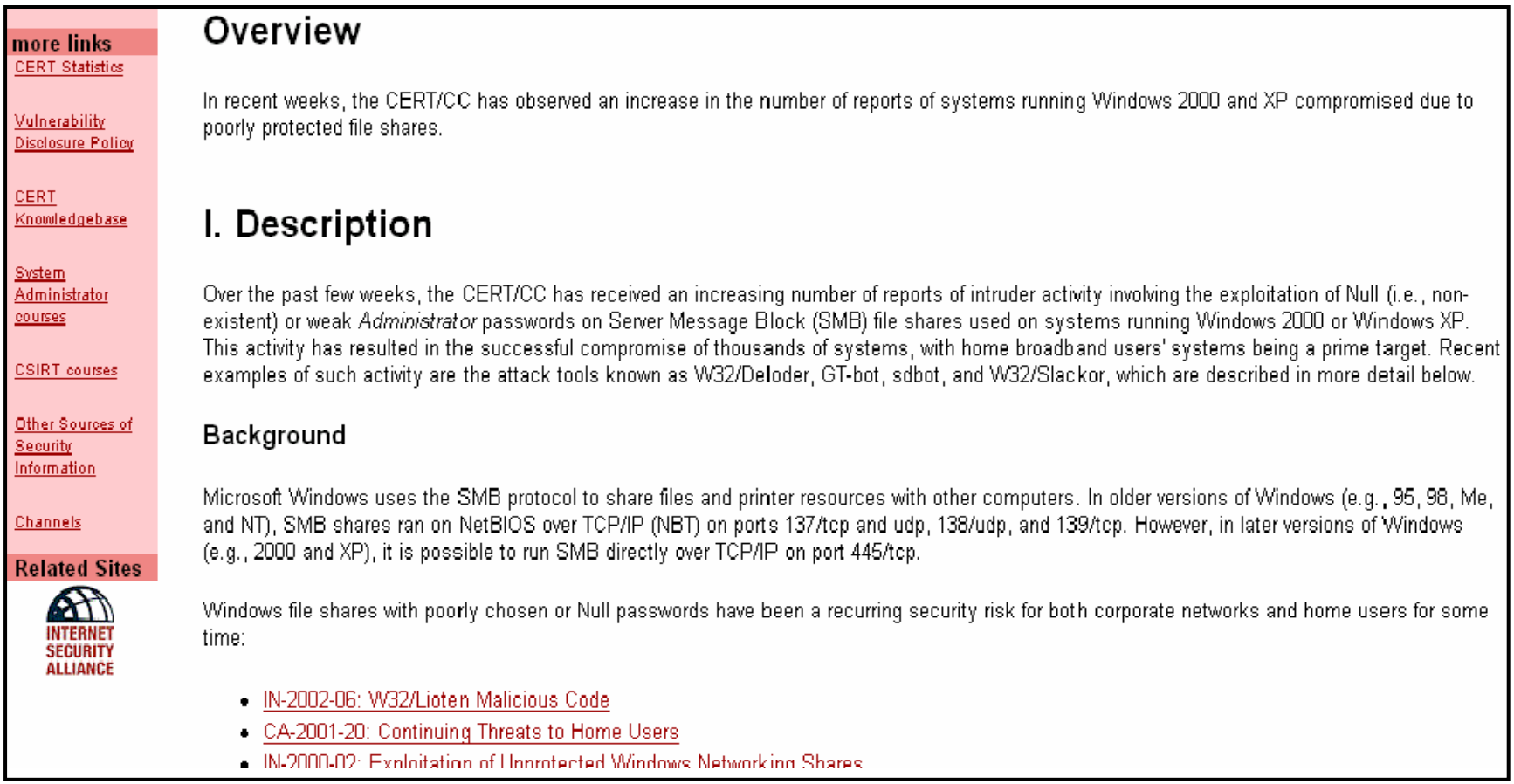
Nessus

- **Vulnerability assessment**
  - **Plug-ins supported**
  - **Any-port inspection**
  - **Custom script/C language**
  - **Updated daily**
  - **Client/server model**
  - **Smart assessing**
  - **Reporting**
  - **SSL/certificate support**
  - **“Non-destructive” mode**
  - **http://www.nessus.org**



CERT® Advisory CA-2003-08
Increased Activity Targeting Windows Shares

- **Also, SANS W4: Unprotected Windows Networking Shares and SANS W5: Anonymous Logon—Null Sessions**



more links
CERT Statistics
Vulnerability Disclosure Policy
CERT Knowledgebase
System Administrator courses
CSIRT courses
Other Sources of Security Information
Channels
Related Sites
INTERNET SECURITY ALLIANCE

Overview

In recent weeks, the CERT/CC has observed an increase in the number of reports of systems running Windows 2000 and XP compromised due to poorly protected file shares.

I. Description

Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak *Administrator* passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor, which are described in more detail below.

Background

Microsoft Windows uses the SMB protocol to share files and printer resources with other computers. In older versions of Windows (e.g., 95, 98, Me, and NT), SMB shares ran on NetBIOS over TCP/IP (NBT) on ports 137/tcp and udp, 138/udp, and 139/tcp. However, in later versions of Windows (e.g., 2000 and XP), it is possible to run SMB directly over TCP/IP on port 445/tcp.

Windows file shares with poorly chosen or Null passwords have been a recurring security risk for both corporate networks and home users for some time:

- IN-2002-06: W32/Lioten Malicious Code
- CA-2001-20: Continuing Threats to Home Users
- IN-2000-02: Exploitation of Unprotected Windows Networking Shares

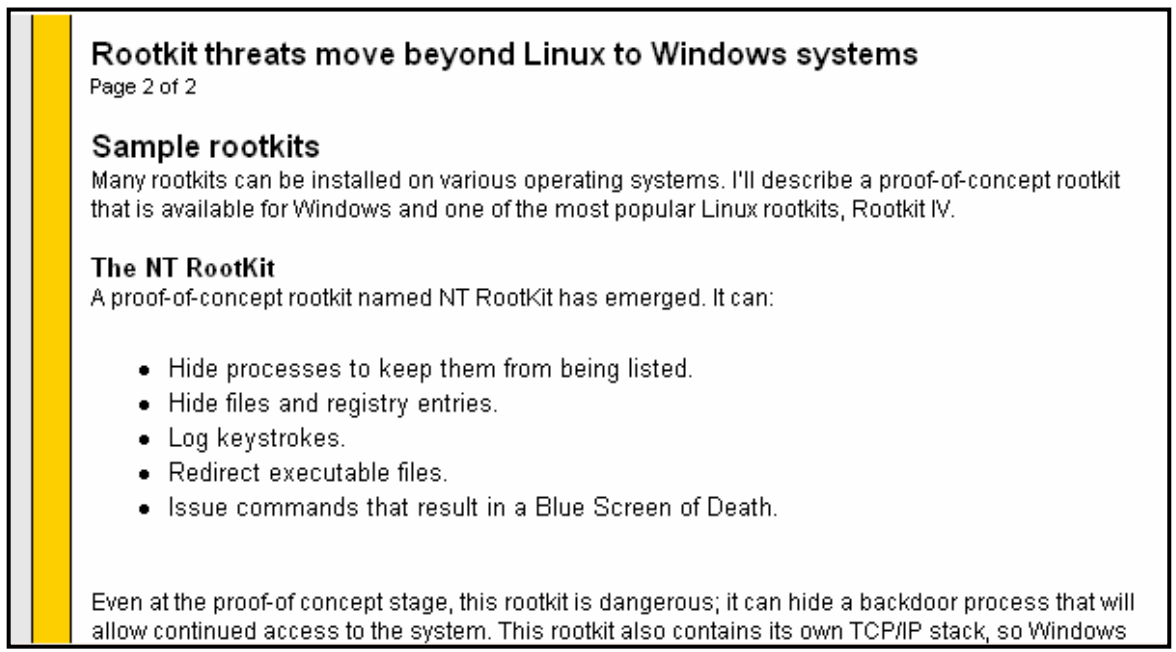
Newer Root Kits

- **The "NT Root Kit":**

  http://www.megasecurity.org/Tools/Nt_rootkit_all.html

- **Propagated by W32/Lioten in December, 2002**

  CERT IN-2002-06



Rootkit threats move beyond Linux to Windows systems

Page 2 of 2

Sample rootkits

Many rootkits can be installed on various operating systems. I'll describe a proof-of-concept rootkit that is available for Windows and one of the most popular Linux rootkits, Rootkit IV.

The NT RootKit

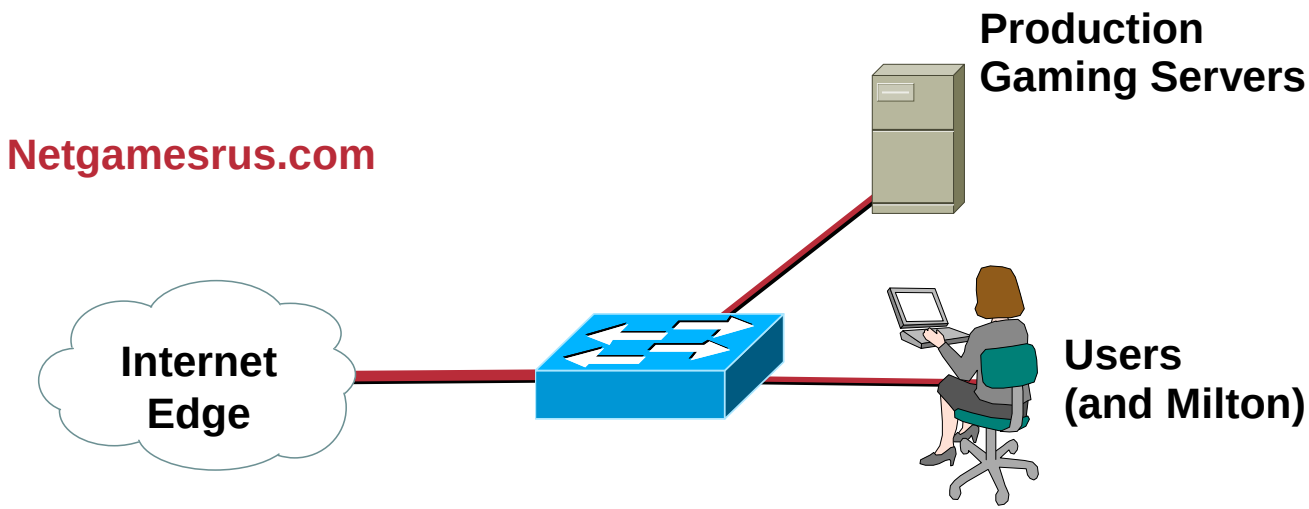
A proof-of-concept rootkit named NT RootKit has emerged. It can:

- Hide processes to keep them from being listed.
- Hide files and registry entries.
- Log keystrokes.
- Redirect executable files.
- Issue commands that result in a Blue Screen of Death.

Even at the proof-of concept stage, this rootkit is dangerous; it can hide a backdoor process that will allow continued access to the system. This rootkit also contains its own TCP/IP stack, so Windows

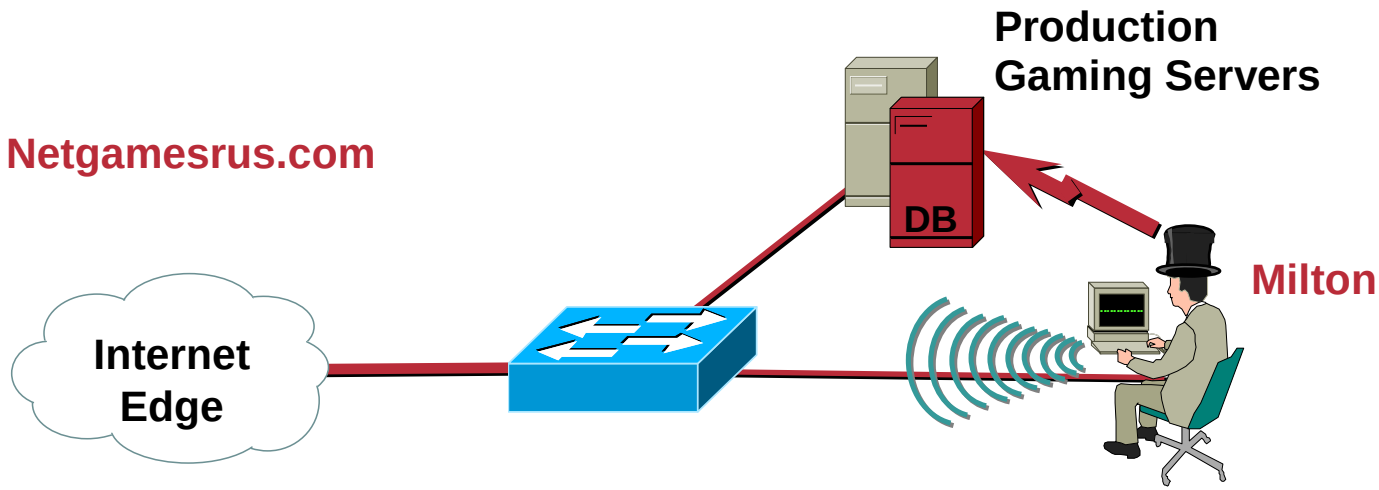
Source: http://asia.cnet.com/itmanager/tech/0,39006407,39100842-2,00.htm

Startups Have Plenty of Bugs



- Players complain about game hickups
- The developers chalk up the errant game play to a bug and spend days debugging the software
  - Eventually they notice erratic file access and discover the NT root kit while debugging
- The administration staff turns off shares after finding remnant root kit installs and enforces authenticated account access and logging

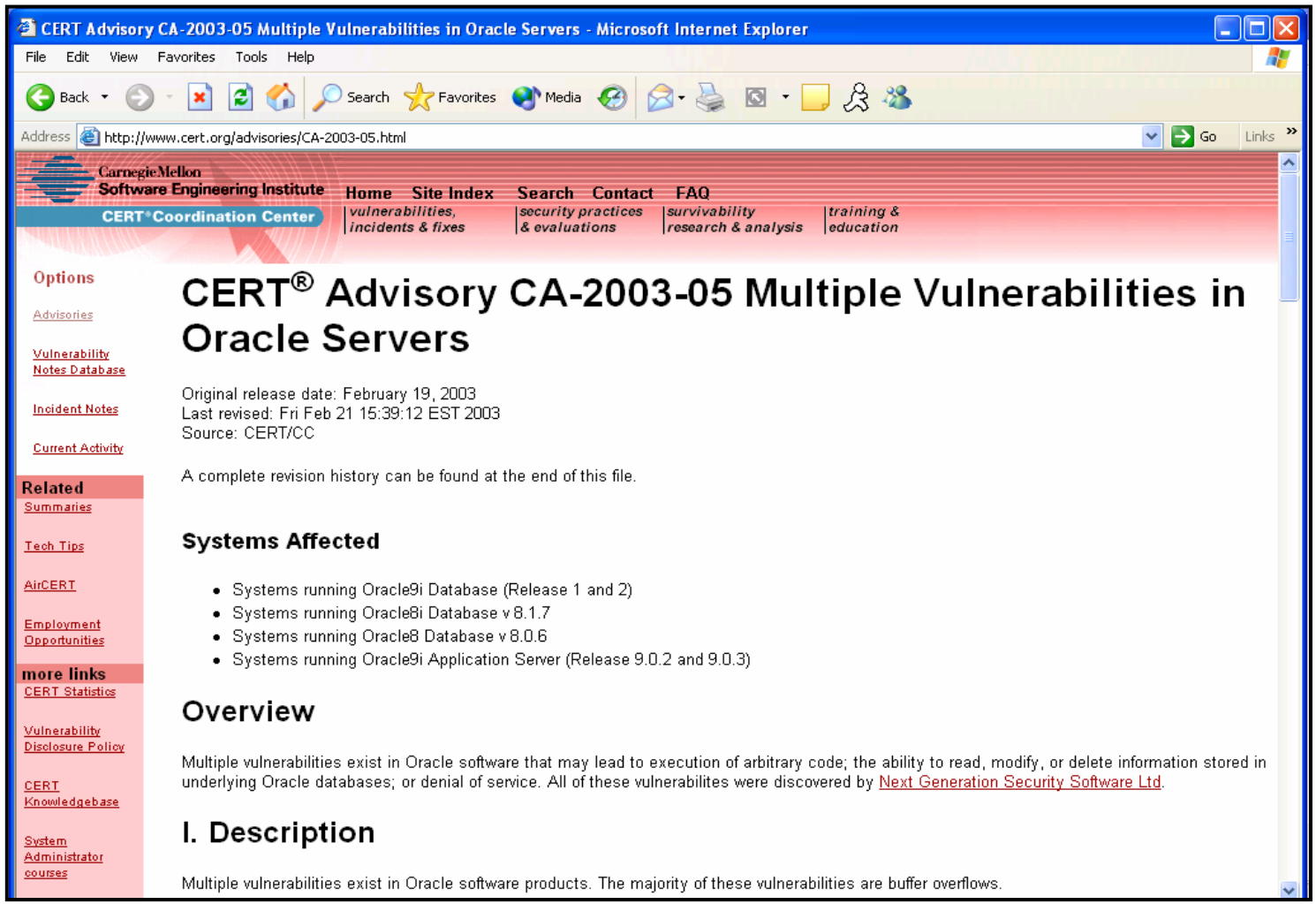
Hey, What Happened?



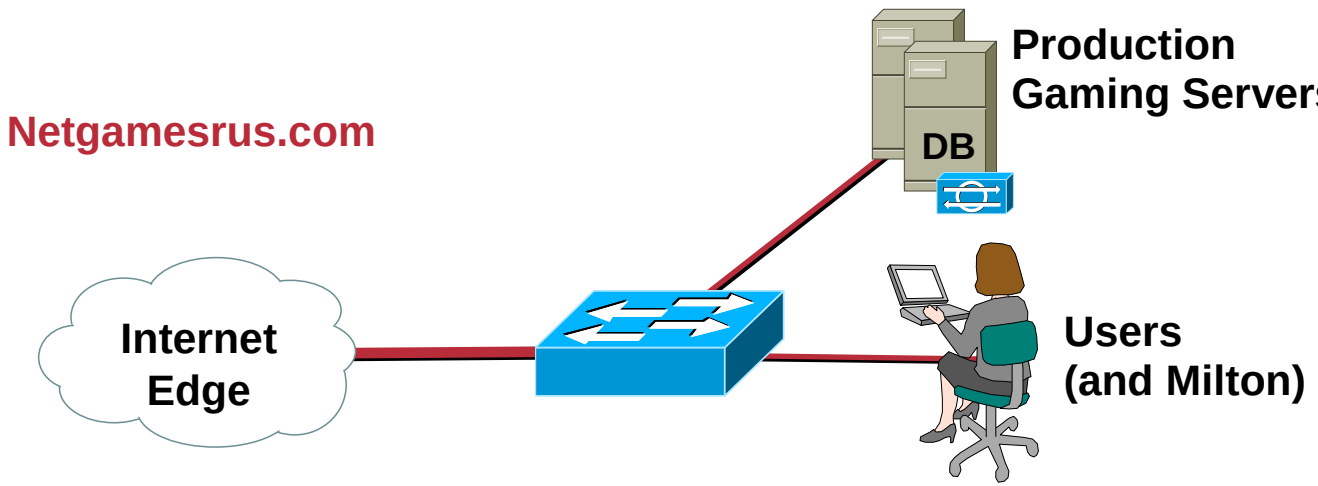
- What happened to “my” system?
- Attempts to exploit file share and learned accounts but fails
- Time to switch gears!
- Scans server segment for additional vulnerabilities and finds a vulnerable Oracle database server
- Via buffer overflow installs root kit and SSH server again, clean logs
- This time removes all game data, Milton is glad he’s not in game support!

CERT® Advisory CA-2003-05
Multiple Vulnerabilities in Oracle Servers

Cisco.com



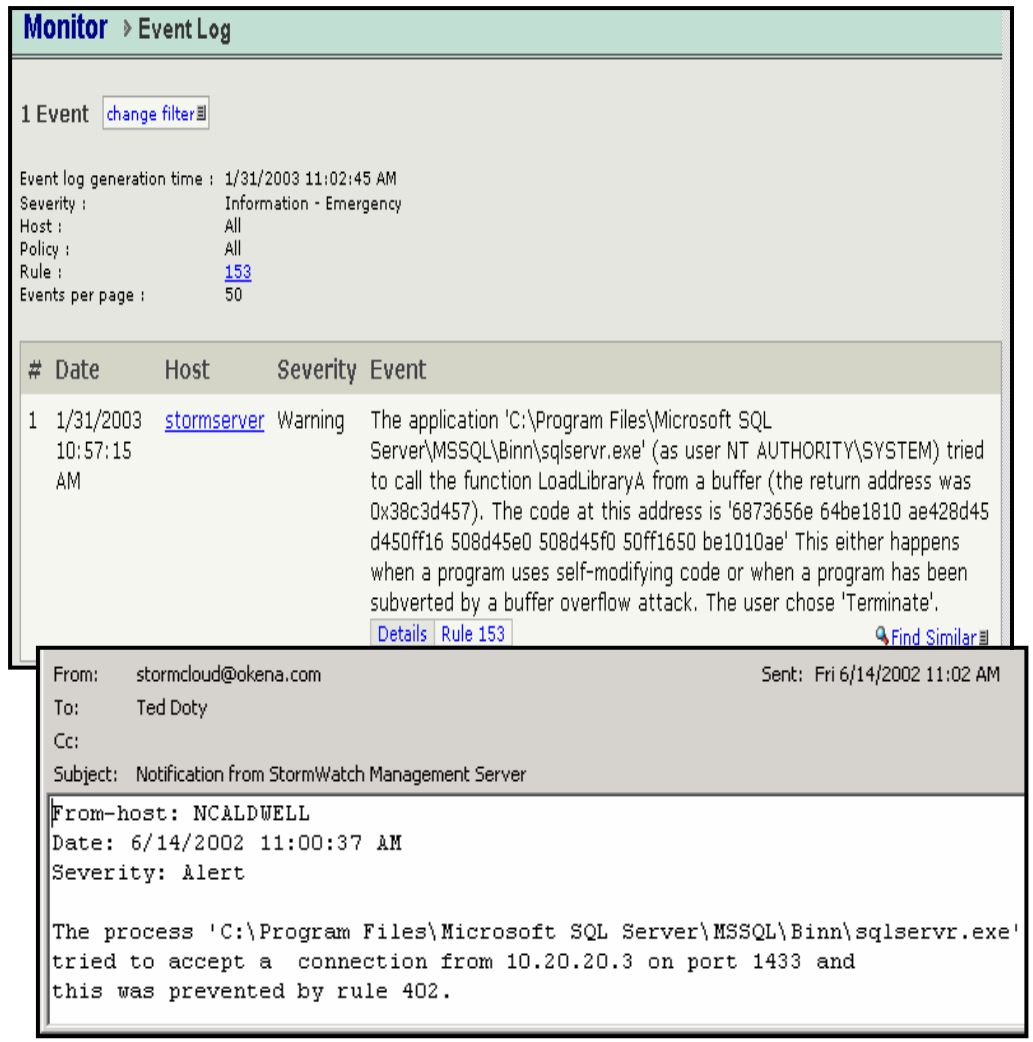
Time to Get Serious



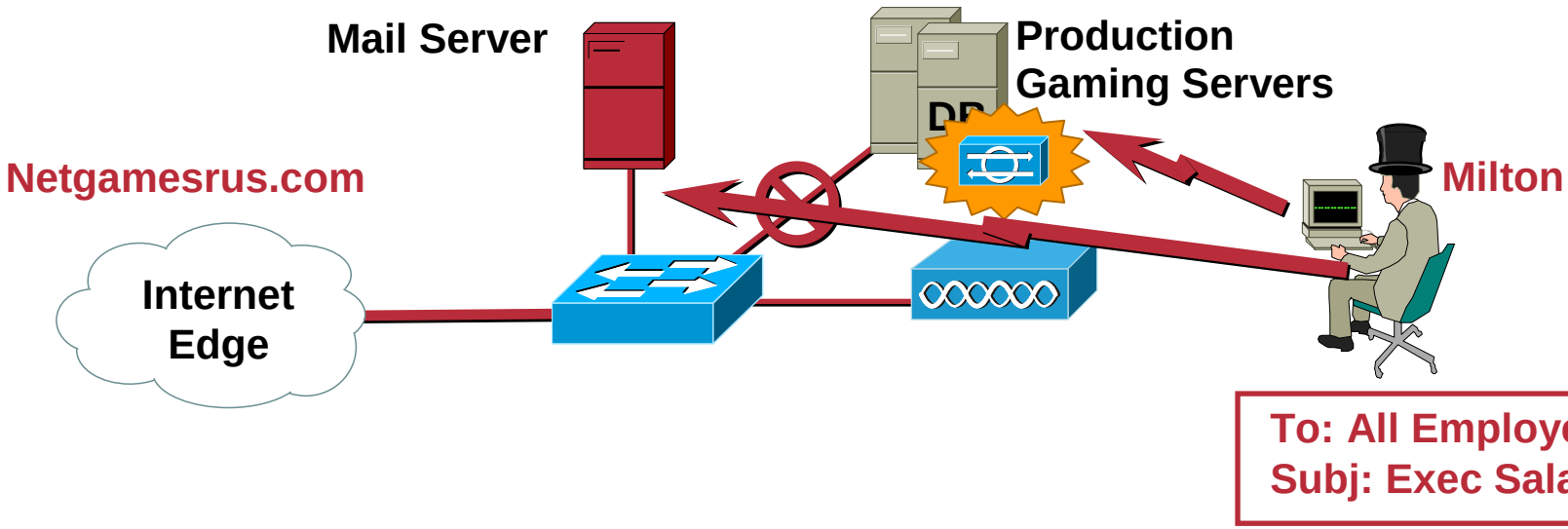
- What happened this time?
- Administration staff investigates and finds their Oracle server vulnerable to multiple exploits
- They then fix and rebuild the gaming servers (thank goodness for tape backup!) as well as turn off unneeded services
- As an added precaution, they install anti-virus throughout the campus and additionally Host-based Intrusion Prevention Systems (HIPS) on the gaming servers
- This must be a hacker on the Internet!

Host Intrusion Prevention (Detection)

- **Host IDS is best installed first on key servers**
- **Features vary per product, including watching for:**
  - **File system**
  - **Process table**
  - **I/O**
  - **System resource usage**
  - **Memory allocation**
- **Actions include alarm and sometimes prevent**
- **Financially and operationally impractical to install on all hosts**



The Inside Line



- **Milton attempts a SSH session over the WLAN using a spoofed MAC address to "hide" his attack but is unsuccessful**

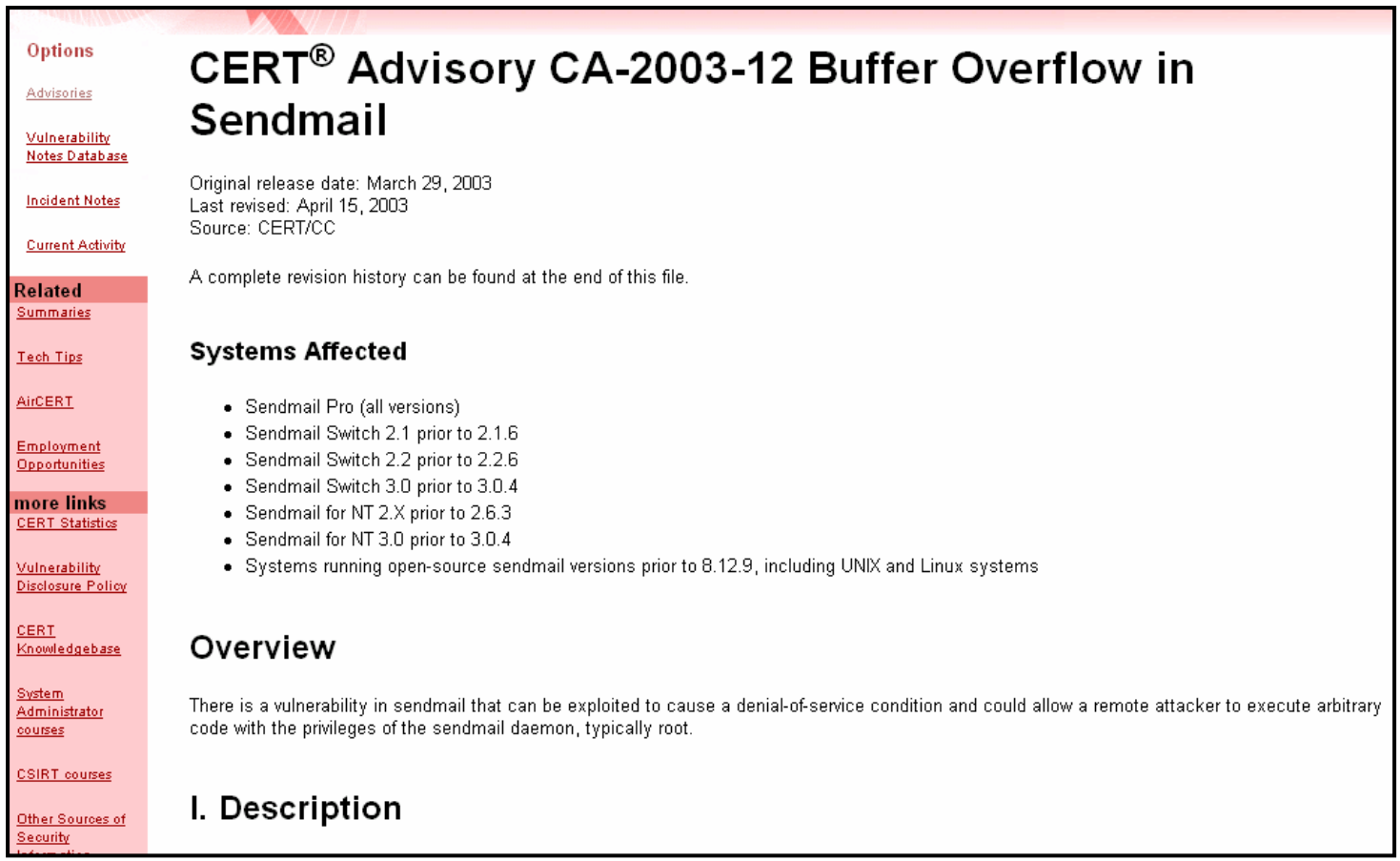
  Rats! No SSH server!

- **He runs another scan, more broadly this time, and finds another vulnerable server, this time the email server**
- **Compromises the server and finds interesting email which he forwards it to everyone in the entire company**

CERT® Advisory CA-2003-12
Buffer Overflow in Sendmail

Cisco.com

Also SANS U8: Sendmail



Options

Advisories

Vulnerability Notes Database

Incident Notes

Current Activity

Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CSIRT courses

Other Sources of Security

CERT® Advisory CA-2003-12 Buffer Overflow in Sendmail

Original release date: March 29, 2003
Last revised: April 15, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sendmail Pro (all versions)
- Sendmail Switch 2.1 prior to 2.1.6
- Sendmail Switch 2.2 prior to 2.2.6
- Sendmail Switch 3.0 prior to 3.0.4
- Sendmail for NT 2.X prior to 2.6.3
- Sendmail for NT 3.0 prior to 3.0.4
- Systems running open-source sendmail versions prior to 8.12.9, including UNIX and Linux systems

Overview

There is a vulnerability in sendmail that can be exploited to cause a denial-of-service condition and could allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon, typically root.

I. Description

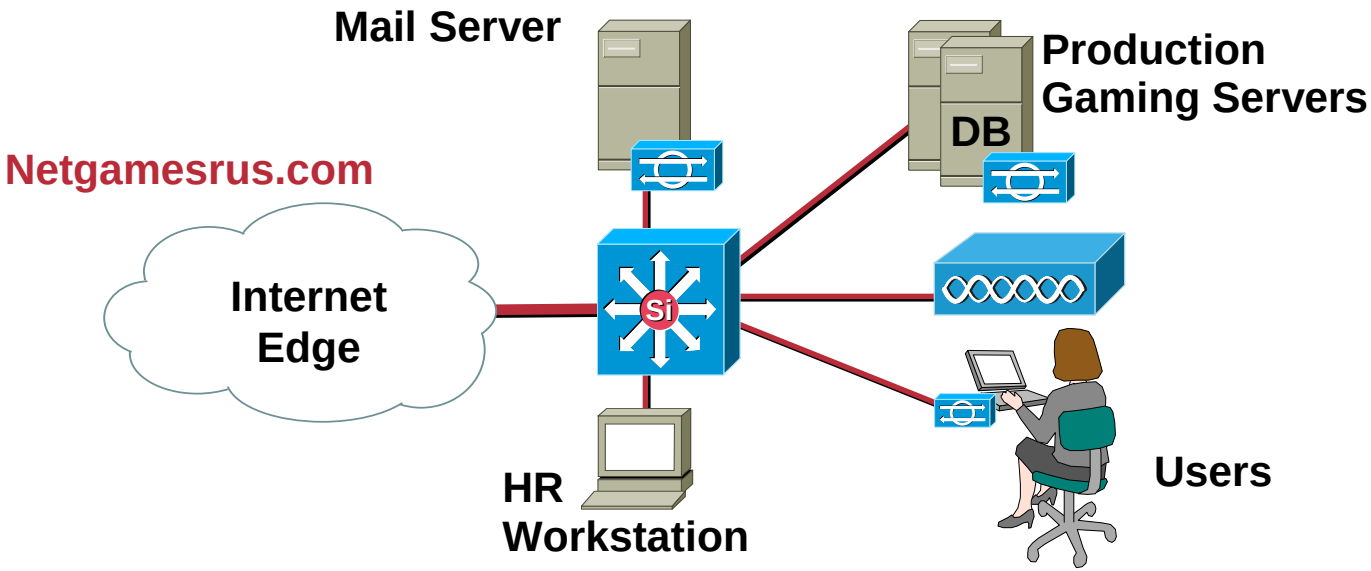
802.11b Is Insecure

- **Even though this is an inside job, WEP still has "issues"**
  - **Security of the WEP Algorithm:**
    http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
  - **Your 802.11 Wireless Network has No Clothes:**
    http://www.cs.umd.edu/~waa/wireless.pdf
  - **Weaknesses in the Key Scheduling Algorithm of RC4:**
    http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps
  - **Using the Fluhrer, Mantin, and Shamir Attack to Break WEP:**
    http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf
  - **Practical implementations of the attacks:**
    http://airsnort.sourceforge.net/
    http://wepcrack.sourceforge.net/
- **Even if WEP were secure (which it's not), the standard makes no provisions for key distribution or management**
  - **Hence WPA**

Airsnort

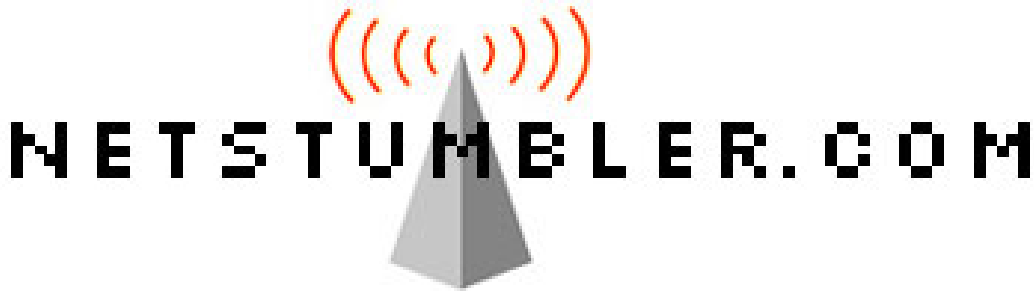
- Easy to use exploit of the “Fluhrer” defined weakness
- Requires 5-10 million WEP encrypted packets
- Guesses the WEP key in under a second

Are You Threatening Me?



- IT is wising up but becoming more concerned at the same time
- Email sent from the server itself???
- Source of scan against DB traced to WLAN to unknown NIC
  - IDS logged the connection attempt
  - Were we hacked from the parking-lot???
- Enable WPA on WLAN infrastructure (PEAP) to mitigate the parking-lot threat
  - Scan for policy violators
- Decide to enforce segmentation between the business functions on the LAN
  - Dedicated routed segments created for users, administrators, production servers, and IP phones

Drive-By Hacking



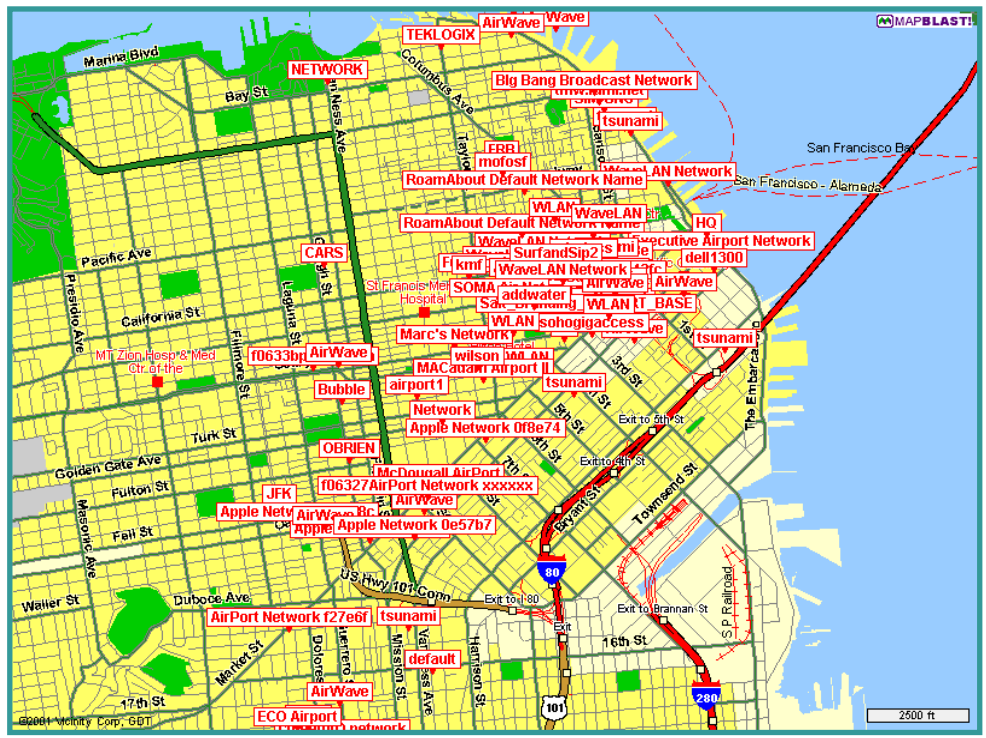
- **Identifies WLAN details (SSID, AP MAC, use of WEP)**
- **Links directly to GPS to give AP location**
- **Can convert into Streetmap.co.uk format using:**

http://www.interrorem.com/software/stumbler.php3

Drive-By Hacking

…is possible as it has been proven by "War Driving" exercises in San Francisco and Other Major Cities:

- **Cruising with a car + laptop + WLAN card**
- **+ GPS scanning for (unprotected) 802.11 wireless networks**
- **+ PERL script to log the SSID, AP's MAC address, best S/N ratio and location (GPS)**



NETSTUMBLER.COM

www.personaltelco.net/index.cgi/WarDriving

Long Distance Hacking

"Over a clear line of sight, with short antenna cable runs, a 12db to 12db can-to-can shot should be able to carry an 11Mbps link well over ten miles."

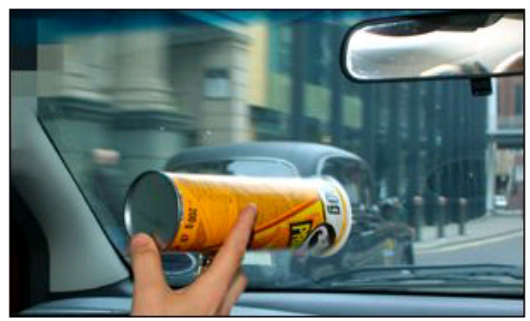
Rob Flickenger, O'Reilly Systems Administrator

- **"Pringles" YAGI antenna**
  - **Cost: $10**
  - **Range: 10 miles**

Moral: Don't rely on physical isolation!

Friday, 8 March, 2002, 09:23 GMT

Hacking with a Pringles tube



A crisp can is an effective tool for curious hackers

http://www.oreillynet.com/cs/weblog/view/wlg/448

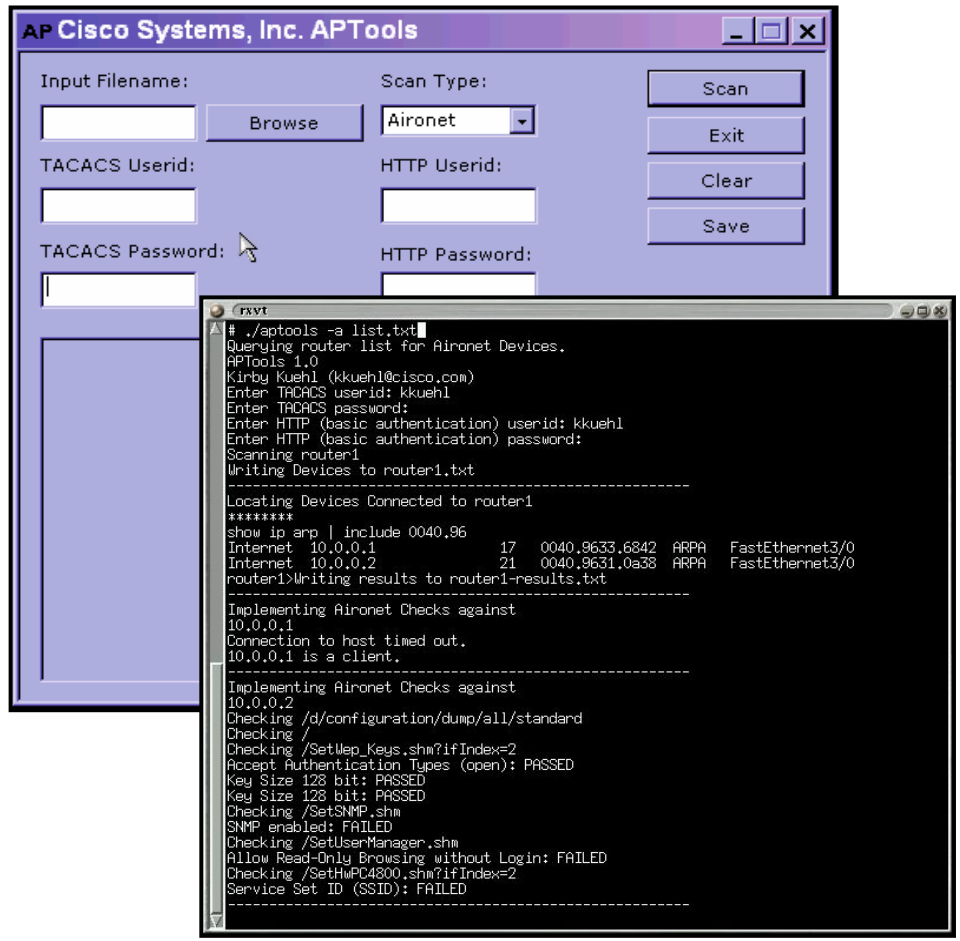
Rogue AP Detection

802.11b detection methods:

- Physical, MAC observation
- Fingerprinting (NMAP, Xprobe)
- 802.11b analyzer (War Driving, other APs)
- SNMP
- 802.1x
- Wireless analyzers
- MAC monitoring (APTools)

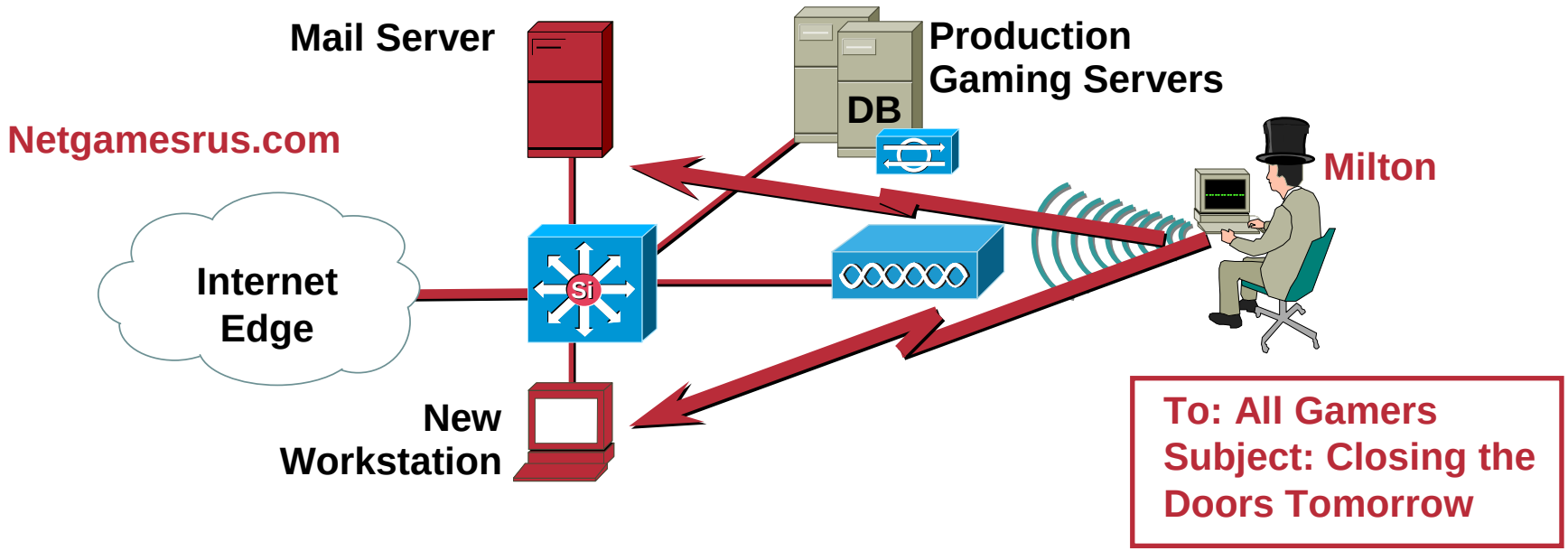
APTools:

- Query routers and switches ARP tables, also NMAP input
- Identifies APs through IEEE OUI and Company_id Assignments
- Audit APs settings
- HTTP basic authentication support



http://winfingerprint.sourceforge.net/aptools.php

My Way or the Highway



- With PEAP enabled Milton can no longer use his own account for WLAN hacking, then again, why bother?
- From a rogue PC on the intranet uses multiple tools (Dsniff, root kits, LC4) to capture user and insecure in-band administration traffic, right off the switch, including usernames and passwords
- Logs into mail server and creates system-wide notification to all gamers

Dsniff Is Not Your Friend

- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH/SSL interception

Dug Song, Author of Dsniff

www.monkey.org/~dugsong/dsniff

SANS W6: Weak Password Hashing

Cisco.com

W6 LAN Manager Authentication -- Weak LM Hashing

W6.1 Description

Although most current Windows environments have no need for LAN Manager (LM) support, Microsoft locally stores legacy LM password hashes (also known as LANMAN hashes) by default on Windows NT, 2000 and XP systems. Since LM uses a much weaker encryption scheme than more current Microsoft approaches (NTLM and NTLMv2), LM passwords can be broken in a very short period of time. Even passwords that otherwise would be considered "strong" can be cracked by brute-force in under a week on current hardware.

The weakness of LM hashes derives from the following:

- Passwords are truncated to 14 characters.
- Passwords are padded with spaces to become 14 characters.
- Passwords are converted to all upper case characters.
- Passwords are split into two seven character pieces.

This hashing process means that an attacker needs only to complete the trivial task of cracking two seven-character, upper-case passwords to gain authenticated access to your system. Since the complexity of cracking hashes increases geometrically with the length of the hash, each seven-character string is at least an order of magnitude simpler to attack by brute-force than would a combined fourteen-character string. Since all strings are exactly seven characters (including spaces) and entirely upper-case, a dictionary-style attack is also simplified. The LM hashing method therefore completely undermines good password policies.

In addition to the risk posed by having legacy LM hashes stored in the SAM, the LAN Manager authentication process is often by default enabled on clients and accepted by servers. As a result, Windows machines capable of utilizing stronger hash algorithms instead send weak LM hashes across the network, making Windows authentication vulnerable to eavesdropping by packet sniffing, and therefore easing the efforts of an attacker to obtain and crack user passwords.

W6.2 Operating Systems Affected

All Microsoft Windows operating systems.

W6.3 CVE Entries

N/A

SANS W7 and U10: No or Weak Passwords

Cisco.com

W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords

W7.1 Description

Passwords, passphrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perha
accounts with bad or empty passwords
password policy far too rare.

The most common password vulnerabili
passwords, (b) regardless of the stren
operating system or additional softwar
passwords, and (d) password hashing
that they are visible by anyone. The b
password policy which includes thorou
checking of password integrity.

W7.2 Operating Systems Affected

Any operating system or application wh

W7.3 CVE Entries

CAN-1999-0506, CAN-1999-0504, CVE

U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

U10.1 Description

Passwords, passphrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even root. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy far too rare.

The most common password vulnerabilities are that (a) user accounts have weak or nonexistent passwords, (b) regardless of the strength of their password, users fail to protect it, (c) the operating system or additional software creates administrative accounts with weak or nonexistent passwords, and (d) password hashing algorithms are known and often hashes are stored such that they are visible by anyone. The best and most appropriate defense against these is a strong password policy which includes thorough instructions for good password habits and proactive checking of password integrity.

U10.2 Operating Systems Affected

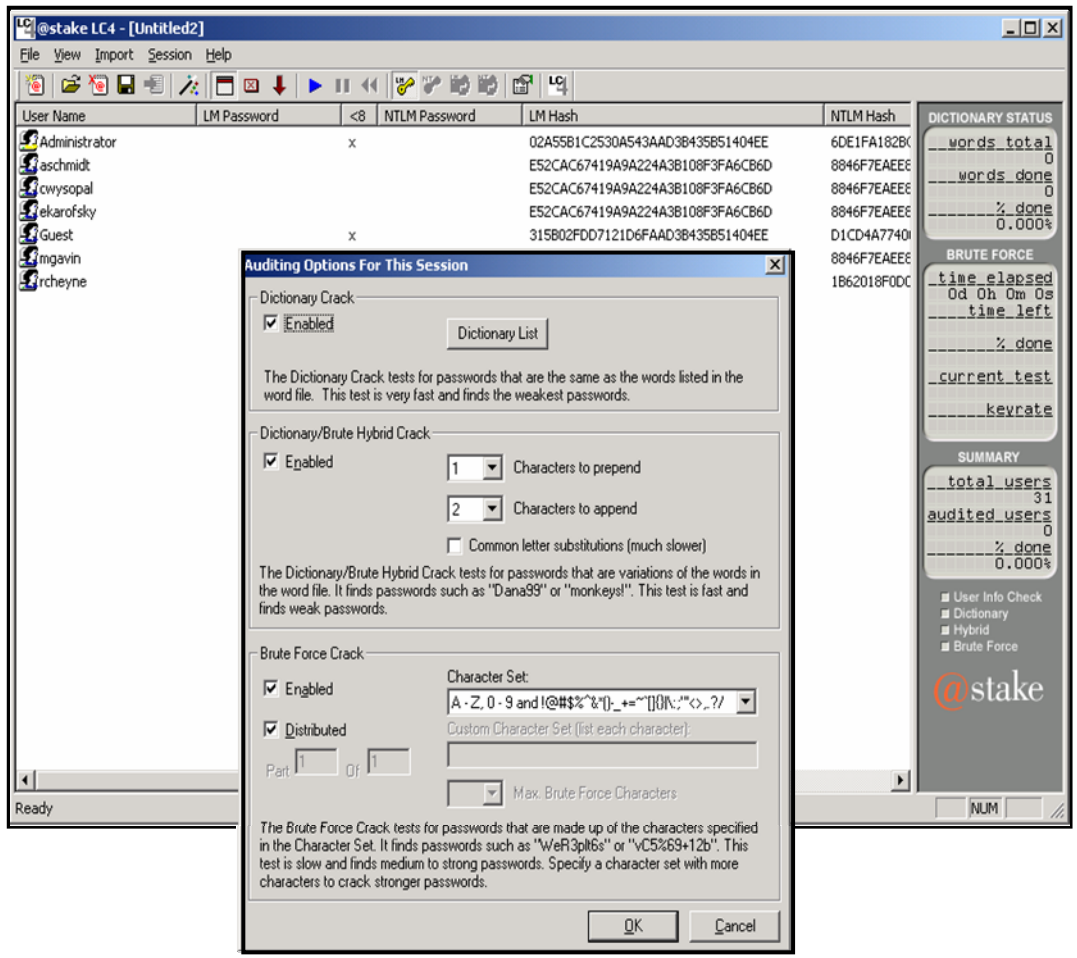
Any operating system or application where users authenticate via a user ID and password.

U10.3 CVE Entries

CVE-1999-0502

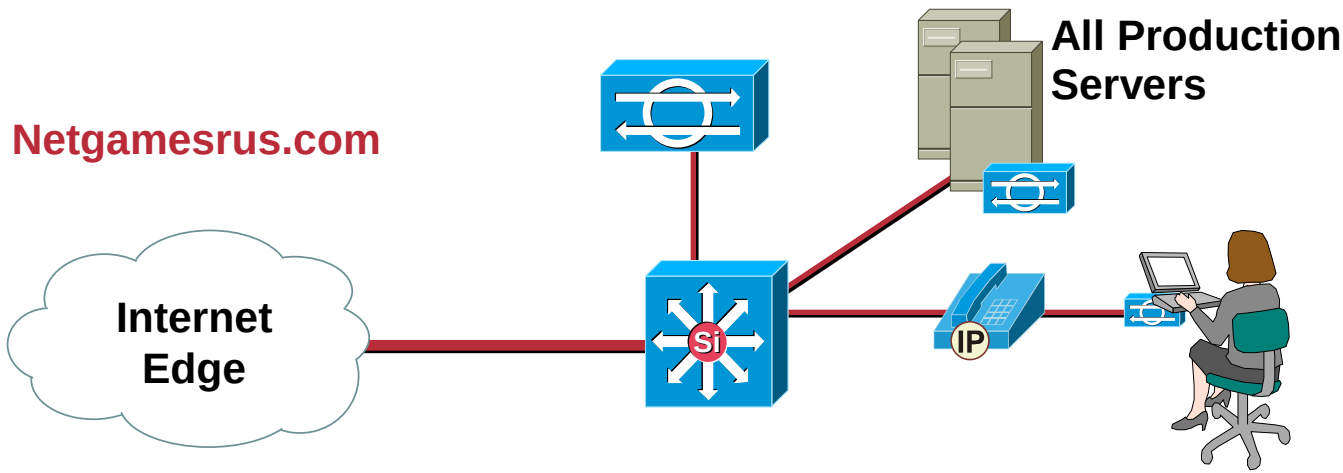
LC4 (aka l0phtcrack)

- **Password auditing/recovery**
  - **Finds weak passwords**
  - **Sampling found 18% in 10 minutes, 90% in 48 hours**
  - **Takes network input or encrypted stores**
  - **Dictionary, brute-force, and hybrid cracking support**
  - **Reporting shows time required to crack**



http://www.atstake.com/research/lc/

Under New Management



- **After bogus email sent some staffing and operational changes occur**
  - **Network IDS (NIDS) is deployed to inspect gaming server segment**
  - **Access control server (aka AAA) deployed to centrally manage management accounts, One-Time-Passwords (OTPs) considered**
  - **Audit all account passwords**
  - **Secure in-band management (SSH/SSL) adopted**

Management Channel Security

- **In-band in the clear**
  - **Optionally with strong authentication**
- **In-band secured**
  - **Application layer encryption (SSH, SSL)**
  - **Network layer encryption (IPsec)**
    - **Good for non-configuration protocols**
      - **Syslog, TFTP, SNMP**
- **Out-of-band management**
  - **Strongest security**
  - **Beware topology sensitive management systems**

NIDS in High Load Environments

- **NIDS value reduced when packet rate too high due to data loss (NIDS fails open)**
- **Tricks for reducing load include:**
  - **Load balancing multiple NIDS devices**
  - **Layer 3 and 4 pre-screening of data**
  - **Unidirectional, not bi-directional, examination (some signatures do not fire properly)**
- **Beware overly sensitive alarming, don't be overwhelmed**

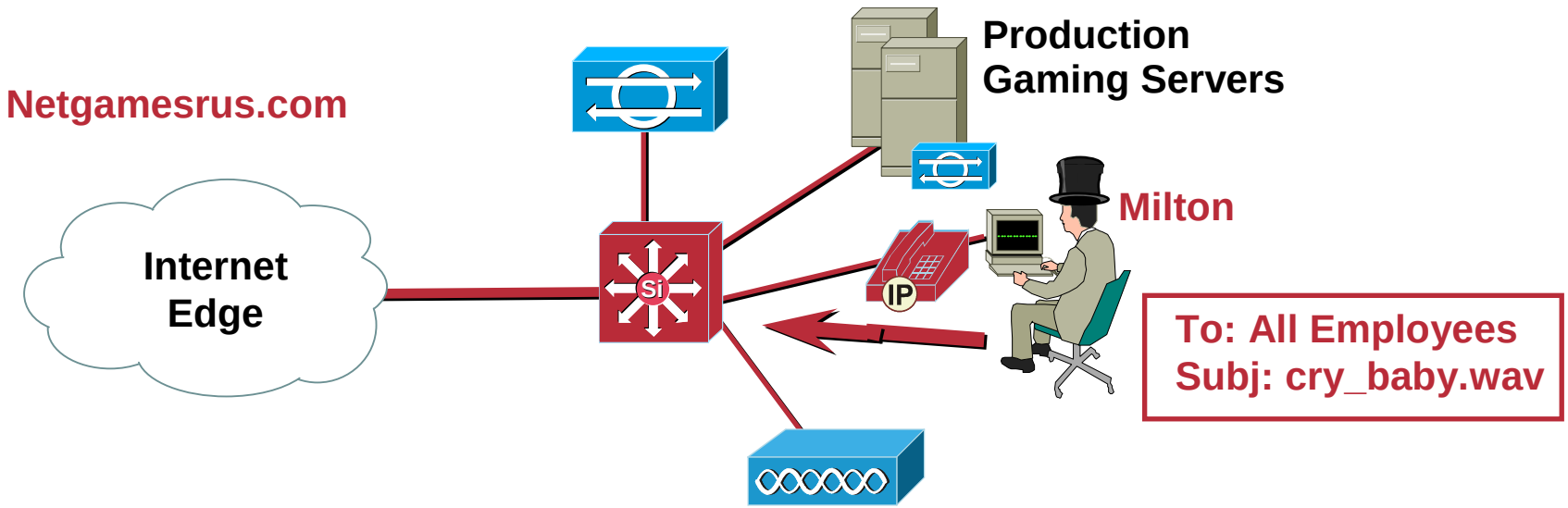
Layer 4 ACLs in Switches

- L4 access control in switches (e.g. CAT6k)
- ASIC/hardware support important for Gigabit environments
- Logging, when available, is unwise at high data rates
  - On a CAT6k performance drops an order of magnitude
- Note access control is stateless
  - Ideal for L3 use
  - L4 multi-channel protocol filtering is hard and insecure (no state tracking)
- Stateful firewalls in switches are now available

One-Time Passwords (OTPs)

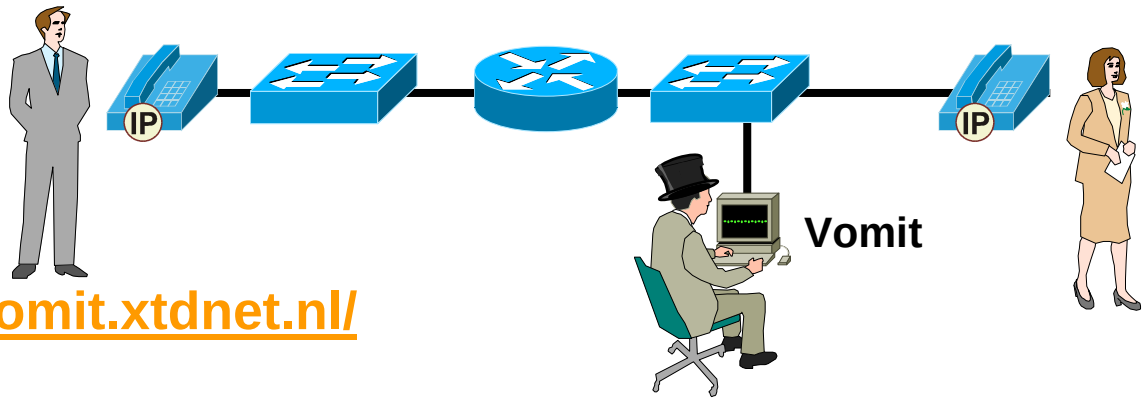
- Commonly used for NAS, device management, and remote access VPNs (don't rely solely on device authentication)
- Mitigate eavesdropping and replay attacks
- Each password only useful once
- Synchronization between authentication server and client
- Agreement may be based on time, sequence, and a PIN
- Software and hardware-based

“And Now for Something Completely Different”



- Milton escalates with Dsniff again, this time in combination with voice tools
- He pulls IP phone conversations off the wire and actually captures a discussion between the CEO and his wife nagging him for working too late
- Sends it to everyone in the company from a free Internet email account

Let's Talk about VOMIT

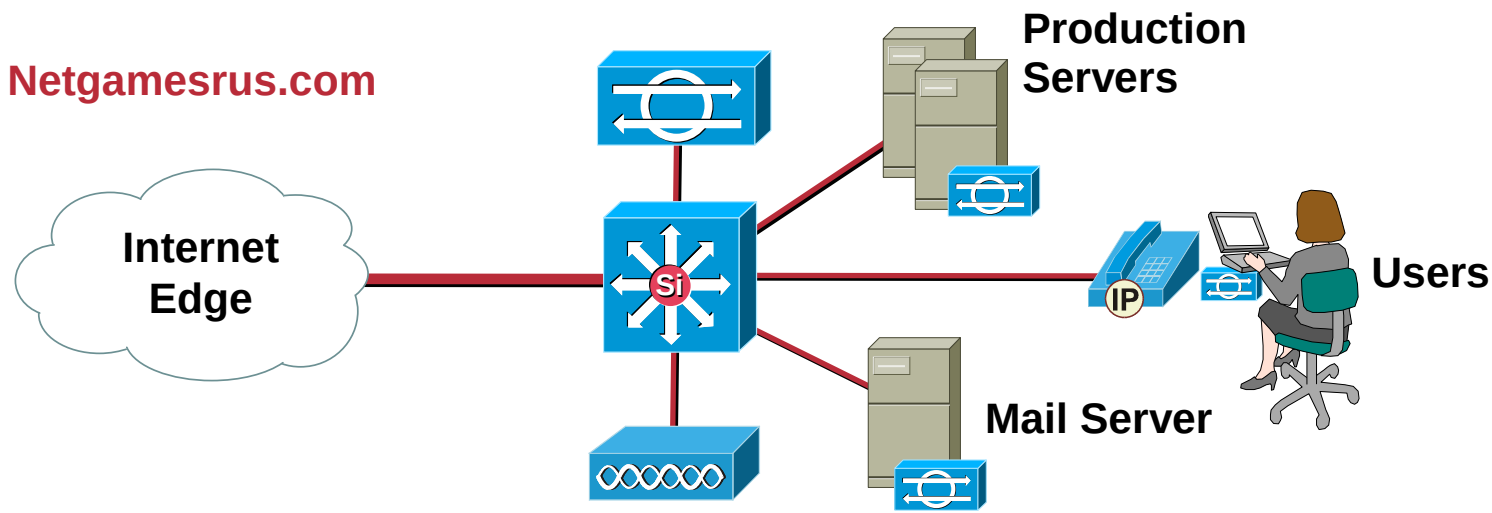


http://vomit.xtdnet.nl/

$ vomit -r phone.dump | waveplay -S8000 -B16 -C1

- **Voice-over-Misconfigured-IP-Telephony (VOMIT)**
  - **Compatible with Cisco IP phones, G.711 codec only**
  - **Man-in-the-middle attack carried out by Dsniff assists in providing a TCPDUMP of the conversation**
  - **VOMIT takes on input the TCPDUMP file and on output generates a WAV file for convenient listening**
  - **Other commercial tools available (e.g. DNA-323) http://www.acterna.com/united_states/Products/data/products_voip.html**

Here We Go Again



- After searching for traditional “bugs” to no avail, research reveals VOMIT and Dsniff
- IT group locks down all switches and routers in the campus
  - L2 lockdown (note change)
- NIDS tuned additionally to inspect all campus VLANs for L2 exploits
- CEO is offered “how to balance your personal life and work” counseling

Layer 2 Security Best Practices 1/2

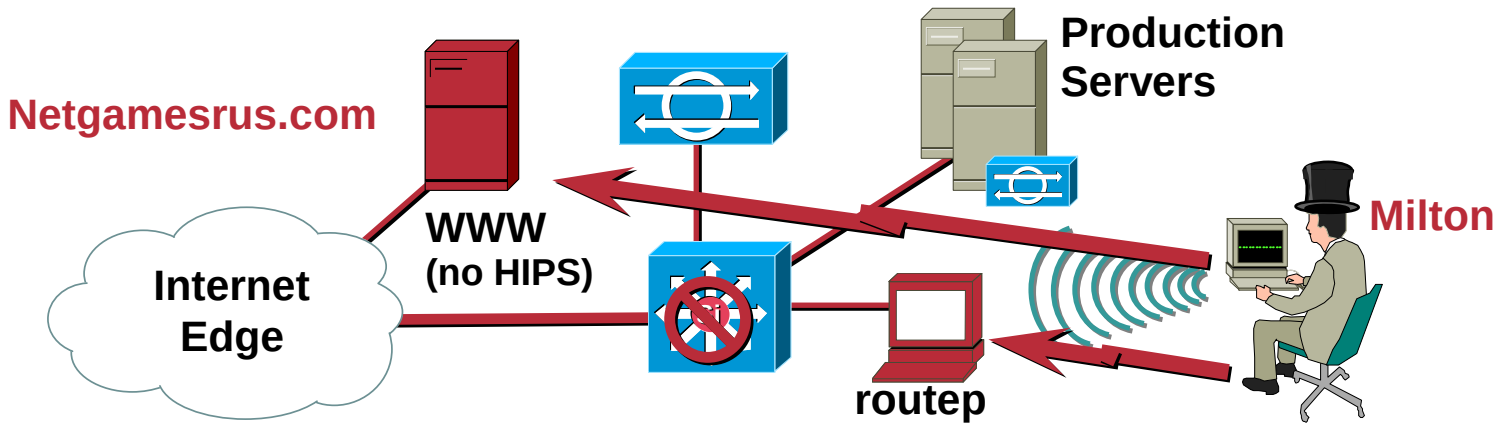
- Manage switches in as secure a manner as possible (SSH, OOB, permit lists, etc.)
- Always use a dedicated VLAN ID for all trunk ports
- Be paranoid: do not use VLAN 1 for anything
- Set all user ports to non trunking
- Deploy port-security where possible for user ports
- Selectively use SNMP and treat community strings like root passwords
- Have a plan for the ARP security issues in your network (ARP inspection, IDS, etc.)

Layer 2 Security Best Practices 2/2

- Enable STP attack mitigation (BPDU Guard, Root Guard)
- Decide what to do about DHCP attacks (DHCP Snooping, VACLs)
- Use private VLANs where appropriate to further divide L2 networks
- Use MD5 authentication for VTP
- Use CDP only where necessary
- Disable all unused ports and put them in an unused VLAN

All of the Preceding Features Are Dependent on Your Own Security Policy

Blasted!



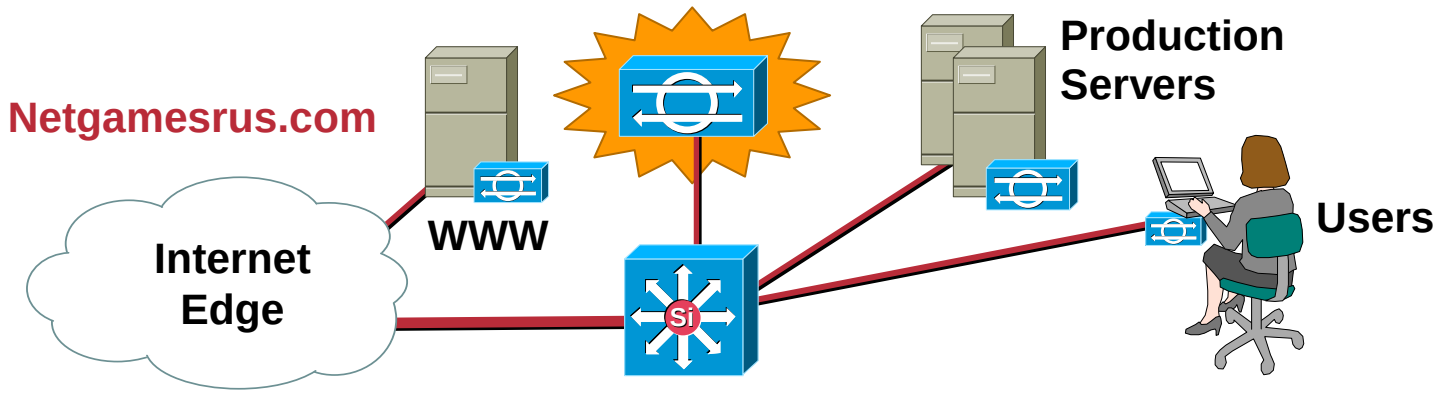
- Milton learns that Dsniff is now inconsequential due to the switch hardening
- He scans yet once again, and finds yet another accessible system—a vulnerable web-server on the Internet DMZ
  - He compromises the web-server and uses its trust relationship with the DB server to acquire customer billing information
  - Milton then installs a custom script called “fetchmydata” that when invoked sends customer billing information to the recipient
  - Milton then finds an accessible (console open) Linux system in the lab and on occasion initiates the routep service to injects bad routes causing network instabilities
  - The IT staff assumes it’s another Code-Red/Nimda worm variant and tells everyone to go home for the day

Beware Where You Store Credentials

Cisco.com

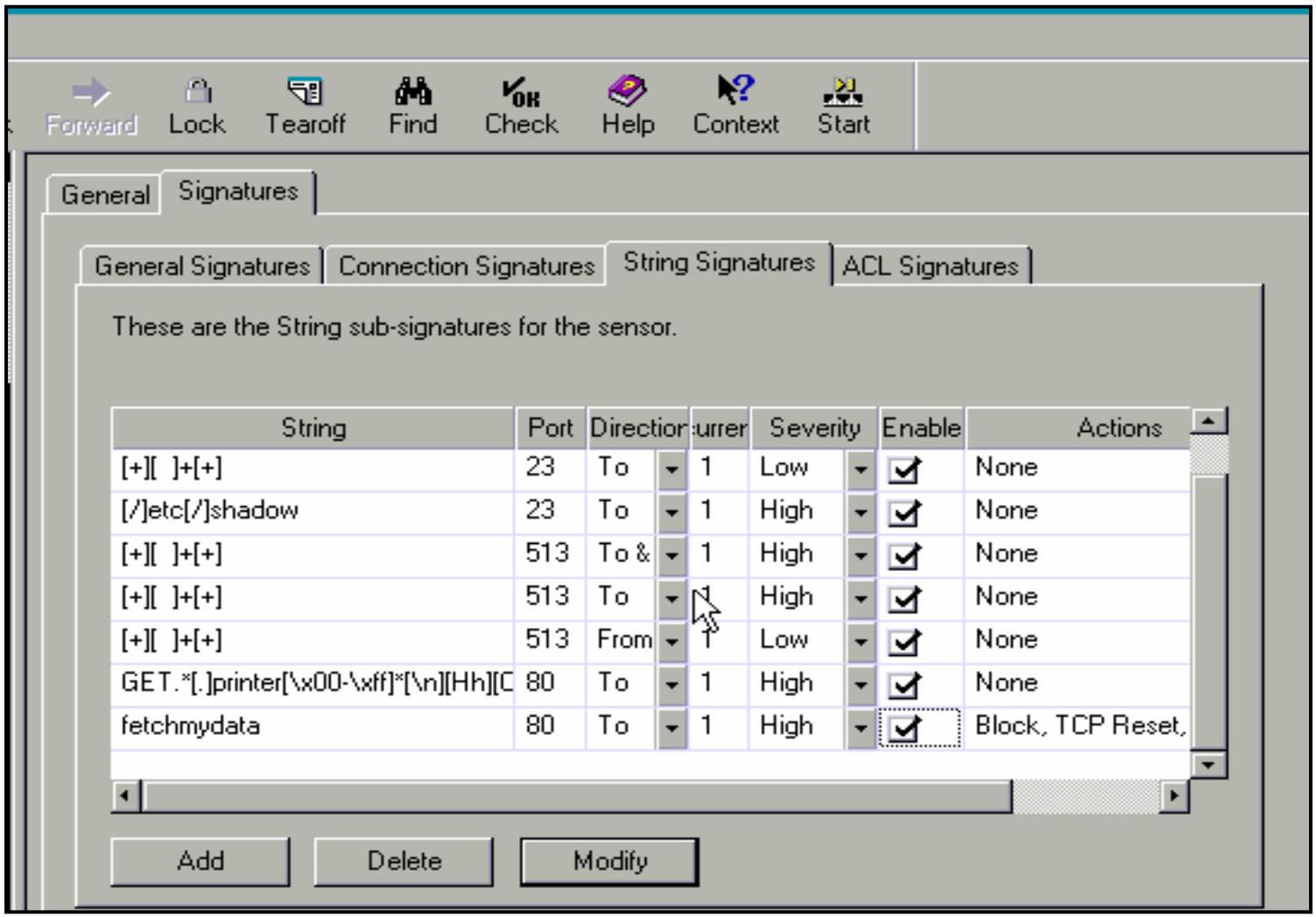
```
…
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
</head>
<body background="_themes/auto/autobkgd.gif" bgcolor="#666666" text="#FFFFFF"
link="#FFCC33" vlink="#CCCC99" alink="#CCCCCC"><!--mstheme--><font face="Arial,
Arial, Helvetica">
<p><img border="0" src="images/pod<%Response.Write
Application("sevt_podnumber")%>.gif" width="640" height="66"></p>
<p>
<%
On Error resume Next
openstr = "DRIVER={SQL Server}; server=192.168.0.10;
database=pubs;UID=pubs;PWD=password"
Set cn = Server.CreateObject("ADODB.Connection")
cn.Open openstr
sql = "SELECT sum(qty) FROM buys; "
…
```

Not Bad



- **NIDS fires, Dsniff mitigated, but strange charges appear on customer's credit cards**
  - **L2 trace finds uncontrolled desktop, IT decides to deploy 802.1X**
  - **DB log check shows recent access from web-server for compromised accounts; in response the system is patched, HIPS is installed, and a custom NIDS signature is deployed searching for "fetchmydata;" finally, host logging is enabled**
- **Administrators determine no-such worm was spreading**
  - **Look into routing protocol neighbor logs and eventually locate rogue router, enable authentication of routing protocol**
  - **Now more clear than ever this is an inside job, install keyboard loggers on all desktops and servers—two can play that game!**

Custom SQL NIDS String

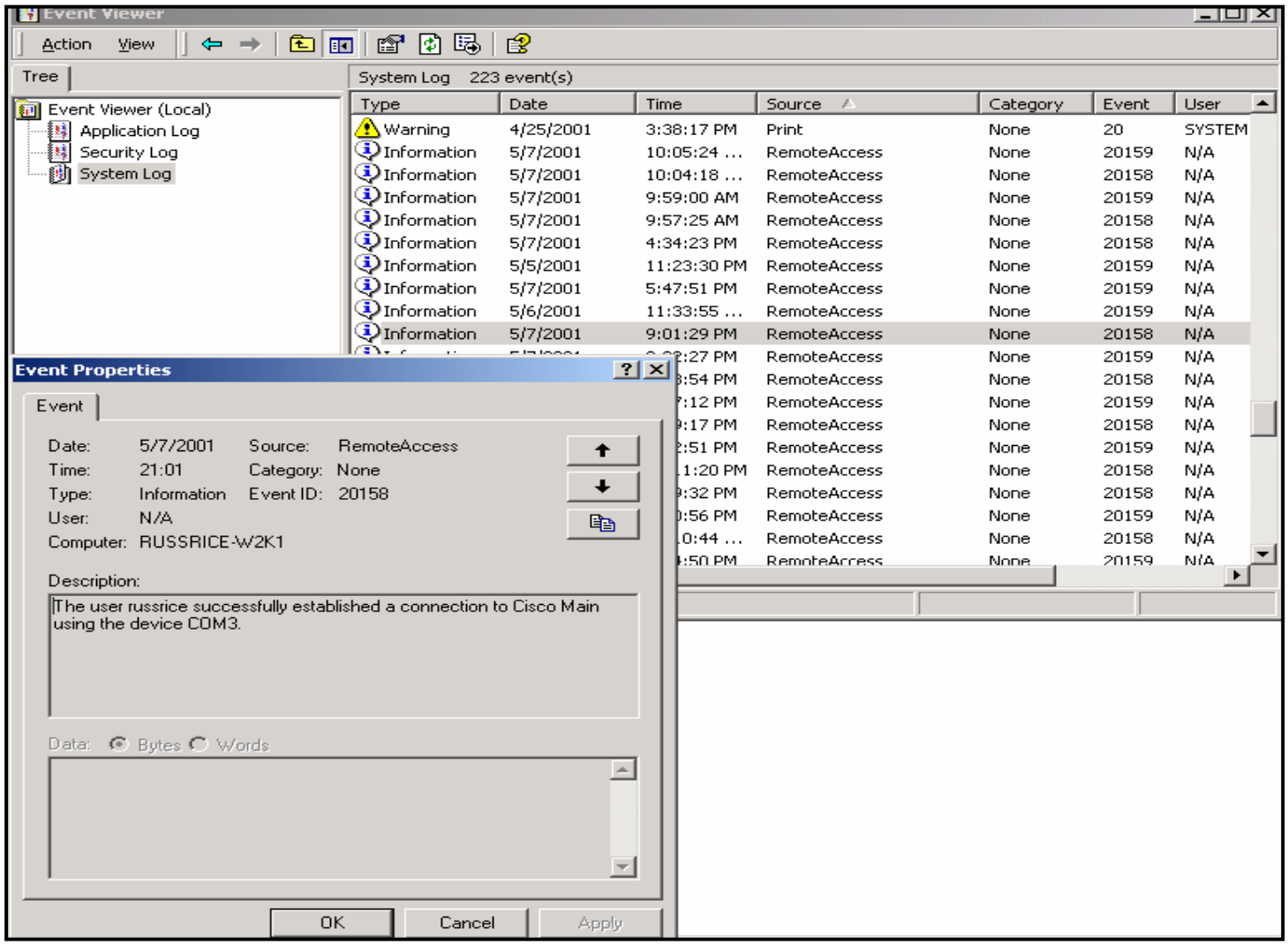


802.1X and Group-Level Authorization

Cisco.com

- **Similar technology to WLAN PEAP (based on EAP as well)**
- **Enables per-port authentication**
  - **Multiple credential-types supported by EAP**
- **Provides VLAN assignment capabilities**
  - **VLAN assignment in combination with the distribution device enforces L3/4 policy for group-level authorization**
  - **E.g. accounts payable verses sales**
  - **Different groups, different access policies**
  - **Works in wired or wireless worlds**

Host System Logs

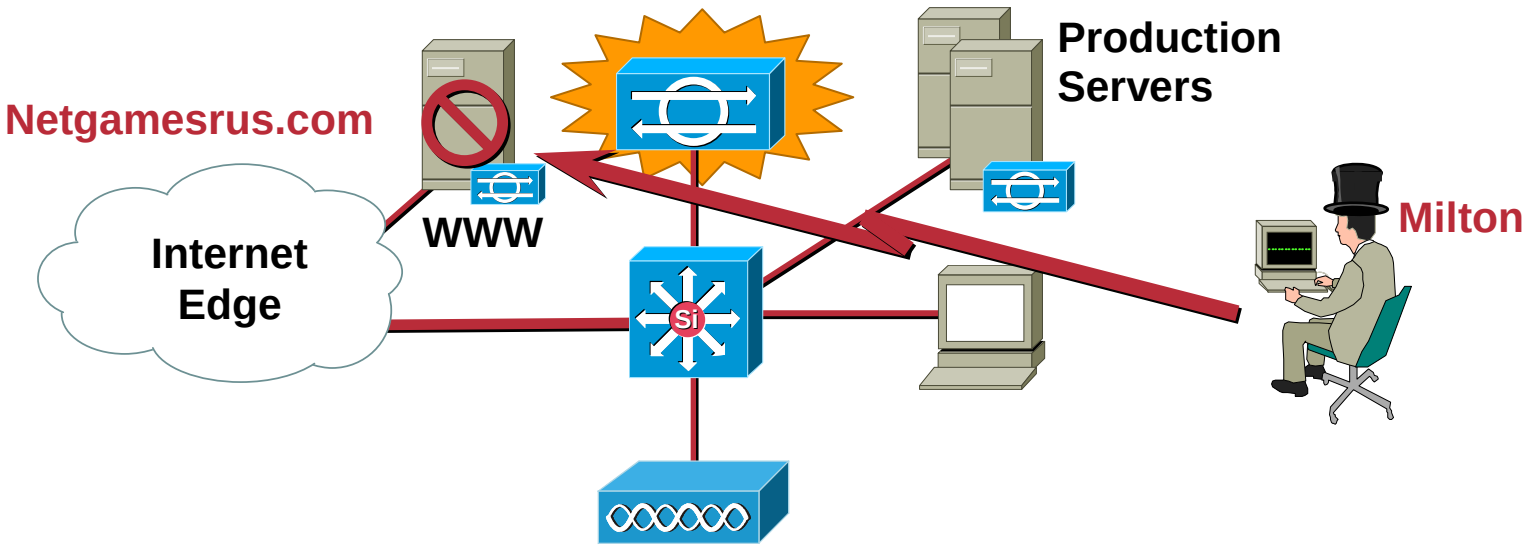


Campus Filtering: Spoof Mitigation

Cisco.com

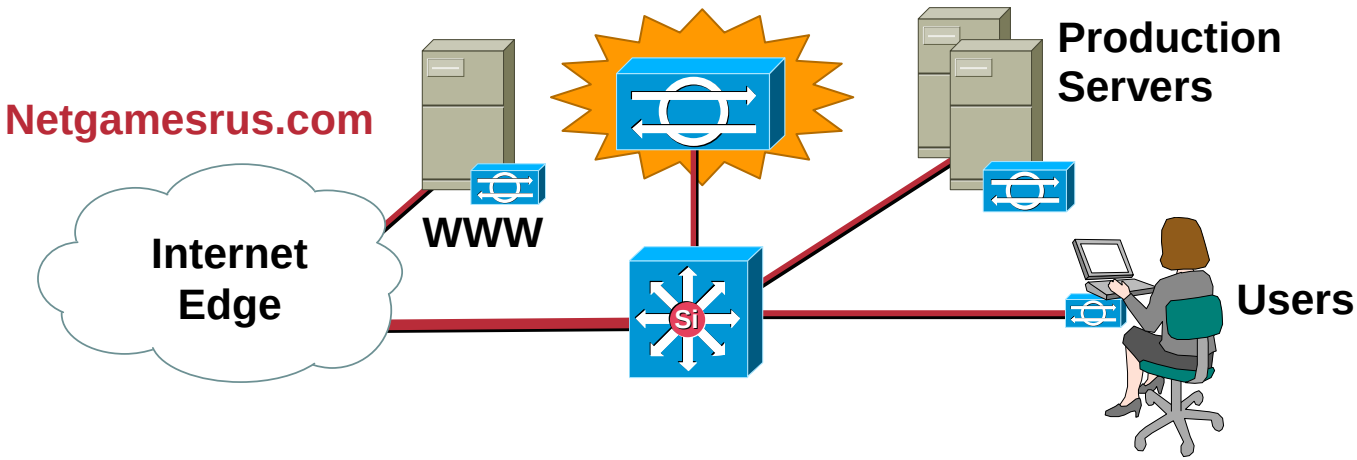
- **Consider dynamic filtering**
  - **802.1x group-ACL extensions**
- **RFC 2827 has its place in the campus**
  - **Given segments with known RFC 1918 subnets should filter out any off-segment sourced traffic and limit inbound and outbound traffic to known ports**
  - **Port granularity more likely in network-service or management segments, not likely for desktops**
- **Filtering between telephony and data or any network segment will reduce the likelihood of attack bleed-over**
  - **E.g. DoS attacks in the data network effecting the voice network**
- **Static WLAN filtering in most environments is not effective**
  - **Exception IPsec**
  - **Again consider 802.1x group-ACL extensions**

PayDay!



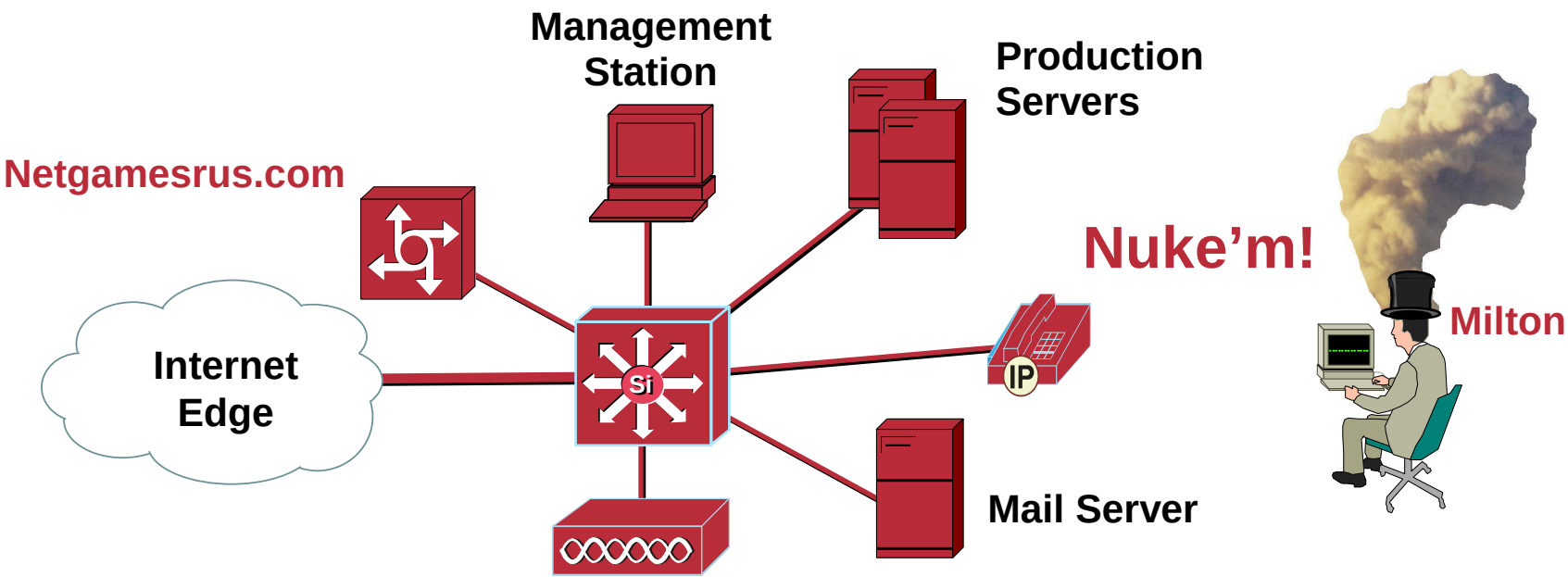
- Milton attempts to run his script from a co-workers PC but to no avail!
- Thinks they may be on to him so he calls in sick for the day

Success!



- NIDS triggers on “fetchmydata” bogus script call (alarms ensue)
- IT backtracks through access logs to determine who had the specific IP at that time and initiate traceback
- *Success* they determine it was sourced from an uncontrolled lab system
- Retrieve keyboard logs, realize it’s someone in Milton’s department!

Vengeance



- **Too many accusations**
  - **Book a ticket to Mexico City**
  - **Finds as many available systems as possible and launches a DDoS against the entire campus LAN, using spoofed addressing to mask source of attack**
  - **"I am going to be a mushroom cloud laying (deleted) on your (deleted)"**

At the End of the Day

- **Milton:**
  - Lots of nail biting
  - Most likely locked up
  - Definitely terminated
  - Definitely lost his stapler
  - Could have profited and left the country
- **Netgamesrus.com:**
  - Several admins and managers
  - $100K or less of gear and software
  - Countless patching, re-imaging, password refreshes
  - Downtime and unhappy customers
  - PR nightmare

Milton

Vs.

Netgamesrus.com

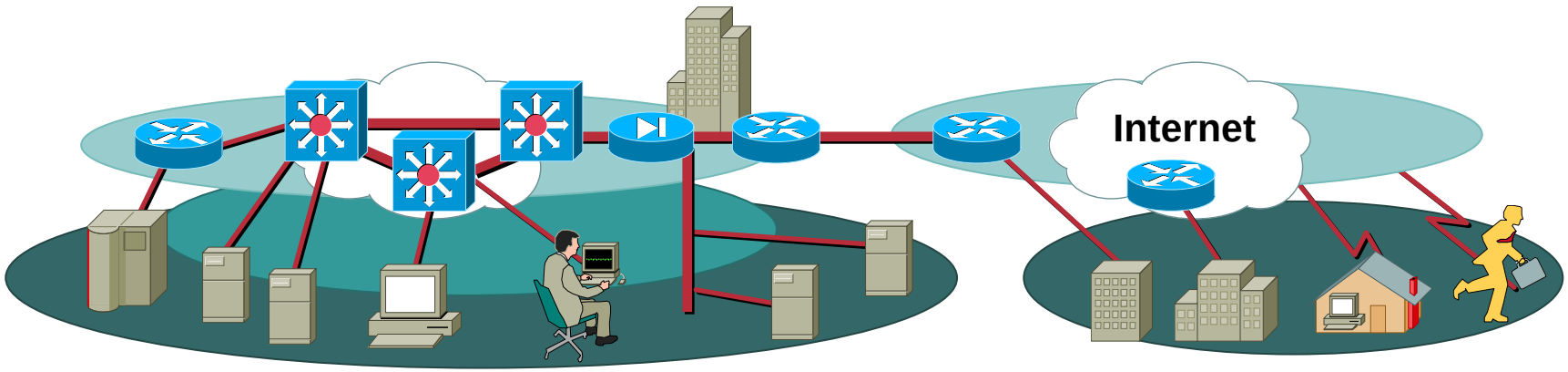
Is There a Better Way?

- **Comprehensive security architecture**
  - Have a security policy
  - Technologies work together as a system
  - No single point of failure
  - Overwhelming defense (barriers, trip-wires, reactions)
- **Skilled staff**
  - Prudent deployment and tuning of products
  - Limit how much is learned the hard way
- **Know the threat and your weaknesses**
  - Track threat tools and security technologies
  - Proactive approach to mitigation
  - Audit posture regularly
- **Cheaper to pay upfront than after the fact**
  - Stay employed and in business!

Campus Design Considerations Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution

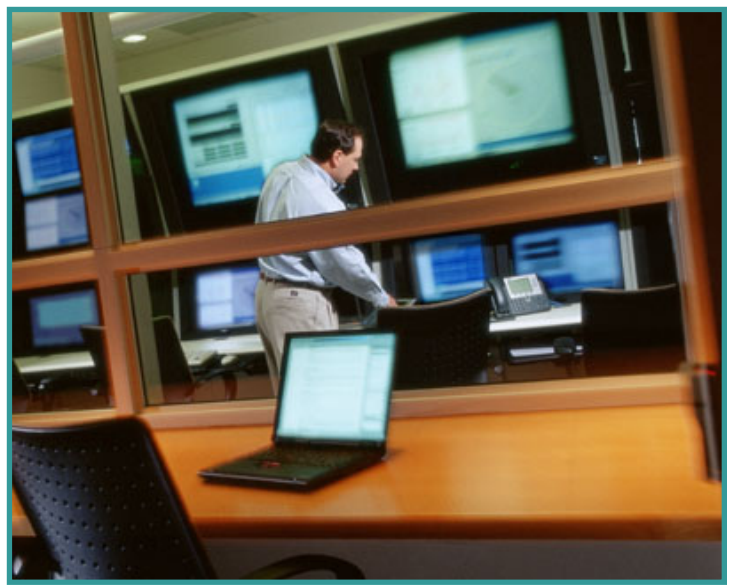
Overall Security Design Goals



- “Network security is a system”
- Security throughout the infrastructure
- Secure management and reporting
- Authentication of key users and operators
- Intrusion detection for critical areas
- Accommodation of emerging network apps
  - WLAN, IP telephony

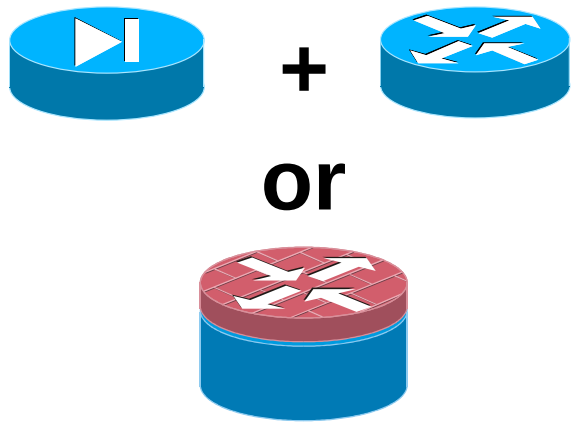
Design Considerations

- **General considerations**
  - **Integrated vs. dedicated security functions**
  - **Device specific**
  - **IDS architecture**
  - **Logging architecture**
- **Wireless LAN**
- **IP telephony**



Integrated vs. Dedicated

- **Performance**
  - **Software vs. hardware**
  - **Wire-rate mostly necessary for campus**
- **Management**
  - **Netops or Secops**
- **Configuration**
  - **Routers and switches default open**
  - **Most security devices default closed**
- **Resilience considerations**
- **Complexity**
  - **Topology vs. device configuration**



Device Specific Security: Routers

- **Potentially a hacker's best friend**
  - **Effect availability of network, not just end-point services**
  - **Eavesdropping, man-in-the-middle**
- **Protection should include:**
  - **Constraining telnet access**
  - **SNMP read-only**
  - **Administrative access with TACACS+**
  - **ACLs to specify the management station**
  - **Turning off unneeded services**
  - **Logging unauthorized access attempts**
  - **Authentication of routing updates**
  - **Secure command and control where possible (SSH, IPsec)**
- **www.cisco.com/warp/public/707/21.html**
- **Cisco IOS Secure Device Manager (SDM)**

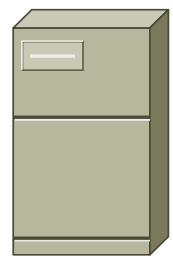
Device Specific Security: Switches

- **Protection needs are similar to routers**
- **VLANs create additional concerns:**
  - **VLANs should not span the distribution unless necessary (e.g. management, WLAN, etc.)**
  - **Remove user ports from auto-trunking**
  - **Use non-user VLANs for trunk ports**
  - **Set unused ports to a non-routed VLAN**
  - **Ensure VLAN separation where appropriate**

- **Remember a switch is designed to enable communications**
- **Consider per-port authentication 802.1X and enforcing group-level authorization privileges**

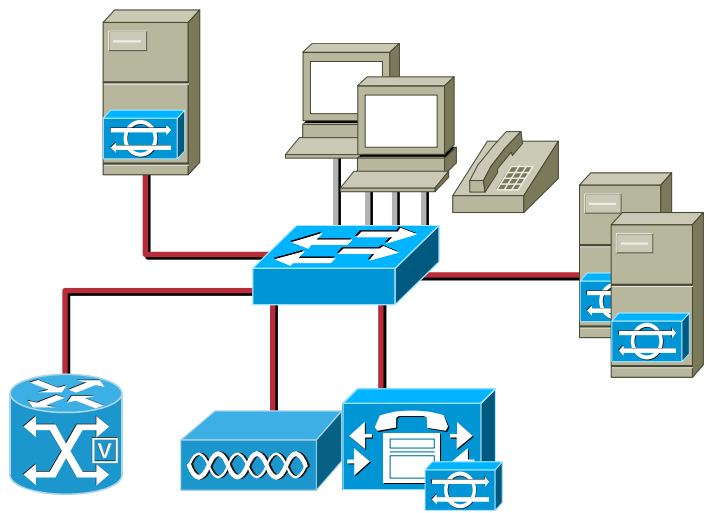
Device Specific Security: Hosts/Applications

- **High visibility makes them easy targets (2002 CSI/FBI survey)**
  - 47% respondents offer WWW site for e-commerce (97% have WWW sites)
  - 38% respondents had unauthorized access or misuse to sites (+50% Y-Y) (21% don't know)
  - 39% of these reported 10+ incidents (-33% Y-Y)
  - 60% attacks from outside, 32% from inside and outside
  - Attack types experienced: 70% vandalism, 55% DoS, 12% theft, 6% financial fraud
- **Ensure that host components are compatible and at the latest version**
  - Hardware platform
  - Operating system and updates
  - Standard applications, patches, and scripts
- **Limit running services to only what's necessary**
- **Audit trails matter**
- **Trust considerations**
  - Between services on the host and between hosts
- **Protect applications**
  - Complexity of applications makes them prone to human error
  - Timely patching (however there are issues)
  - Public domain, commercial, or self-developed?
- **Provide layered security though deployment of anti-virus and HIPS**



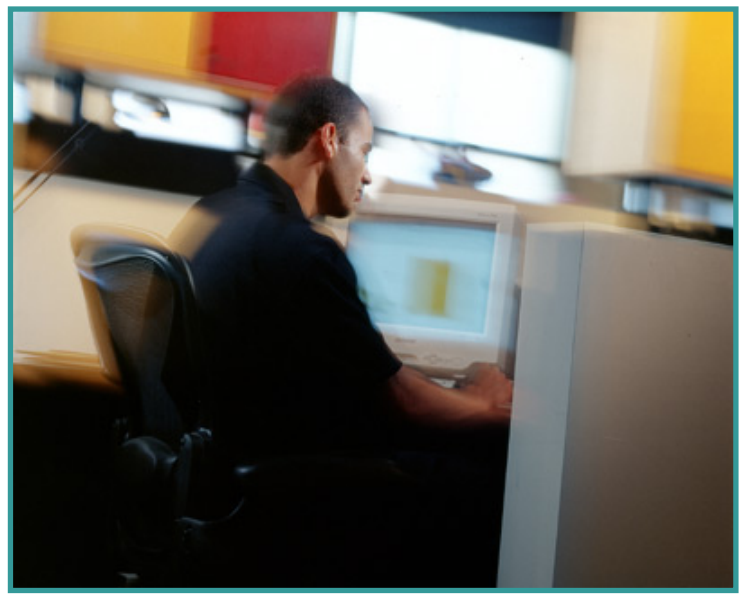
Intrusion Detection Systems

- **Host and network**
  - **Both have their place**
  - **NIDS in campus environments may easily become overwhelmed**
  - **False positives**
- **Placement**
- **Alarm or enforce?**



Logging Architecture

- Device priority
- Where to log (multiple servers? One for historical, one for tactical? Tiered?)
- What to log (log levels)
- Some servers are log protocol and/or function specific (post office vs. syslog)
- Scaling considerations (per server, per network device, filtered display based on alarm level)



Design Considerations

Cisco.com

- General considerations
- Wireless LAN
  - Wireless networks are targets
  - WLANs are weapons
  - AP security options
  - LEAP WLAN design
  - VPN WLAN design
- IP telephony

Wireless Networks Are Targets

Cisco.com

- IT can’t keep up with deployments
- WLAN devices ship with all security features disabled
- Generic 802.11b devices don’t have effective security options
- WindowsXP informs users of available WLAN networks
- 2.4 GHz jamming is trivial (cordless phones, baby monitors, microwave ovens, bluetooth devices)
- Most WLAN APs have only clear-text management options

Wireless Networks Are Targets

- **Access point security recommendations:**
  - **Enable user authentication for the management interface**
  - **Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often**
  - **Consider using SNMP read only if your management infrastructure allows it**
  - **Disable any insecure and nonessential management protocol provided by the manufacturer**
  - **Limit management traffic to a dedicated wired subnet**
  - **Encrypt all management traffic where possible**
  - **Enable wireless frame encryption where available**
- **Client security recommendations:**
  - **Disable ad hoc mode**
  - **Enable wireless frame encryption where available**

WLANs Are Weapons

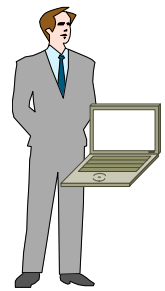
- APs are small and cheap
- Physical building security is weak (tailgaters)
- Most buildings allow campus connectivity on all ports
- All this adds up to a cheap, effective, and anonymous hacking opportunity
- Consider the following:
  - MAC address limitations on switches
  - Conference rooms use wireless access with authentication and privacy
  - Perform regular physical and RF sweeps for APs

Who Installs Rogue APs?—
"Focus on the Frustrated Insider"

Frustrated insider

>99.9% of Rogue APs

- User that installs wireless AP in order to benefit from increased efficiency and convenience it offers
- Common because of wide availability of low cost APs
- Usually ignorant of AP security configuration, default configuration most common



Jones from Accounting

Malicious hacker

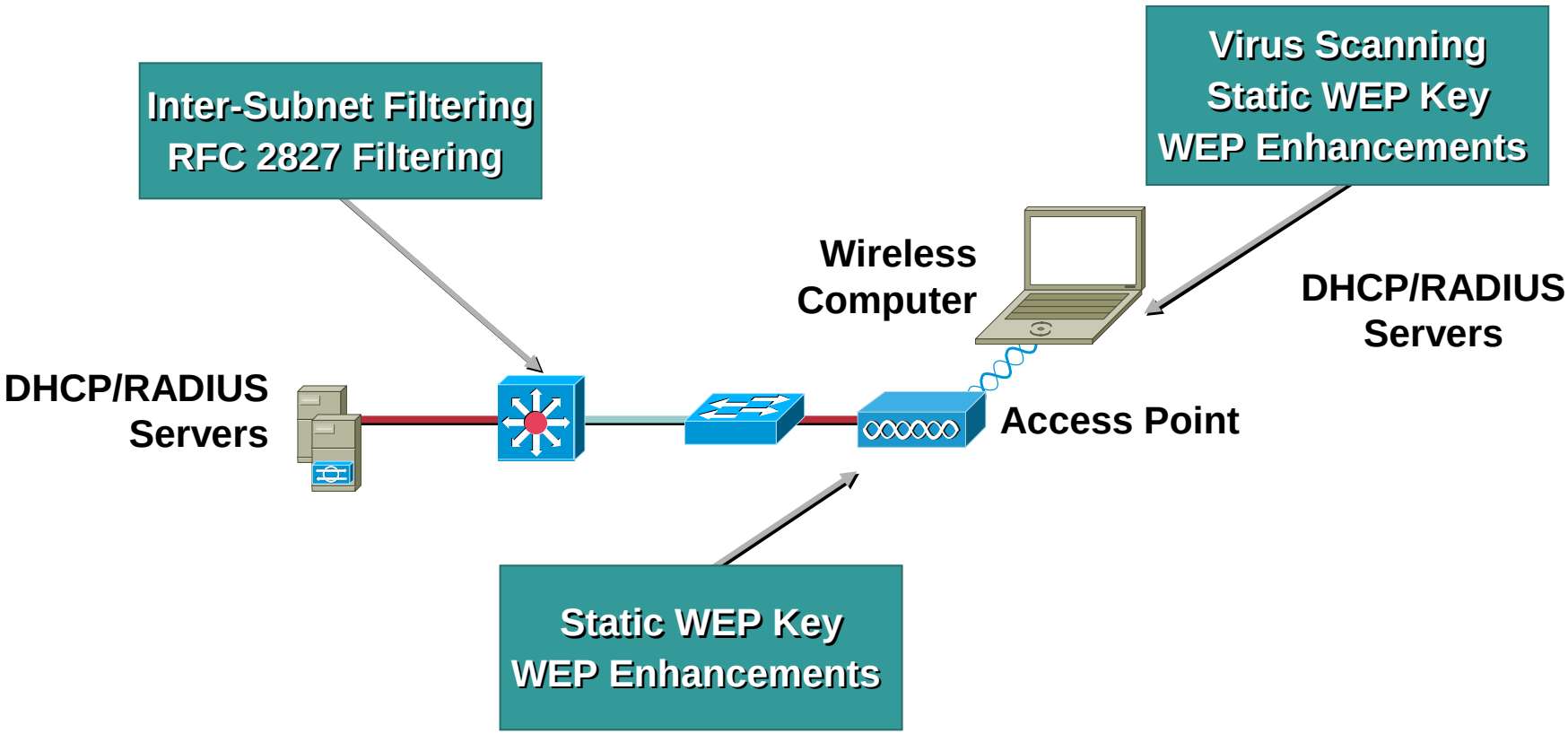
<.1% of Rogue APs

- Penetrates physical security specifically to install a rogue AP
- Can customize AP to hide it from detection tools
- Hard to detect—more effective to prevent via 802.1x and physical security
- More likely to install LINUX box than an AP

James Bond

WEP WLAN Design

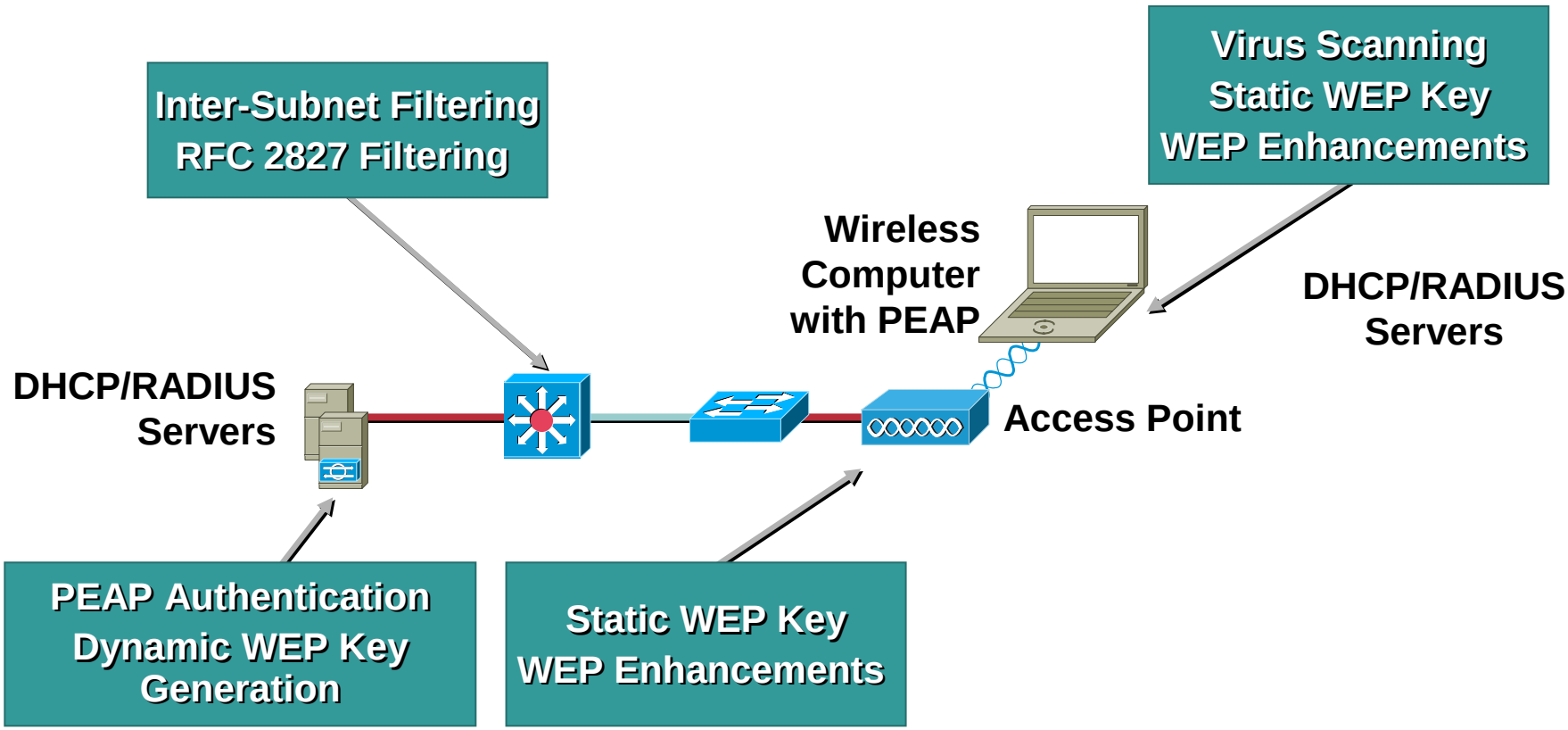
Be Aware of the Limitations



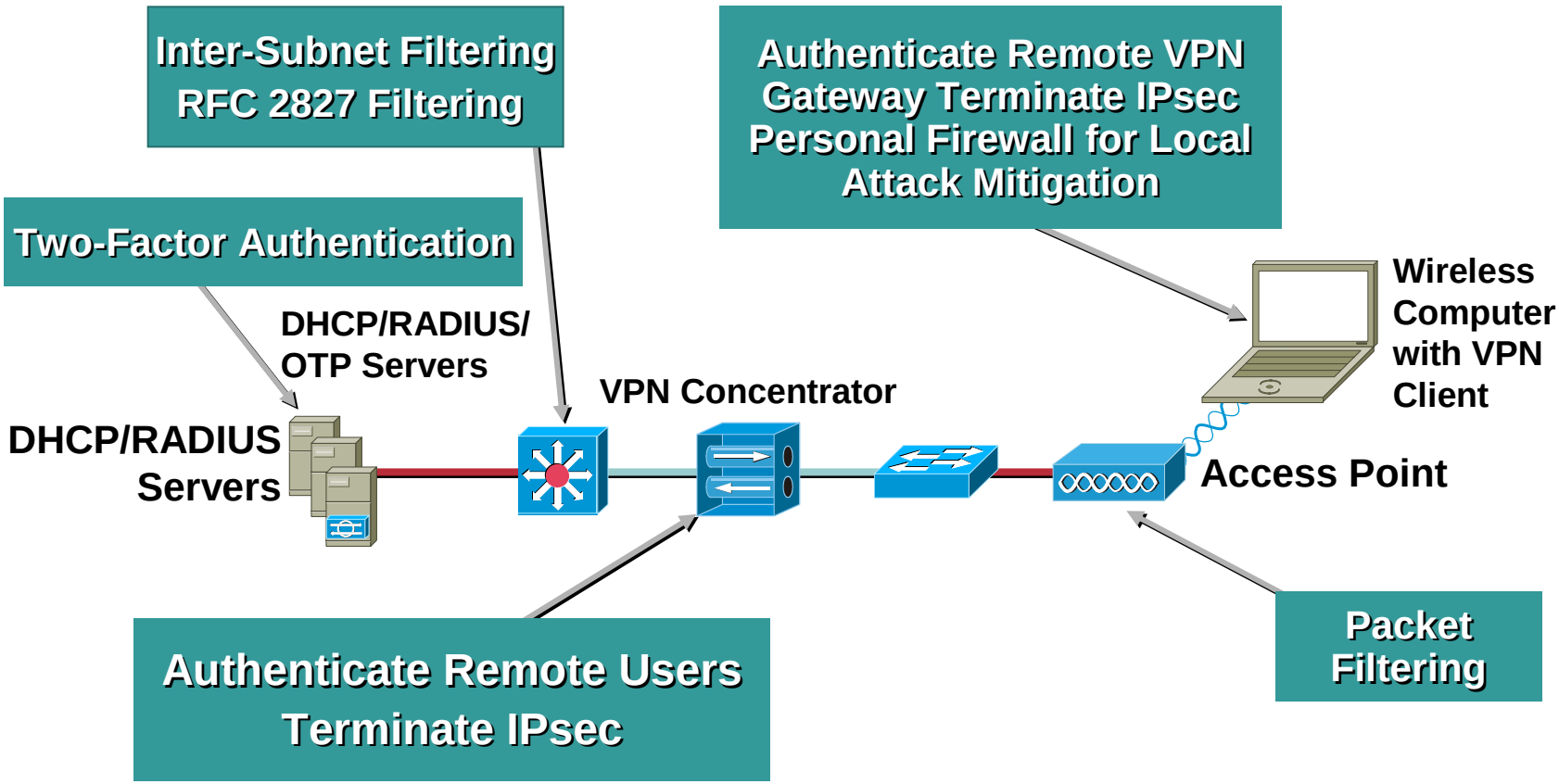
PEAP-TKIP WLAN Design

Cisco.com

LEAP/PEAP



VPN WLAN Design



What EAP Types Are Available?

	LEAP	EAP-TLS	EAP-PEAP
Server Authentication	Password	Certs/PKI	Certs/PKI
Client Authentication	Password	Certs/PKI	Password[1]
Single Sign on	Yes	Yes	No[2]
Vulnerable to Password Attack	No[3]	No	No
OTP/LDAP Support	No	N/A	Yes
Additional Infrastructure	No	Yes/CA	Yes/CA

[1] Not limited to password schemes, but that is what is currently available

[2] MS native supplicant supports SSO w/EAP-MS-CHAPv2

[3] Requires strong passwords

Coming:Wi-Fi Protected Access (WPA)

- **Components of WPA:**
  - **Authenticated key management using 802.1X:**
    - **EAP authentication and Pre-Shared Key (PSK) authentication**
    - **EAP-TLS and RADIUS are the nominated EAP test mechanism**
  - **TKIP: per-packet keying**
  - **Message Integrity Check (MIC)**
  - **Unicast and broadcast key management**
  - **IV expansion: 48 bit IVs**
  - **Migration mode—coexistence of WPA and non-WPA devices**

Design Considerations

- General considerations
- Wireless LAN
- IP Telephony
  - The state of IP telephony
  - Voice attacks
  - Data and voice segmentation

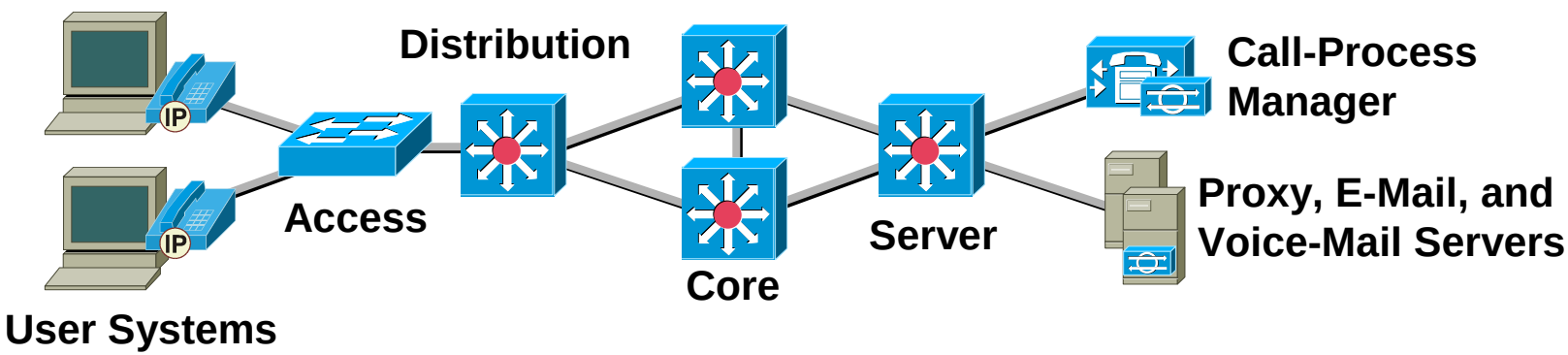
The State of IP Telephony

- **Today there is no single widely deployed standard for call signaling**
  - **Virtually all vendors rely on proprietary protocols**
  - **Standards-based protocols lack features or have feature disparity**
- **Voice protocols are still relatively new**
  - **Hackers are not familiar with them yet**
  - **There are not many documented attacks**
- **Security and IP telephony are in the initial integration phase**
  - **Most protocols today do not support confidentiality or strong device/user authentication features**
  - **However, there are many issues than we can address today with existing technologies**

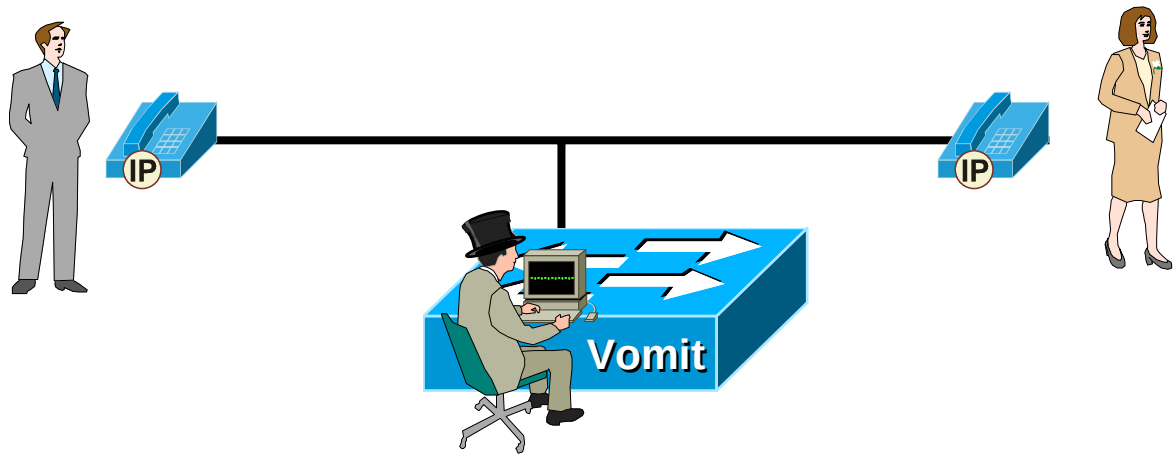
Data and Voice Segmentation

- **Use the same access, core, and distribution layers for the two segments**

  Technologies such as layer 3 access control, stateful firewall, and VLANs make this possible



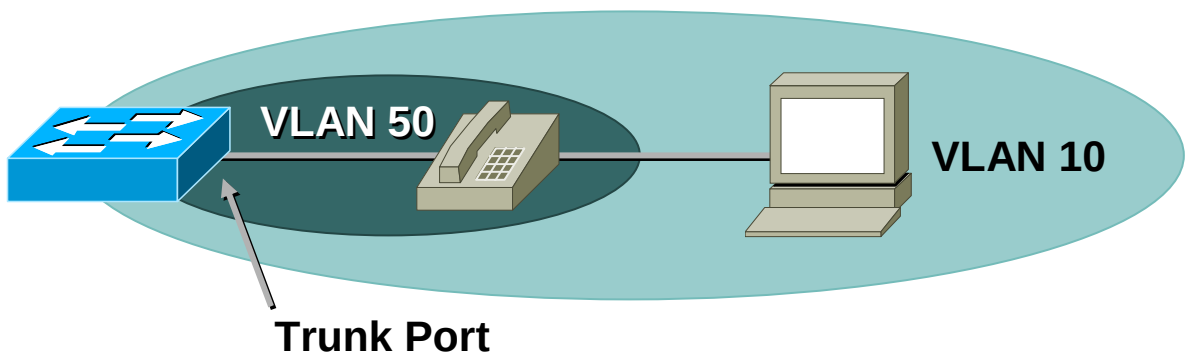
Voice Attacks: Back to VOMIT



- **The majority of IP telephony devices don't support confidentiality**
- **Data-voice segmentation and a switched infrastructure will greatly reduce the likelihood of eavesdropping by tools such as VOMIT**
  - **Again, the IP phones are not really missconfigured, just lack confidentiality**

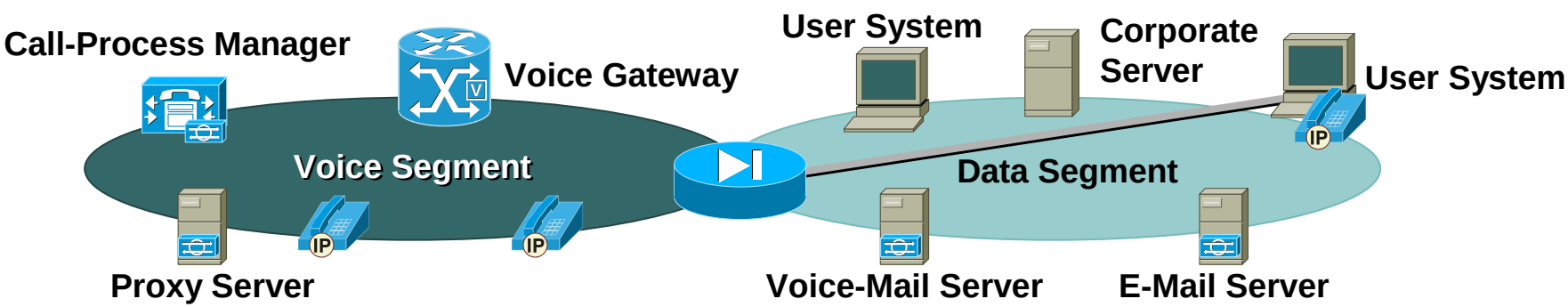
Data and Voice Segmentation II

- **IP phones typically provide access to both segments**
  - **IP phones support a "data port" for the local PC so that only a single cable is necessary**
  - **Make sure that the phone supports separation of the two segments (e.g. via VLAN support)**
  - **We don't recommend you rely solely on VLANs for separation, in the interest of layered security you should also provide layer 3 filtering at the access layer**



Data and Voice Segmentation III

- **Deploy a stateful firewall to broker the data-voice segment interaction**
  - Provides dynamic pinpoint access and mitigation against TCP connection starvation, UDP flood, and spoofing attacks
  - Feasible in front of voice services
  - Placement of voice and related services is key
  - Make certain the stateful firewall vendor you chose supports stateful inspection of the voice protocols you decided to deploy
- **Use private address space for data-voice segments, such as RFC 1918**
  - Partitioned addressing facilitates filtering and recognition
  - 1918 is not routeable (well, most of the time) which reduces the likelihood of reconnaissance scans even if NAT is misconfigured
  - Spoof mitigation filtering virtually guarantees that hosts are who they claim to be in local segments
  - This also eases manageability and troubleshooting

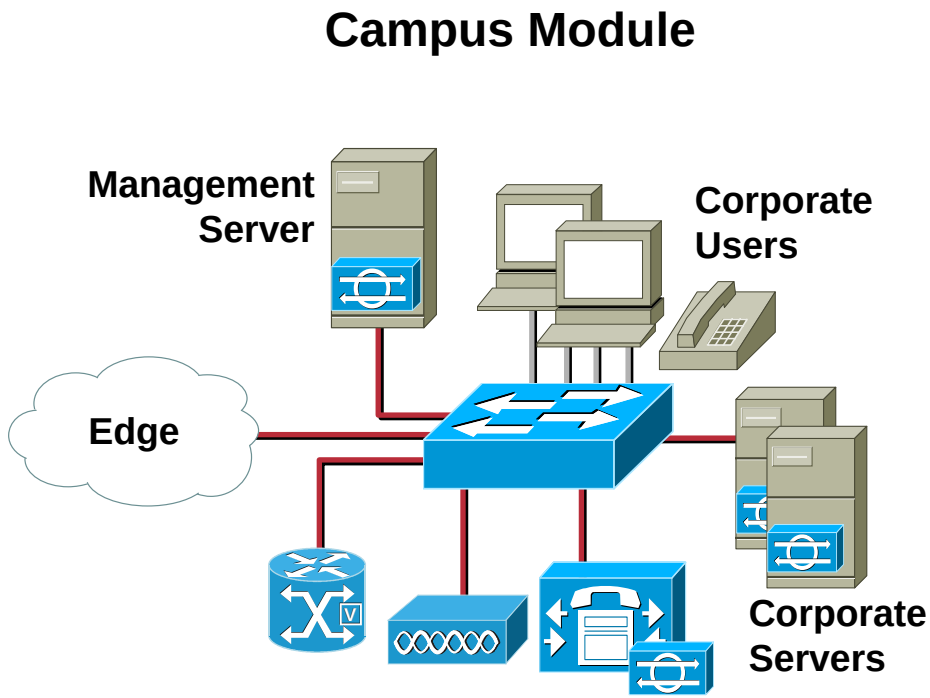


Agenda

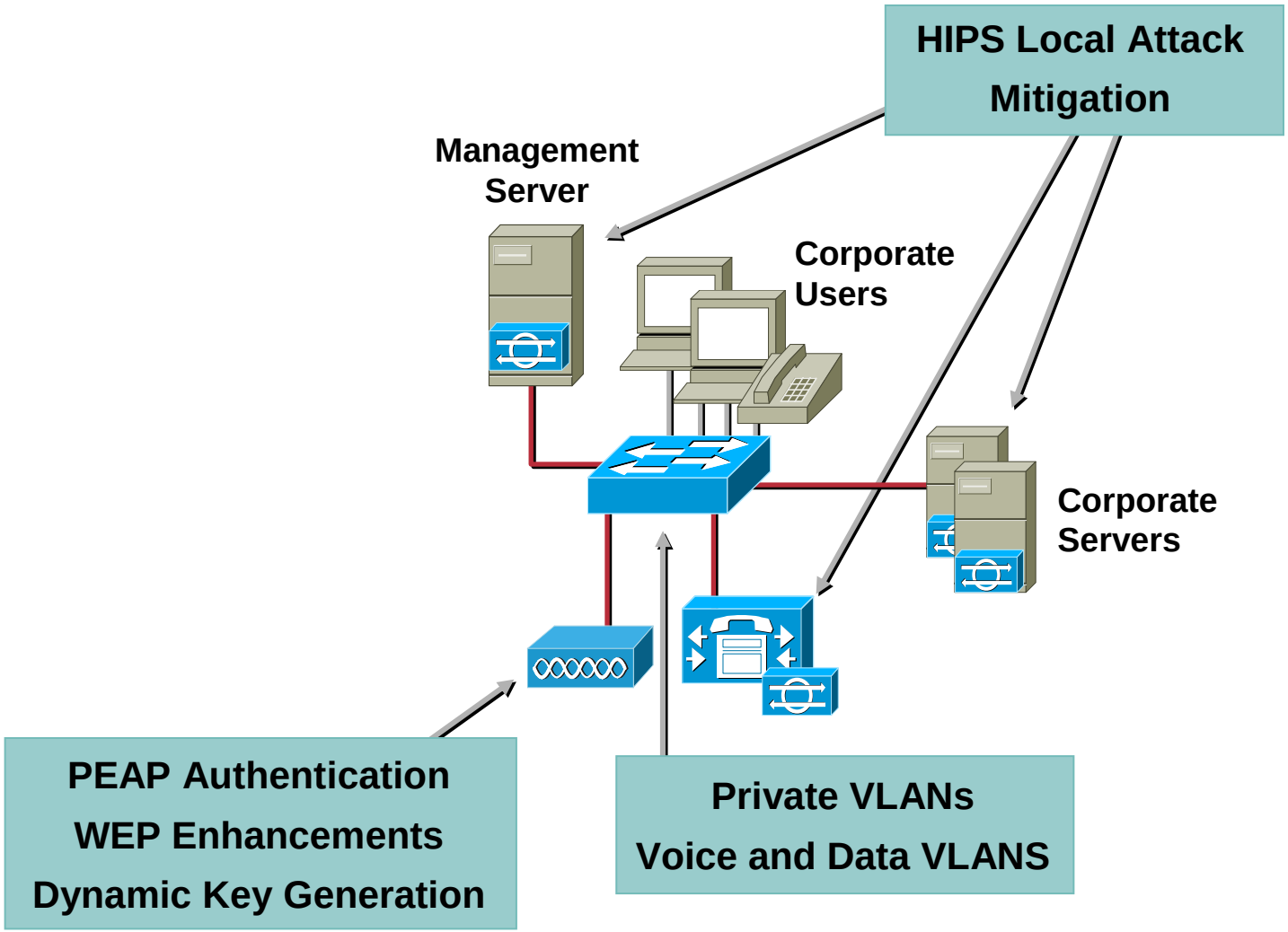
- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution

Integrated Detailed Model

- **Design goals**
  - Security throughout the infrastructure
  - Secure management and reporting
  - Authentication of key users and operators
  - Intrusion detection for critical areas
  - Accommodation of emerging network apps (WLAN, IPT)
  - Minimize cost
  - Integration of features
- **Alternatives**
  - How accomplish inter-vlan filtering?
  - Deploy NIDS?



Attack Mitigation



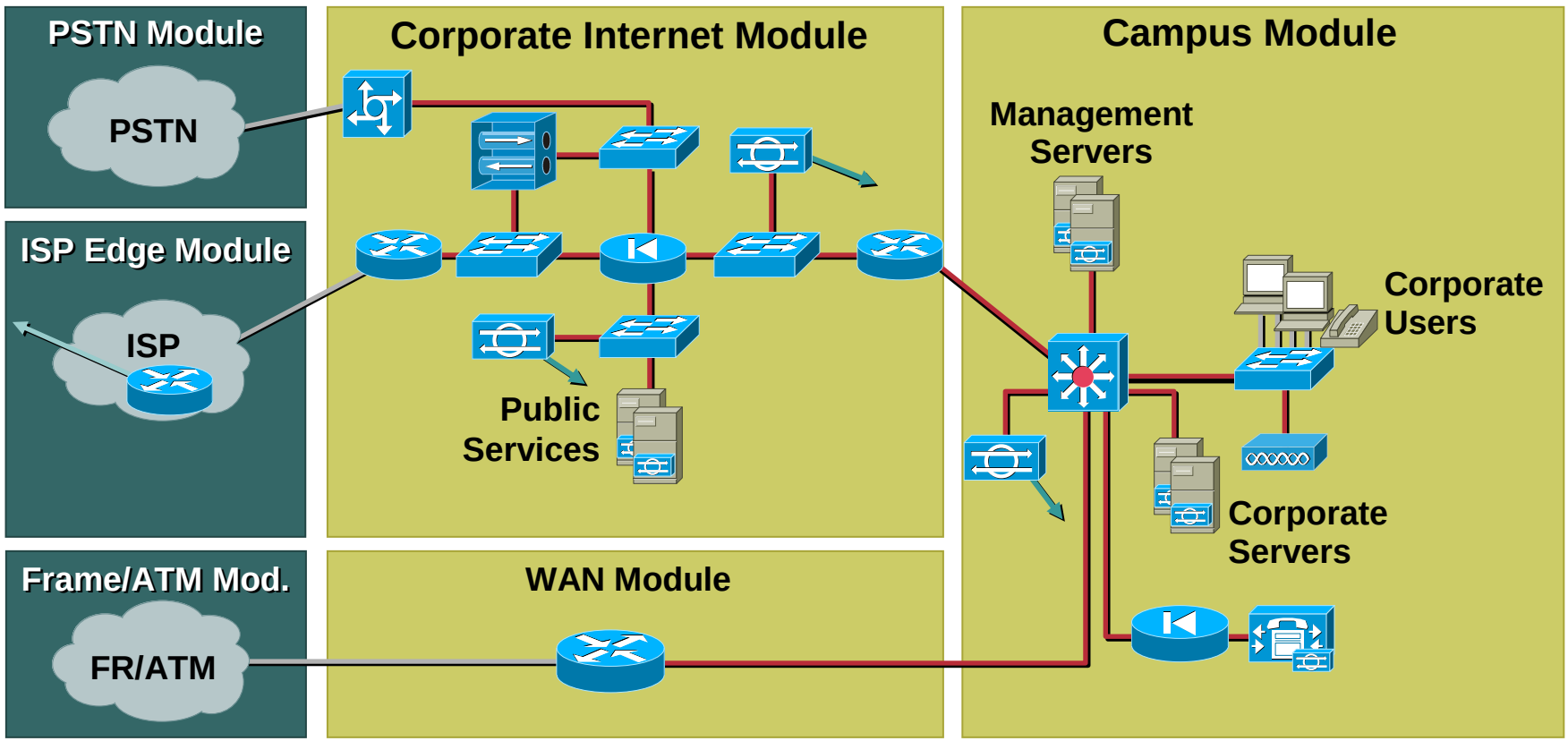
Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution

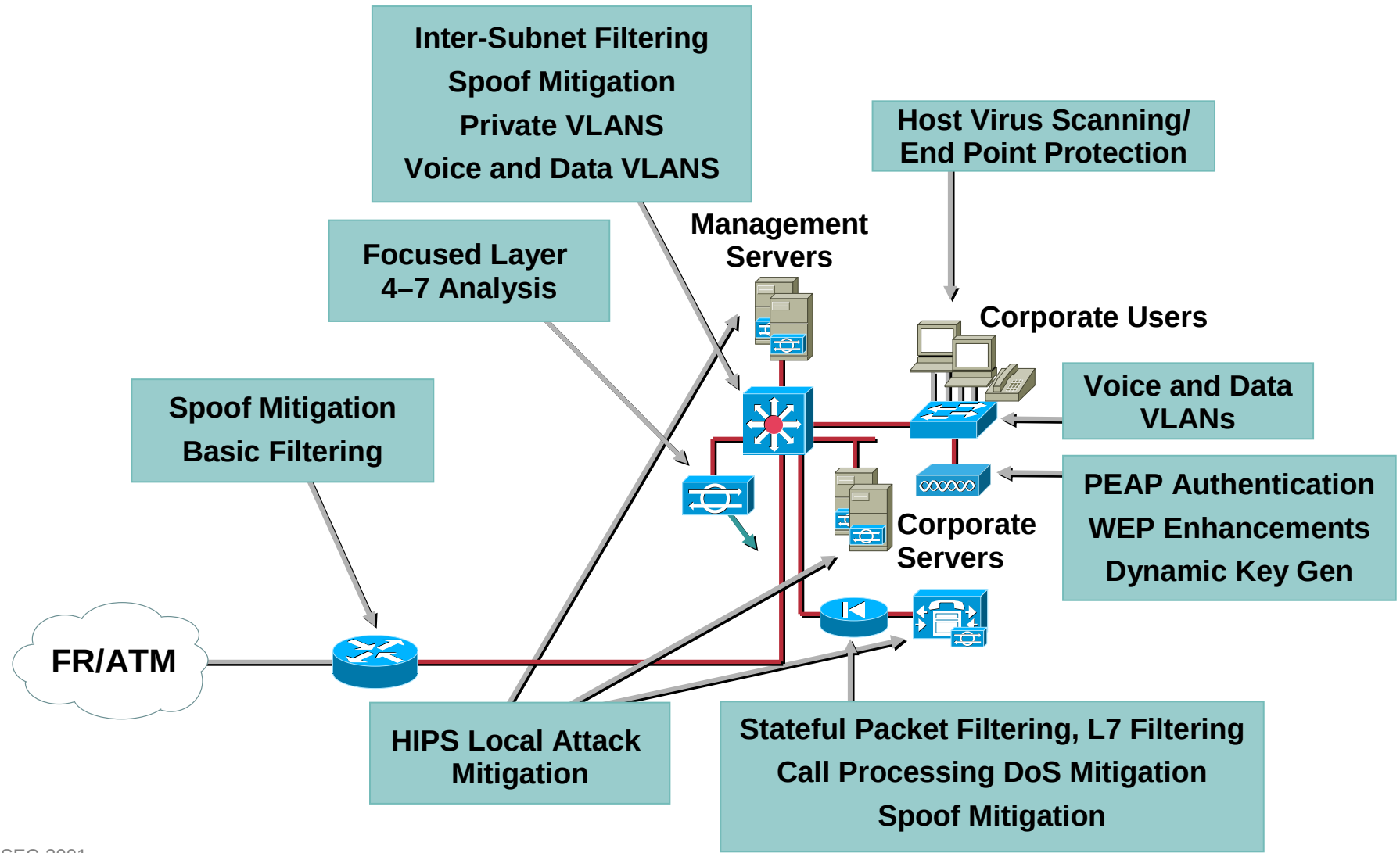
Distributed Security Solution

- **Design goals**
  - Security throughout the infrastructure
  - Secure management and reporting
  - Authentication of key users and operators
  - Intrusion detection for critical areas
  - Accommodation of emerging network apps
  - Performance
  - Separation of security function
  - No single point of total compromise
- **Distributed security design considerations**
  - Management
  - Configuration complexity
  - Cost

Distributed Security Detailed Model



Distributed Security Detailed Model: Campus and WAN



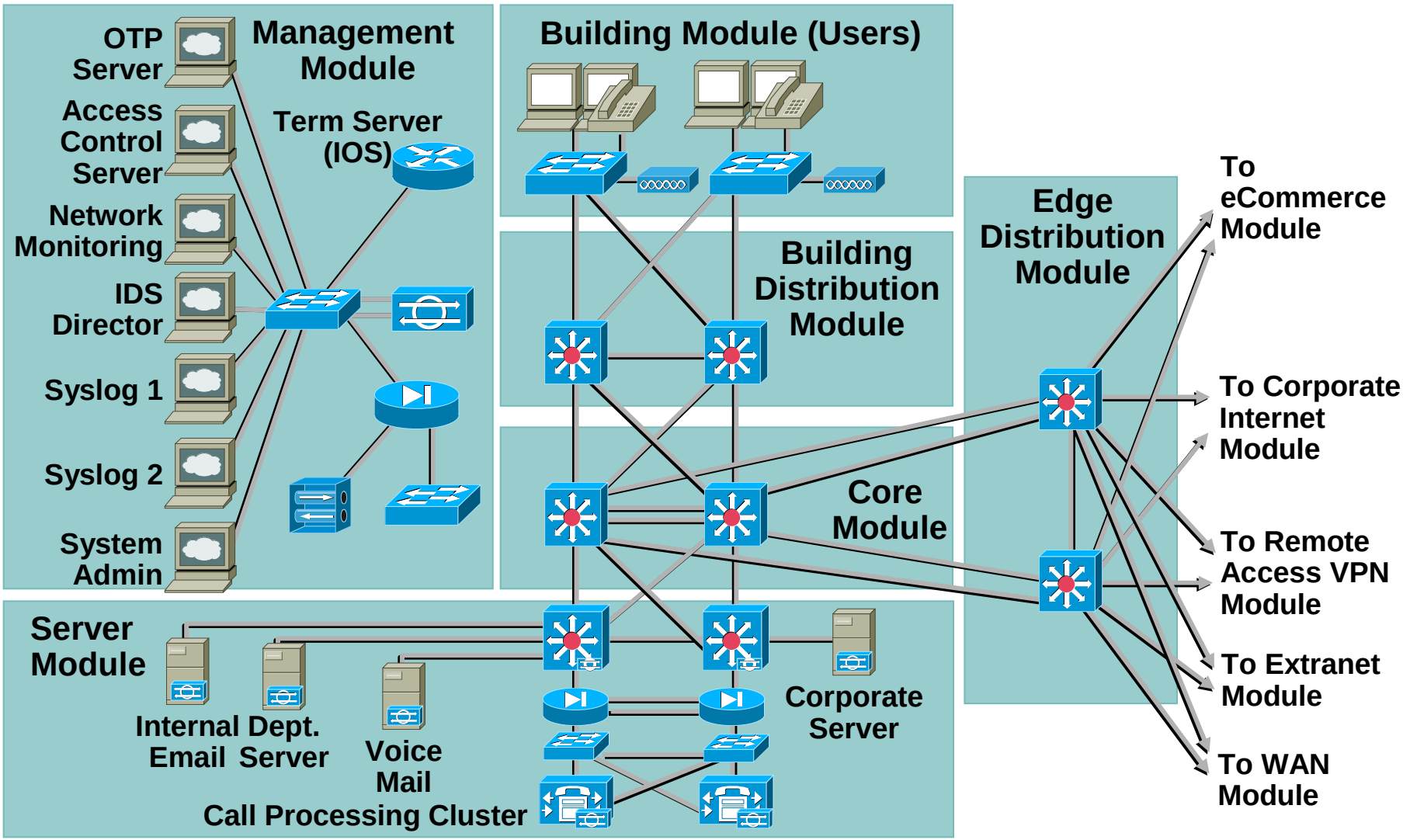
Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution

High-End Resilient Solution

- **Design Goals**
  - Security throughout the infrastructure
  - Secure management and reporting
  - Authentication of key users and operators
  - Intrusion detection for critical areas
  - Accommodation of emerging network apps
  - Performance
  - Resilience
  - Scalability
  - Out-of-band management
  - No single point of total compromise
  - Separation of security function
- **Design Considerations**
  - Complexity of design
  - Number of devices
  - Asymmetric routing vs. state awareness
  - Management infrastructure
  - Administrative roles
  - Cost

High-End Resilient Campus Detail



Campus Network Section

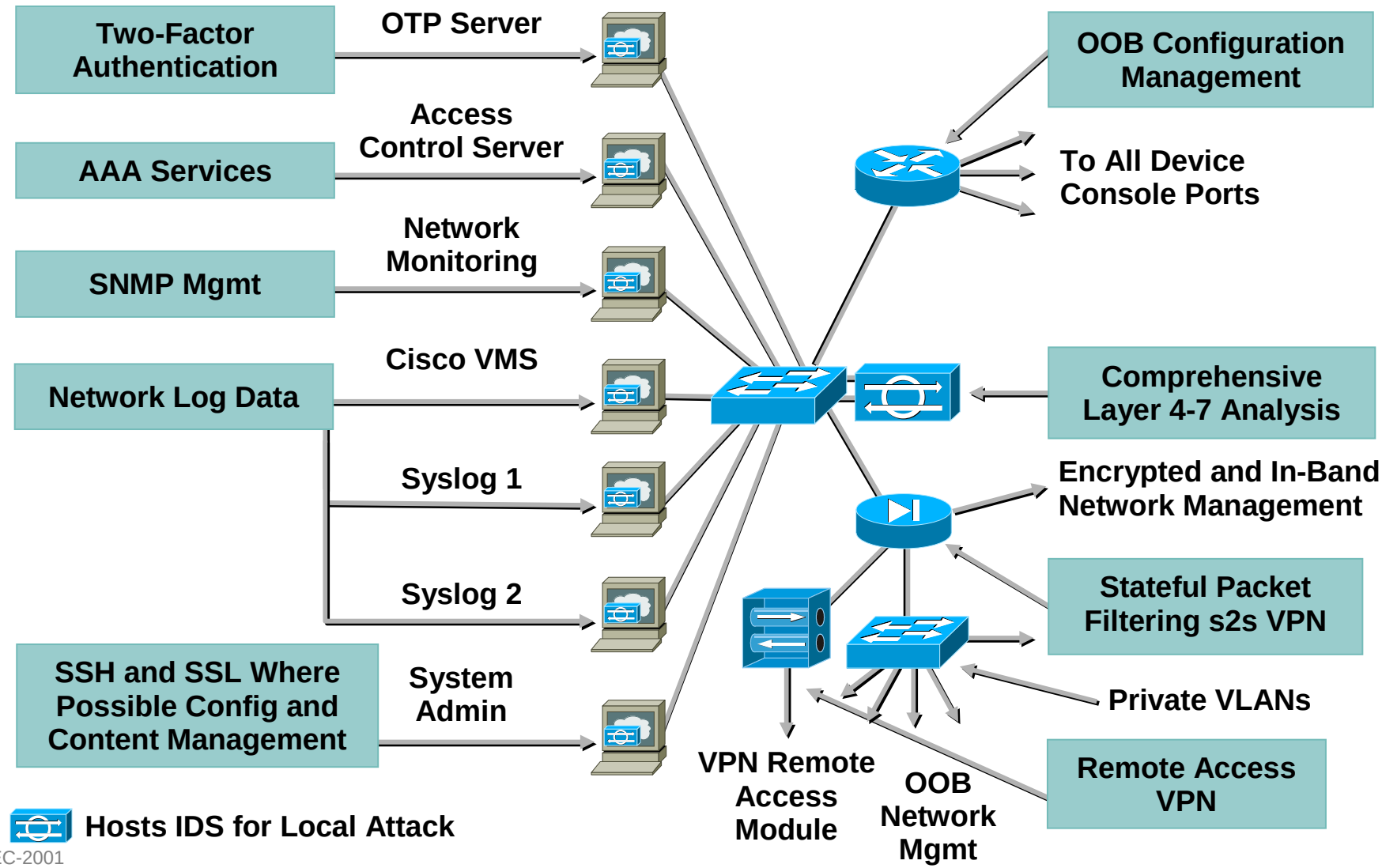
- **Management module**
- **Building access and distribution**
- **Core and server modules**

Management Module Design Goals

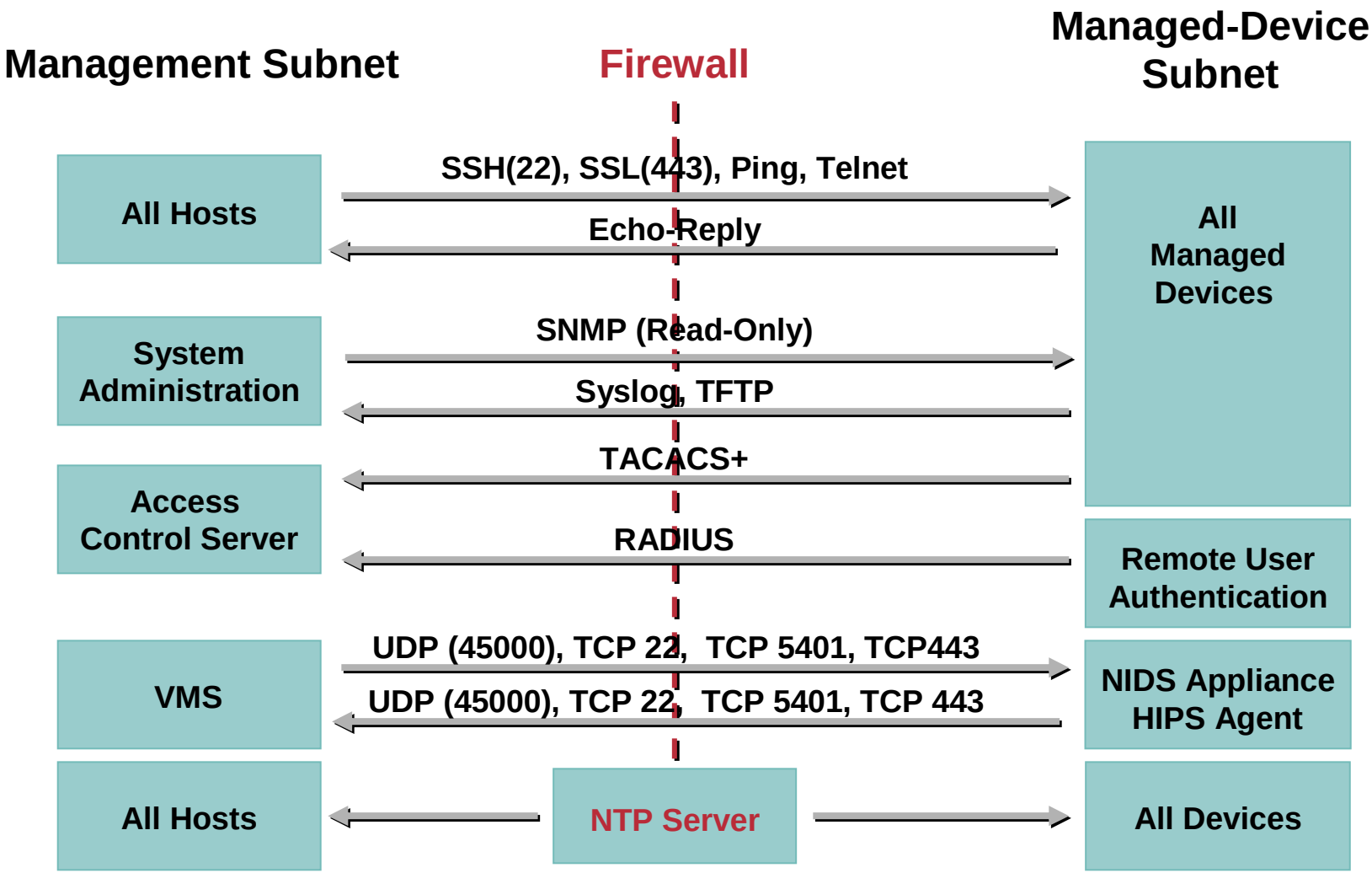
- **Out-of-band management**
  - **Separate physical networks**
  - **Separate address space (i.e. 192.168.25x.xxx)**
  - **Use IPsec if physical separation is not possible**
- **Firewall between management subnet and managed-device subnet**
- **Isolate managed ports to minimize impact of compromised device**
- **NIDS and HIPS on the management subnet**
- **One-time passwords for authentication of administrators**
- **SNMP read-only**

```
snmp-server community Txo~QbW3XM RO 98
access-list 98 permit host 192.168.253.51
```

Attack Mitigation Roles for Management Module

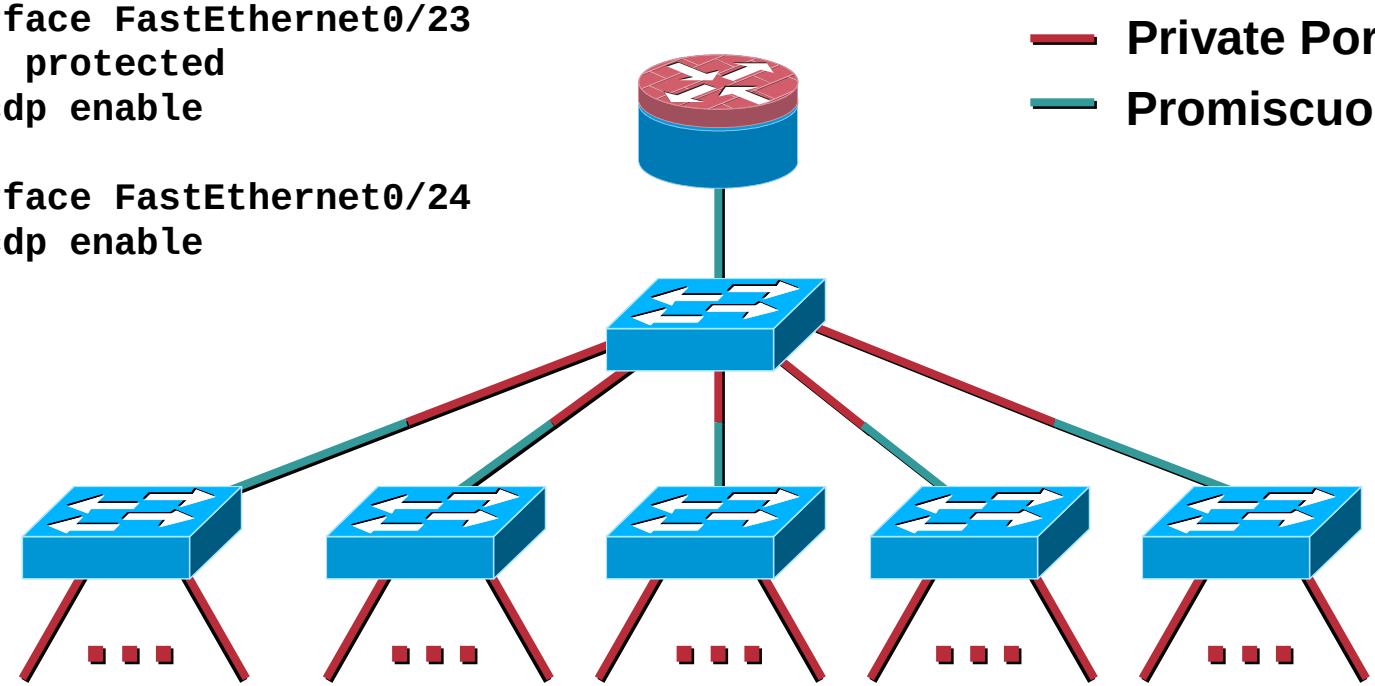


Management Firewall—Stateful Packet Filtering



Managed Device Subnet


```
interface FastEthernet0/23
 port protected
 no cdp enable
!
interface FastEthernet0/24
 no cdp enable
```



To Dedicated Management LAN Port on Each Device

OOB Mgmt Access Control

Cisco.com

```
! Access control configuration for all managed routers
!
! Inbound ACL
access-list 101 permit icmp any any
! Required for Tacacs+
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.13 established
! Required for TFTP
access-list 101 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.13 gt 1023
! Other Management Access
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.13 eq telnet
access-list 101 permit udp host 192.168.253.51 host 192.168.254.13 eq snmp
access-list 101 permit udp host 192.168.253.53 host 192.168.254.13 eq tftp
access-list 101 permit udp host 192.168.254.57 host 192.168.254.13 eq ntp
access-list 101 deny   ip any any log
! Outbound ACL (local router isn't affected by ACLs)
access-list 102 deny   ip any any log

! Management Interface Settings
interface FastEthernet0/0
 ip address 192.168.254.13 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
 no cdp enable
```

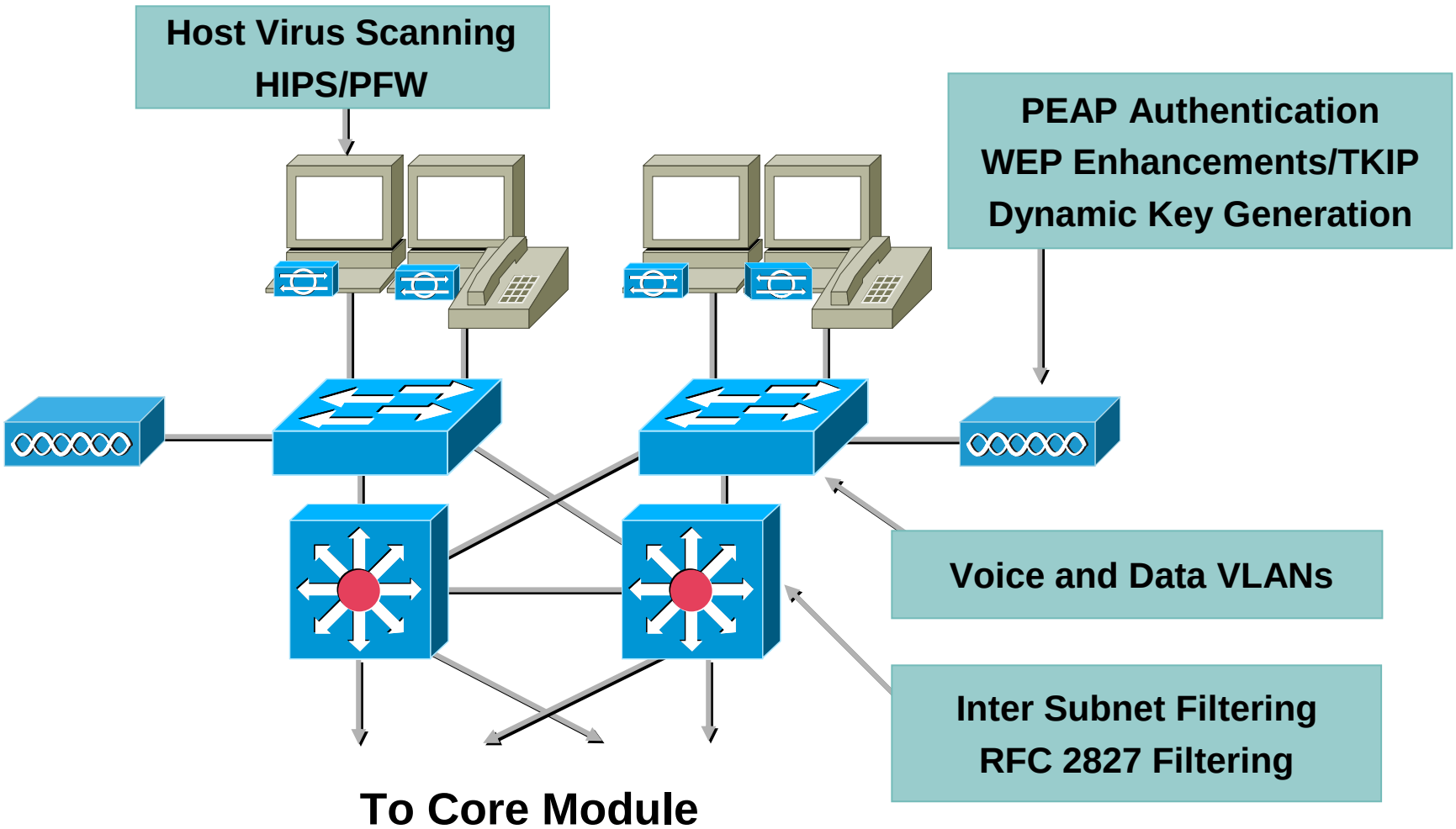
Campus Network Section

- **Management module**
- **Building access and distribution**
- **Core and server modules**

Building and Distribution Design Goals

- **Using VLANs, layer 2 separation for:**
  - **Data and voice ports**
  - **Ports between corporate departments**
- **Host virus scanning and end point protection for WLAN/VPN clients**
- **Layer 3 access-control at distribution prevents IP spoofing and filters traffic**
- **WLAN support**

Attack Mitigation Roles for Building and Distribution Modules



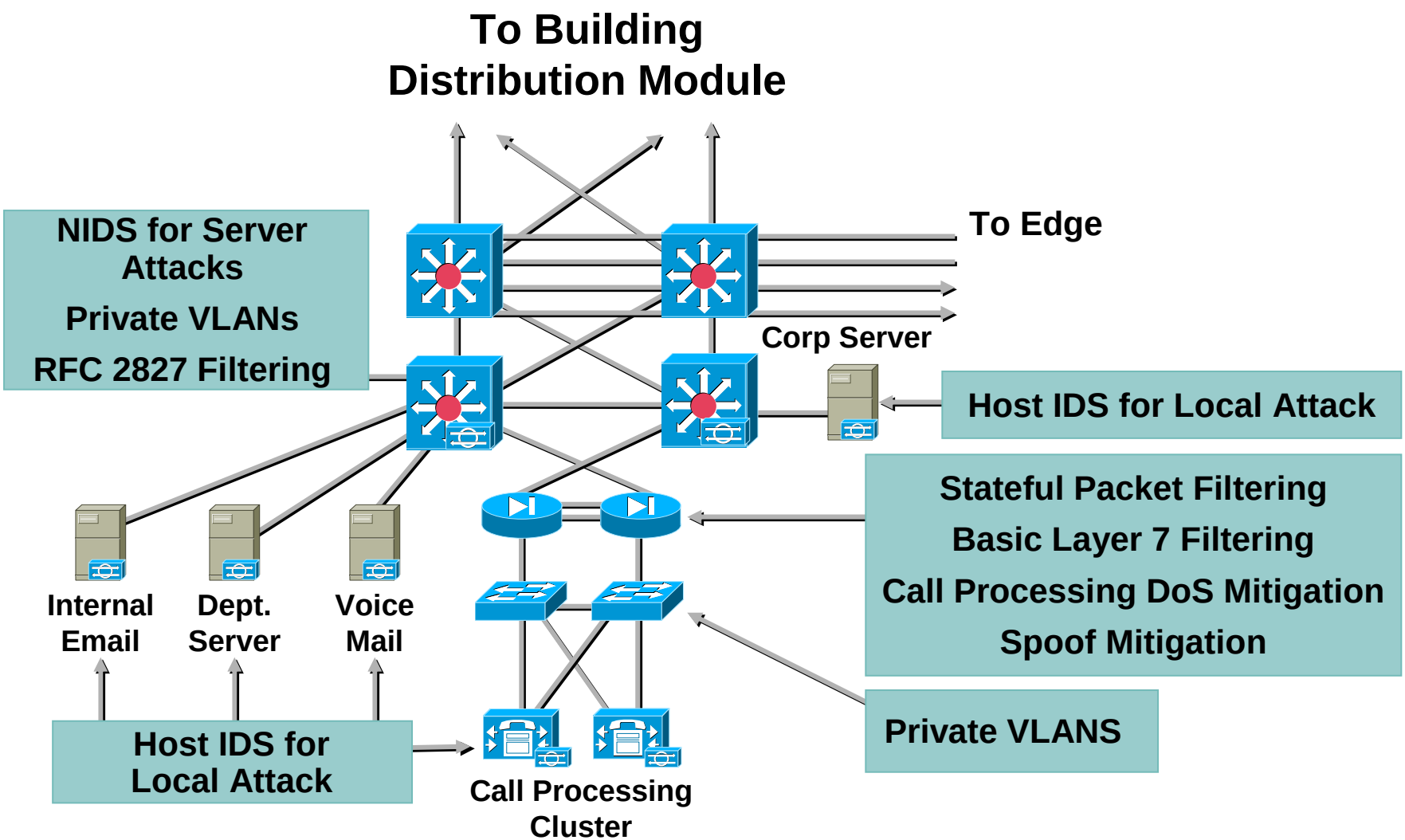
Campus Network Section

- **Management module**
- **Building access and distribution**
- **Core and server modules**

Core and Server Module Design Goals

- **L3 switching with authenticated routing protocol**
- **Private VLANs between servers that do not need communication**
- **Layer 3 access control**
- **HIPS and NIDS to protect server resources**

Attack Mitigation Roles for Core and Server Modules



Crunchy on the Outside… Crunchy in the Middle

Implementing Security: Where Do I Start?

- "Network security is a system"
- Develop a security policy based on business requirements and likely threats
- Perform a network vulnerability analysis
- Use a modular approach to designing and deploying a security solution
- Maintain security posture through disciplined system and network administration

Further Reading

- Office Space: http://www.foxstore.com/detail.html?item=253
- SAFE http://www.cisco.com/go/safe
  - www.cisco.com/go/security
  - www.cisco.com/go/evpn
  - www.cisco.com/go/securityassociates
- Networking Professionals Connection (forums.cisco.com)
- Improving Security on Cisco Routers
  - http://www.cisco.com/warp/public/707/21.html
- Essential Cisco IOS Features Every ISP Should Consider
  - http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
- Increasing Security on IP Networks
  - http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm
- www.cert.org
- www.sans.org