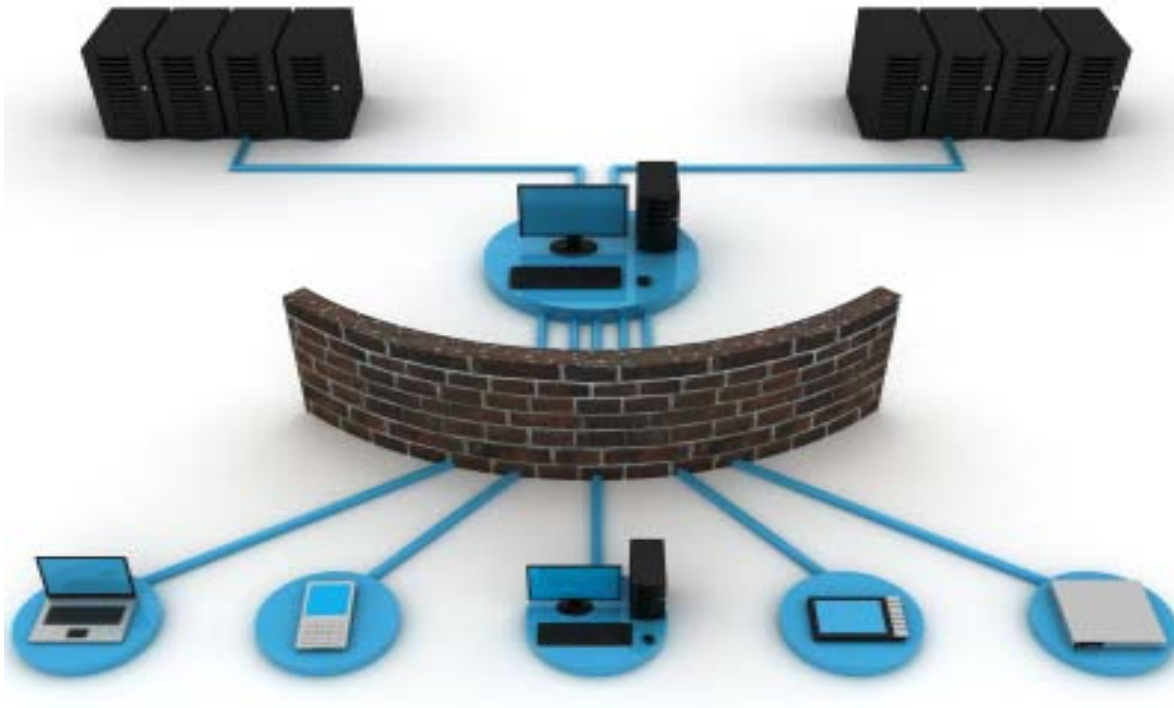


Network Security

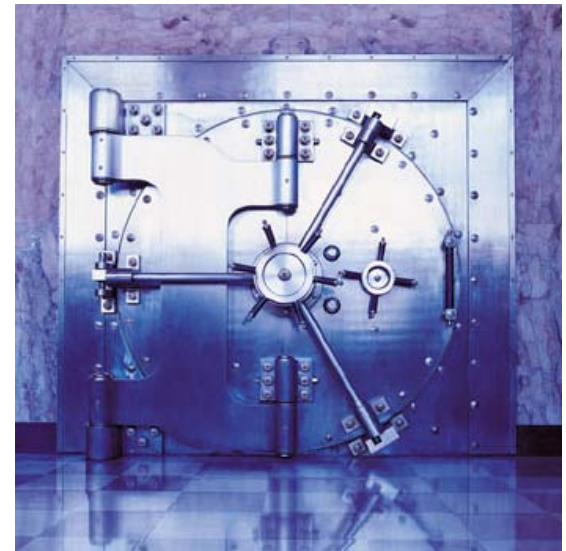


Amir Vossough Nov2009
vosough@aryahamrah.com



Overview

- What is security?
- Why do we need security?
- Who is vulnerable?
- Common security attacks and countermeasures
 - Firewalls & Intrusion Detection and Prevention Systems
 - Denial of Service Attacks
 - TCP Attacks
 - Packet Sniffing
 - Social Problems



What is “Security”



■ Dictionary.com says:

- 1. Freedom from risk or danger; safety.
- 2. Freedom from doubt, anxiety, or fear; confidence.
- 3. Something that gives or assures safety, as:
 - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
 - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
 - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm’s smaller plant.

...etc.

Why do we need security?



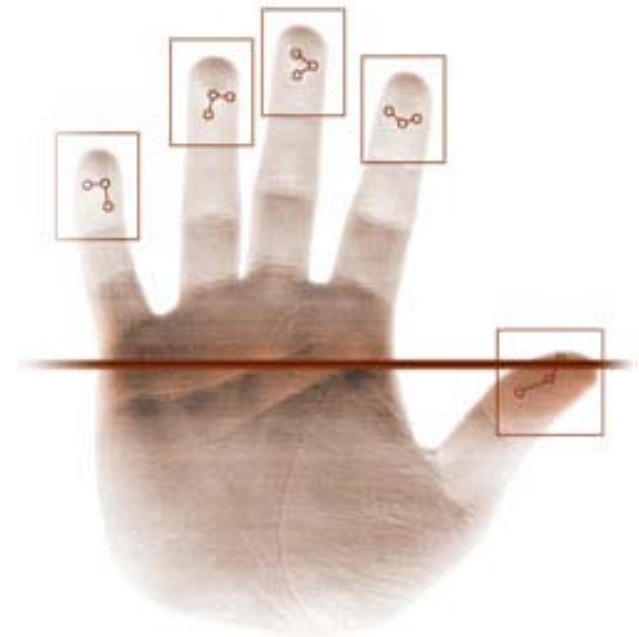
- Protect vital information while still allowing access to those who need it
- Provide authentication and access control for resources
- Guarantee availability of resources

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Attacks, their countermeasures

- Finding a way into the network
 - Firewalls
- Exploiting software bugs, buffer overflows
 - Intrusion Detection and Prevention Systems
- Denial of Service
 - Ingress filtering, IDS, IPS
- TCP hijacking
 - IPSec
- Packet sniffing
 - Encryption (SSH, SSL, HTTPS)
- Social problems
 - Education



Firewall

In construction, a firewall is a fire-resistance rated wall assembly intended to slow the spread of fire from one side to the other



Firewalls



- **Basic problem: Many network applications and protocols have security problems that are fixed over time**
 - **Difficult for users to keep up with changes and keep host secure**
 - **Solution**
 - Administrators limit access to end hosts by using a firewall
 - Firewall is kept up-to-date by administrators
 - Firewall: computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet)

Firewalls



- A firewall is like a castle with a drawbridge
 - Only one point of access into the network
- Can be hardware or software
 - Some routers come with firewall functionality
 - ipfw, ipchains, pf on Unix systems, Microsoft ISA-Server, Windows XP and Mac OS X have built in firewalls

Intrusion Inspection



- Used to monitor for “suspicious activity” on a network and protect it against them
 - **Intrusion prevention system (IPS)** is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

Intrusion Inspection



- **Stateful Packet Inspection** is done by firewalls that keeps track of the state of network connections. Stateful firewalls just checks the header portion of a packet
- **Deep Packet Inspection (DPI)** is the act of any IP network equipment which is not an endpoint of a communication using any field other than the layer 3 destination IP address for any purpose.

Dictionary Attack



- We can run a dictionary attack on the passwords
- This is why your passwords should be meaningless random junk!

Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
 - SYN flooding
 - SMURF
 - Distributed attacks
 - Mini Case Study: Code-Red

Denial of Service

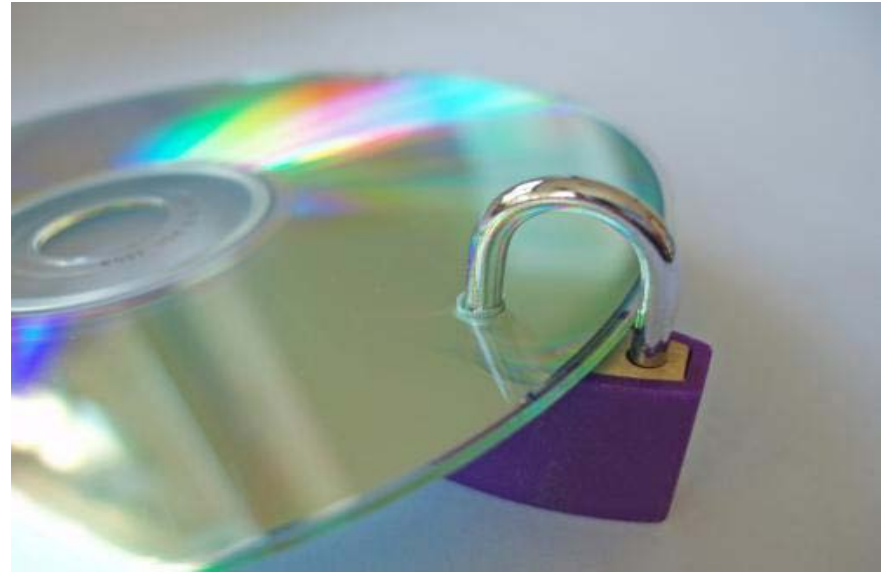
- How can we protect ourselves?
 - Ingress filtering
 - If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it
 - RFC 2267 has more information about this
 - Stay on top of CERT advisories and the latest security patches
 - A fix for the IIS buffer overflow was released **sixteen days before CodeRed** had been deployed!

TCP Attacks



- Recall how IP works...
 - End hosts create IP packets and routers process them purely based on destination address alone
- Problem: End hosts may lie about other fields which do not affect delivery
 - Source address – host may trick destination into believing that the packet is from a trusted source
 - Especially applications which use IP addresses as a simple authentication method
 - Solution – use better authentication methods

TCP Attacks



- How do we prevent this?
- IPSec
 - Provides source authentication
 - Encrypts data before transport

Packet Sniffing



- Recall how Ethernet works ...
- When someone wants to send a packet to some else ...
- They put the bits on the wire with the destination MAC address ...
- And remember that other hosts are listening on the wire to detect for collisions ...
- This works for wireless too! In fact, for any broadcast-based medium

Packet Sniffing



- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
 - Passwords are the most popular

Packet Sniffing



- How can we protect ourselves?
- SSH, not Telnet
 - Many people at CMU still use Telnet and send their password in the clear (use PuTTY instead!)
 - Now that I have told you this, please do not exploit this information
 - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
 - Especially when making purchases with credit cards!
- SFTP, not FTP
 - Unless you *really* don't care about the password or data
- IPSec
 - Provides network-layer confidentiality

Social Problems



- People can be just as dangerous as unprotected computer systems
 - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
 - Most humans will breakdown once they are at the “harmed” stage, unless they have been specially trained
 - Think government here...

Social Problems



■ Fun Example :

- Someone calls you in the middle of the night
 - “Have you been calling Egypt for the last six hours?”
 - “No”
 - “Well, we have a call that’s actually active right now, it’s on your calling card and it’s to Germany and as a matter of fact, you’ve got about \$2000 worth of charges on your card and … read off your AT&T card number and PIN and then I’ll get rid of the charge for you”

Social Problems



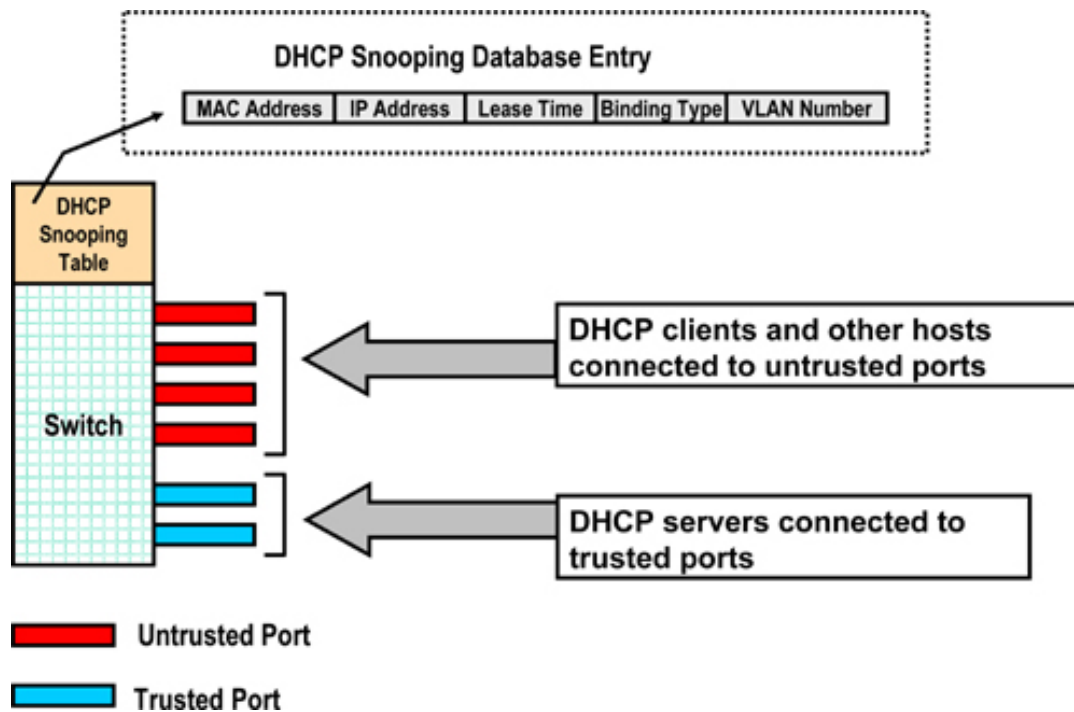
- There aren't always solutions to all of these problems
 - Humans will continue to be tricked into giving out information they shouldn't
 - Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
- So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information
 - But, this solution is still not perfect

Switching Security

■ DHCP Snooping

- The DHCP Snooping feature provides network protection from rogue DHCP servers. It creates a logical firewall between untrusted hosts and DHCP servers. The switch builds and maintains a DHCP snooping table (also called DHCP binding database). In addition, the switch uses this table to identify and filter untrusted messages from the network. The switch maintains a DHCP binding database that keeps track of DHCP addresses that are assigned to ports, as well as filtering DHCP messages from untrusted ports. For incoming packets received on untrusted ports, packets are dropped if the source MAC address does not match MAC in the binding table entry.

DHCP Snooping



802.1X Port-Based Authentication

802.1X defines 802.1X port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

Until a client is authenticated, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which the client is connected. After authentication succeeds, normal traffic can pass through the port.

Logging network activities

Every network device on your network has some type of logging capability. Switches and routers are extremely proficient in logging network events. Your organization's security policy should specify some level of logging for all network devices. Your access lists surely contain the log command for all denied ports and protocols. It's important to deny traffic you don't want in your networks, but you also need to know who's sending that traffic. Some resourceful hacker could be hammering away at your outside interface and eating up bandwidth and processes. You need to know where that traffic is coming from. But the truth is that admins typically don't log routers and switches. When a problem occurs, we just reboot them or bounce an interface, and then chalk it up to a hardware glitch. Don't go another day without setting up a centralized logging server.

Routers and switches will send log traffic on UDP 514 in a syslog format. It's just a matter of providing a secure platform to collect that information. I recommend setting up a Linux box to handle the traffic. It's simple and inexpensive, and it provides data security to some of the most valuable information about your network.