

# Internet Security

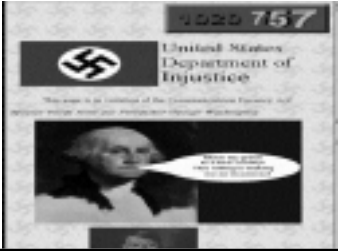
*“Securing Your Internet Company”*

**Presenters :-**  
 Matthew Morin  
 Jitender Miglani  
 Gail Slawson  
 Genhu Li

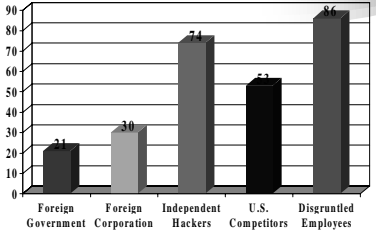
**March 10, 2000**

## *What is Computer Security on the Internet?*

- Much more than hackers!



## *Likely Sources of Attack*



Source	Percentage
Foreign Government	21
Foreign Corporation	30
Independent Hackers	74
U.S. Competitors	53
Disgruntled Employees	86

CSFBI 1999 Computer Crime and Security Survey  
 Source: Computer Security Institute  
 460 Respondents

## *What is Computer Security on the Internet?*

- It covers:
  - Accidental loss and/or damage
  - Insiders
  - Hackers
  - Espionage
  - Viruses
  - ... any other financial loss introduced through the networked environment.

## *Why Should I Care About Security?*

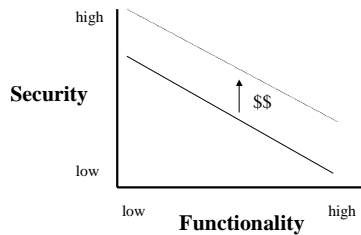
- Pros:
  - Web site generates 100% of revenue
  - Only link to our customers
  - Failure / disruption = loss of market
  - Plan on being bigger
- Cons
  - Costs money, time, and expertise (opportunity)
  - May have more to lose by being safe and slow than fast and loose.

## *Definition of Computer Security:*

Computer security is the definition, implementation, and enforcement of a policy which will determine who can use a resource and how that resource is to be used.

*William Yang  
 Ohio State Supercomputer Center*

## Fundamental Concept



## What is the Threat?

- Unauthorized Access
- Unlawful Monitoring (sniffers)
- Theft of Information
- Destruction of Information
- Denial of Service
- Viruses
- Trojan Horses
- Unlawful / Inappropriate Activities
- Shotgun Probes

## CEO's View of Security

"Buy enough locks, build enough walls, and hire enough guards so that I can be relatively assured that my business will be there in the morning."

Would you be able to sleep at night knowing that a disgruntled employee, hacker, or competitor could destroy your company with a few keystrokes?

## Security Framework

- Prevention
- Detection
- Response

## Prevention

- Security Policy
- Firewalls
- Encryption basics
- SSL/S-HTTP
- VPNs
- PGP
- Backup Policy

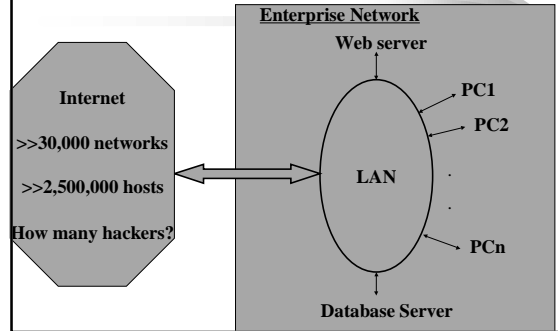
## Security Policy

- Network Layout and Growth Policy
- Internet/email usage Policy
- Account access Policy
- Information access Policy
- Physical access

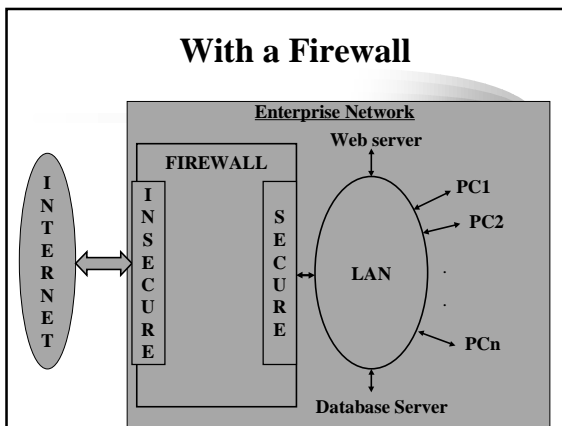
## Firewall

- A Firewall is a system that protects your internal network from an external untrusted network.
- Firewall enforces an Access Control Policy
  - All are allowed except a few
  - All are denied except a few
- Firewall can be a combination of hardware and software

## Without a Firewall



## With a Firewall



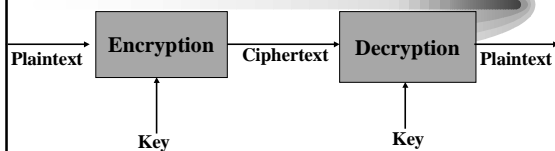
## Firewall - Which one to go for ?

Look for :

- OS required/other OSs supported ?
- CPU/RAM/Disk space ?
- Authentication scheme ?
- Logging supported ?
- Hardware Provided ?
- Price ?
- Other features ?

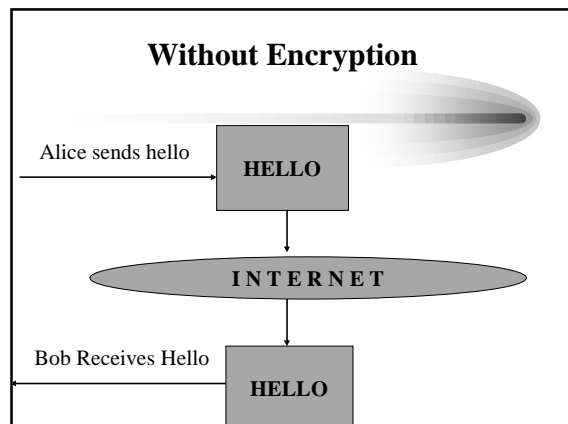
Source : [http://www.data.com/Lab\\_Tests/Firewalls.html](http://www.data.com/Lab_Tests/Firewalls.html)

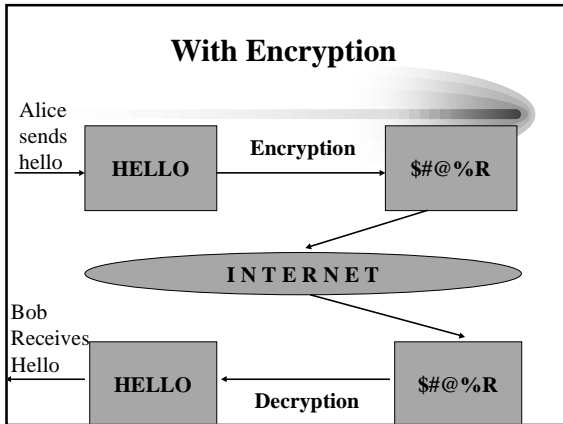
## Encryption basics



- Encryption - Process of disguising a message
- Decryption - Process of recovering a message from its ciphertext

## Without Encryption





## SSL/S-HTTP

### SSL-Secure Socket Layer

- Developed by netscape to provide security over the Internet
- creates a secure encrypted channel of data

### S-HTTP - Secure-Hyper Text Transfer Protocol

- Another protocol to provide security over Internet
- Limited to specific software implementing it
- encrypts each message individually

## VPN - Virtual Private Network

- To enable communication between different branch offices over Internet
- Provides remote data access securely to business partners and employees
- reduces the cost of communication by 23-50%

**RADIUS** - Remote Access Dial In User Service

- A way to implement VPNs
- supports authentication, authorization and accounting for remote users

## PGP - Pretty Good Privacy

- Freeware electronic mail security Program
- Uses public key encryption. So, To communicate one need not agree on a secret key first.
- Can be used for authentication of messages as well. So, one can know exact origin of messages
- Available on a wide variety of Platforms

• To obtain PGP freeware, go to :  
<http://web.mit.edu/network/pgp.html>

## Backup Policy

- Make full Backup of your machine. Perform Incremental backups daily and full backups at week-ends.
- Use CD-R or Tapes to backup your data
- Use backup software according to your platform

• otherwise, contact online data backup services providers  
[www.backupnet.com](http://www.backupnet.com)  
[www.offsite.com](http://www.offsite.com)

## Detection of Security Breach

### Why do we care about detection?

- Loss of Time/Money
- Loss of Data
- Loss of System Availability
- Loss of Reputation

If some 16 year old punk hacks in and “owns” your system - will you be able to sleep well at night?

## Detection of Security Breach

### What are we trying to detect?

- Computer Viruses
- Trojan Horses
- Sniffers (wire taps)
- Password Crackers
- Denial of Service Attacks



## Detection of Security Breach

### How do we detect security breaches?

- Notification from protection software
- Routinely check network logs
- User Awareness:
  - System running slow
  - Can't save - out of disk space
  - Can't run applications
  - Data is missing
  - Passwords don't work
  - More junk than usual in e-mail inbox



## Detection Software

### • Virus & Trojan Horse Detection

- McAfee (NAI) [www.mcafee.com](http://www.mcafee.com) [www.nai.com](http://www.nai.com)
- Norton AntiVirus (Symantec) [www.symantec.com](http://www.symantec.com)



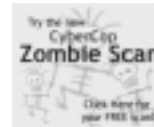
South Park Trojan



## Detection Software

### • Denial of Service

- Sniffer Technologies [www.nai.com](http://www.nai.com)
- CyberCop Zombie Scan [myCIO.com](http://myCIO.com)



## Detection Software

### • Intrusion Detection

- CyberCop (Network Associates) [www.nai.com](http://www.nai.com)
- Norton Internet Security 2000 [www.symantec.com](http://www.symantec.com)



## Local Security Experts

### Call in the Network/Security Experts:

- CyberCom, Inc. [www.cybercominc.com](http://www.cybercominc.com)
- ComTest [www.comtest.com](http://www.comtest.com)

## Response

I've been hit with a Denial of Service Attack. None of my customers can reach me. HELP!

**SOLUTION:** Contact your upstream service provider (ISP) and ask for help.

## Response

A hacker has root level access to my host. What do I do?

1. Take off the site from network;
2. Try to figure out how the compromising;
3. Reinstall Operating System (OS);
4. Reinstall all critical patches;
5. Reinstall the software, and try again !

## Response

Several customers are complaining about bad charges on their credit cards, and they're blaming me. What's up with that?

There's a good chance a hacker grabbed your credit card database  
Solution: Don't do anything and hope the problem goes away.

**WRONG! WRONG!! WRONG!!!**

Contact the credit card fraud departments, clean up the mess, and hope your customers forgive you.

## Response

- Should you contact law enforcement?
  - Cons
    - Bad publicity
    - Loss of control
    - Best handled through civil action
  - Pros
    - Law Enforcement has unique tools
    - Justice is done
    - Civic duty (Internet is a global community)

## *Some useful online links*

- [www.2600.com/hacked\\_pages](http://www.2600.com/hacked_pages)
- [www.hackernews.com/defaced](http://www.hackernews.com/defaced)
- [www.rootshell.com](http://www.rootshell.com)
- [www.cert.org](http://www.cert.org)
- [www.gocsi.com](http://www.gocsi.com)
- [www.hackers.com](http://www.hackers.com)
- [www.cs.purdue.edu/coast/coast.html](http://www.cs.purdue.edu/coast/coast.html)

## Summary



Questions  
or  
Comments

?