Network Security

Carmela Troncoso, KU Leuven (COSIC)

Computer Security Course, University of Vigo

22nd-July-2009

Not a fully traditional Network Security talk

- I won't explain what a network is
- I won't explain the OSI architecture, TCP, IP, ...
- I won't explain the any packet format
- I won't explain how to exploit the finger, nmap,... commands
- I want to convince you that it is an issue and give hints on how and where to find solutions

Outline

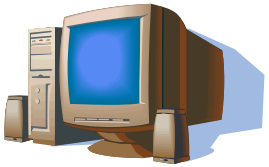
- Introduction
- Threats
- Firewalls
- IDS
- Peer-to-peer

History

- 50-60s: Mainframe computer

- 60-70s: terminals connected to the mainframe
  - Several users on one computer

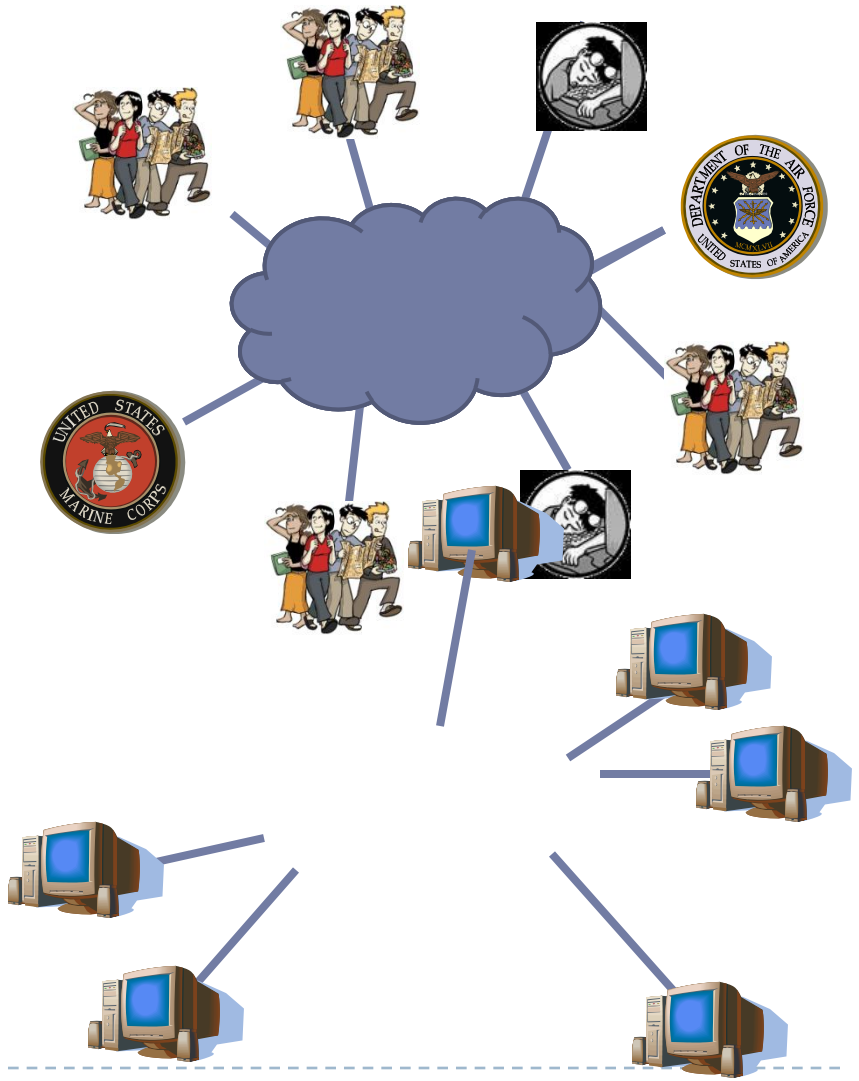
- 70-80s: PC
  - One user one computer



- 90s-Now: Networked PCs
  - and servers, databases, clouds,...
  - Untrusted content
  - Untrusted code running
  - ...

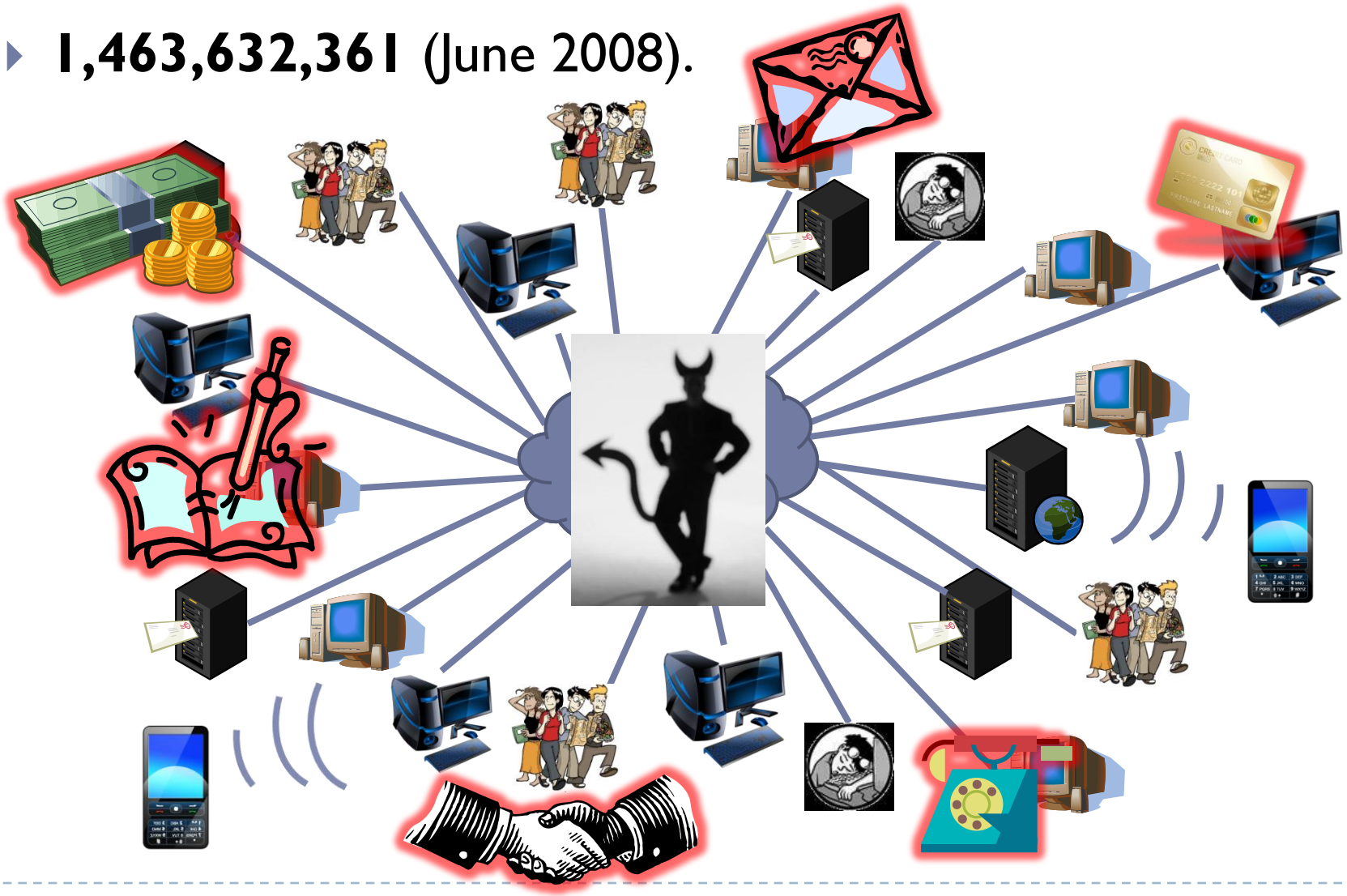
Security was not a design criterion

- ARPANET (1969)
  - DoD&Academy
  - Link mainframe computers
  - Optimized for availability
  - 4 hosts
- Internet and Milinet (1983)
  - 562 hosts
  - TCP/IP
- Pizza Hut offers pizza ordering (1994)
  - Almost 4M hosts of all kinds



Now

- **1,463,632,361** (June 2008).



Threats

What do bad guys do?

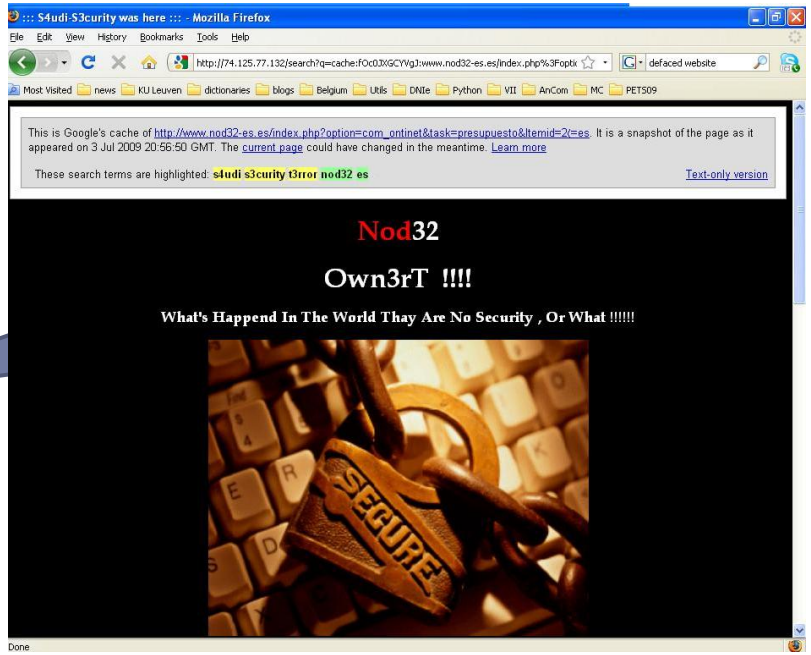
- Passive eavesdropping
  - Industrial espionage
  - National security
  - Bank information to be reused
- Unauthorized access to resources
  - Password cracking/stealing/guessing
- Impersonations
  - Spoofing IP addresses or hijack connection
- Web defacement
  - Ideology, fun, challenge
- Denial of service
  - Shutdown the network

Whom are they bad with?

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

Website defacement

- Common security incident
  - 400 between 1st-13th July 2009



Source: http://www.zone-h.org

8th July 2009 - S4udi-S3curity-T3rror

- Admin mistakes, known vulnerability OS, social engineering,...
- Even automatic: *MultiInjector v0.3* released
  - Automagically join the Administrators family on DB machine
  - Automatic defacement: Try to concatenate a string to all user-defined text fields in DB

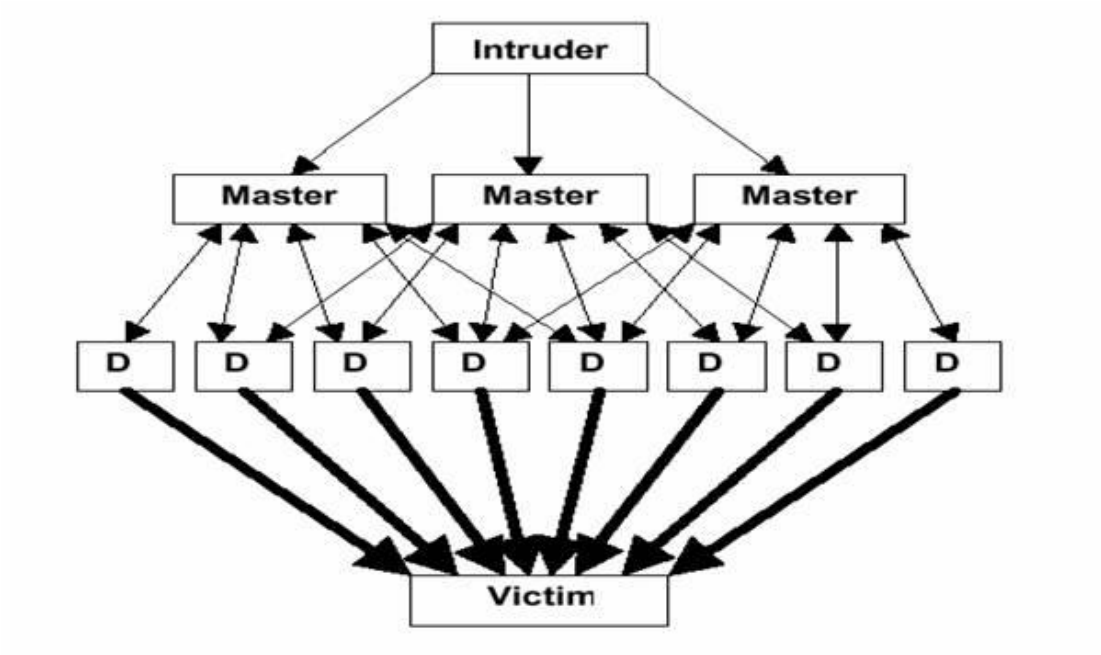
Denial of Service

- Deprive legitimate users to access one service
- Flood the web server until:
  - Send CPU utilization to 100%
  - Crash the OS
  - Crash a vital service
- In each case the legitimate users of the computer are affected

Simple DoS: “Smurfing”

Source: Craig A. Huegen CISCO SYSTEMS

Complex: DDoS



- A DOS attack is launched from many "zombie" locations simultaneously; each must be identified and stopped

Slammer Worm (2003)

- Spread worldwide in 8 min
  - Double each 8.5 seconds
  - Estimated damage ~1M $
    - **Bank of America** Many ATMs unavailable on Saturday, some other financial services affected
    - **Continental Airlines** Some flights delayed or canceled because of online ticketing and electronic check-in problems
    - **Microsoft** Windows XP can't be activated
    - ...
  - Simple: exploit buffer overflow, resend to random IP
- Vulnerability had been announced and patched by Microsoft 6 months earlier to the day

Backdoors

- Software enables outsiders to access system remotely
  - Trojan horses
  - Back Orifice (1997): client-server architecture
- Purpose
  - Deletion of files
  - Modification of files
  - Uploading of files
  - Downloading of files (e.g. passwords, credit card information)
  - Use of the machine to launch DDoS attacks
  - Keystroke logging
  - Viewing the user's screen

Social engineering

- Why try complicated tricks when you can just ask?

- Impersonate person with legitimate need for information
  - Phone call
  - Phishing (eBay, PayPal,...)

	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of unique phishing email reports received by APWG from consumers	24,007	33,928	33,261	34,758	24,357	23,187
Number of unique phishing web sites detected	21,507	26,303	27,209	27,739	19,480	15,709
Number of brands hijacked by phishing campaigns	237	231	229	264	269	252
Country hosting the most phishing websites	USA	USA	Sweden	USA	USA	USA
Contain some form of target name in URL	52.52 %	89.13%	63.18%	60.87%	16.62%	67.89%
No hostname; just IP address	5.94%	0.74%	0.29%	0.26%	1.17%	5.80%
Percentage of sites not using port 80	0.43%	0.06 %	0.01%	0.01%	0.03%	0.13%

Source: http://www.antiphishing.org/ Phishing Attack Trends Report - Second Half 2008

The monetization of the malware

- A network can be a valuable asset
  - More computers = more computing power
  - More computers = more bandwidth

- Botnets: collection of *zombie* computers running software
  - Can be rented to spammers
  - Can be rented to phishers
  - Can be used as a threat (DDoS)
  - Only 100$ per hour...

Further reading: **"Spamalytics: An Empirical Analysis of Spam Marketing Conversion"**
C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage
Proceedings of the 15th ACM Conference on Computer and Communications Security (ACM CCS), Alexandria, Virginia, pp. 3-14 October 2008

Defenses: Secure Protocols

Network Security Protocols

- SSL/TLS
  - Secure sockets layer / Transport layer security
  - Used mainly to secure Web traffic

- IPsec
  - IP-level security suite
  - Network layer security

SSL/TLS

- Mid '90s introduced concerns over credit card transactions over the Internet
- SSL designed to respond to these concerns, develop e-commerce
- Initially designed by Netscape, moved to IETF standard later

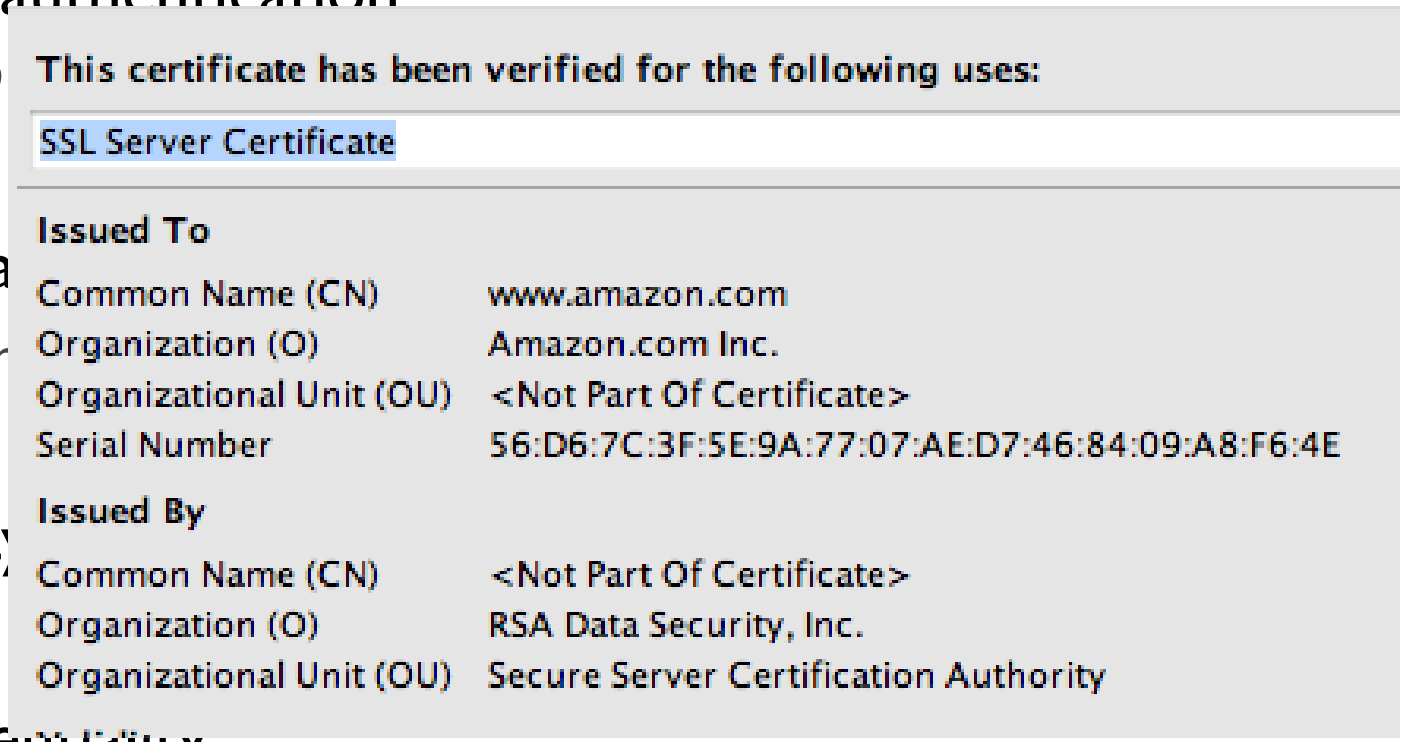
SSL model

- Client server architecture

- Implements a socket interface
  - Any socket-based application can be made to run on top of SSL
- Protect against:
  - Eavesdroppers
  - MITM attacks

SSL protections

- Server authentication
  - X.509
- Client a
  - Deper
- Integrity
- Confidentiality

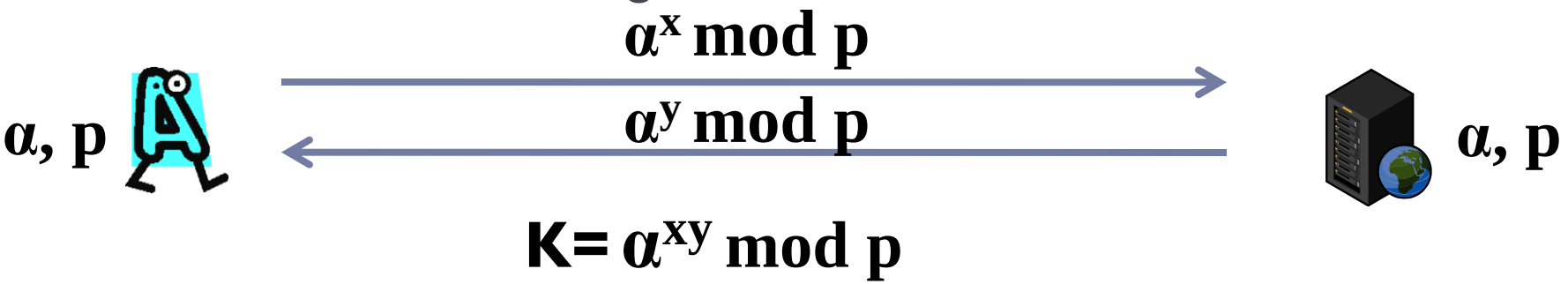


SSL Handshake

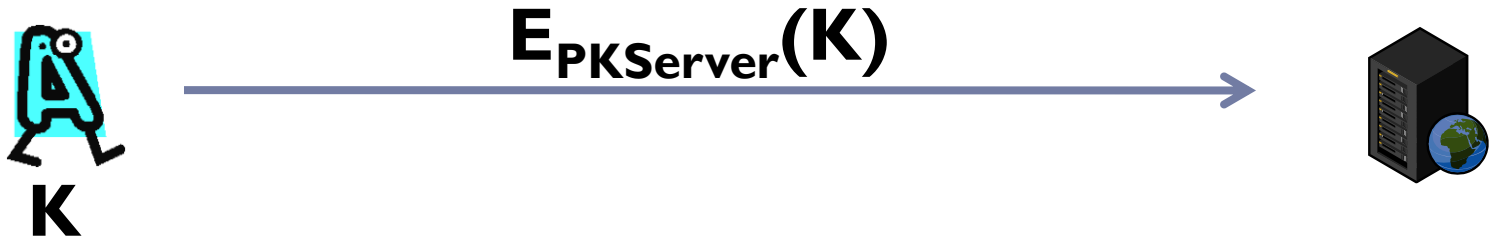
- Negotiate parameters
  - Client and server exchange their capabilities:
    - cipher suites
    - key exchange algorithms
      - Earlier versions used 40-bit keys for export reasons
      - Later versions switched to 128-bit keys, with an option to use 40-bit ones with legacy servers/client
    - protocol versions
- Key exchange and authentication
  - They generate a key for the communication
  - Client authenticates server (vice versa)
- Then encrypted session follows

SSL key exchange

- Client and server establish a common key for the rest of the communication
  - Diffie Hellman exchange



  - RSA-based key exchange
    - Encrypt secret *K* with public key of server



SSL authentication

- Anonymous (no authentication)
- RSA authentication (implicit)
- Sign Diffie-Hellman parameters
  - Station To Station Protocol
  - Achieves *perfect forward secrecy*

Perfect forward secrecy

- Suppose Client sends credit card to Server over SSL today
- Suppose tomorrow Eve breaks the Server's key
  - Want credit card to remain secure
- What happens with RSA key exchange?
- What happens with Diffie-Hellman?

SSL counter arguments

- Hard to set up
  - Expensive certificates
  - Resource-intensive
- Insufficient verification
  - Do people notice the lock icon?
  - Do people check the URL?
- Improper use

IPsec

- Part of IPv6 suite
  - One of the key features v6 was supposed to bring
  - Backported to IPv4
- Two options: AH (authentication) and ESP (encapsulated security)
- Two modes: transport and tunnel

AH vs EPS

- Authentication (AH)
  - Simple design: add header with authentication data
  - Security parameters
  - Authentication data (usu. SHA1-HMAC)

- Encapsulated mode (EPS)
  - Encapsulate datagram rather than add a header
  - Encrypt & authenticate

Transport vs. Tunnel Mode

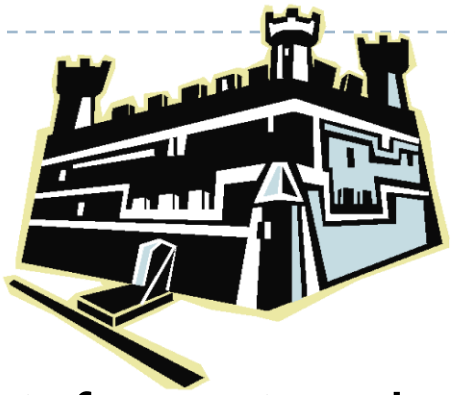
- Transport mode: add headers to IP
  - data protected but header left in clear
  - can do traffic analysis but is efficient
- Tunnel mode: rely traffic through "untrusted cloud"
  - Encapsulates an entire IP packet within a new IP packet
  - Virtual Private Networks

IPsec discussion

- Deployment of IPsec limited
- Some reasons
  - Global PKI infrastructure hard to set up
  - Fixes a "solved" problem
    - SSL & SSH work well
- IPsec success: VPN

Defenses: Firewalls

What is a firewall?



- Analogous to a gatehouse in a castle
  - Only entrance point
- HW or SW monitors packets of digital information that enter or leave a network
  - Enforces security policy
  - Eliminate unwanted traffic (filtering)
  - Create security domains
- They are only a part of the solution
  - Physical security, employees education,...

Security tasks

- Restrict access to the outside (proxy role)
- Protects critical resources against attacks (DDoS, worms, trojans,...)
- Enable documentation
  - weak points
  - auditing
- Provide authentication

Packet filtering

- Key functionality
  - Also port filtering, application filtering, content filtering
- Transport layer
- Filters depending on header data
- Should not take up much bandwidth

Stateless vs Stateful

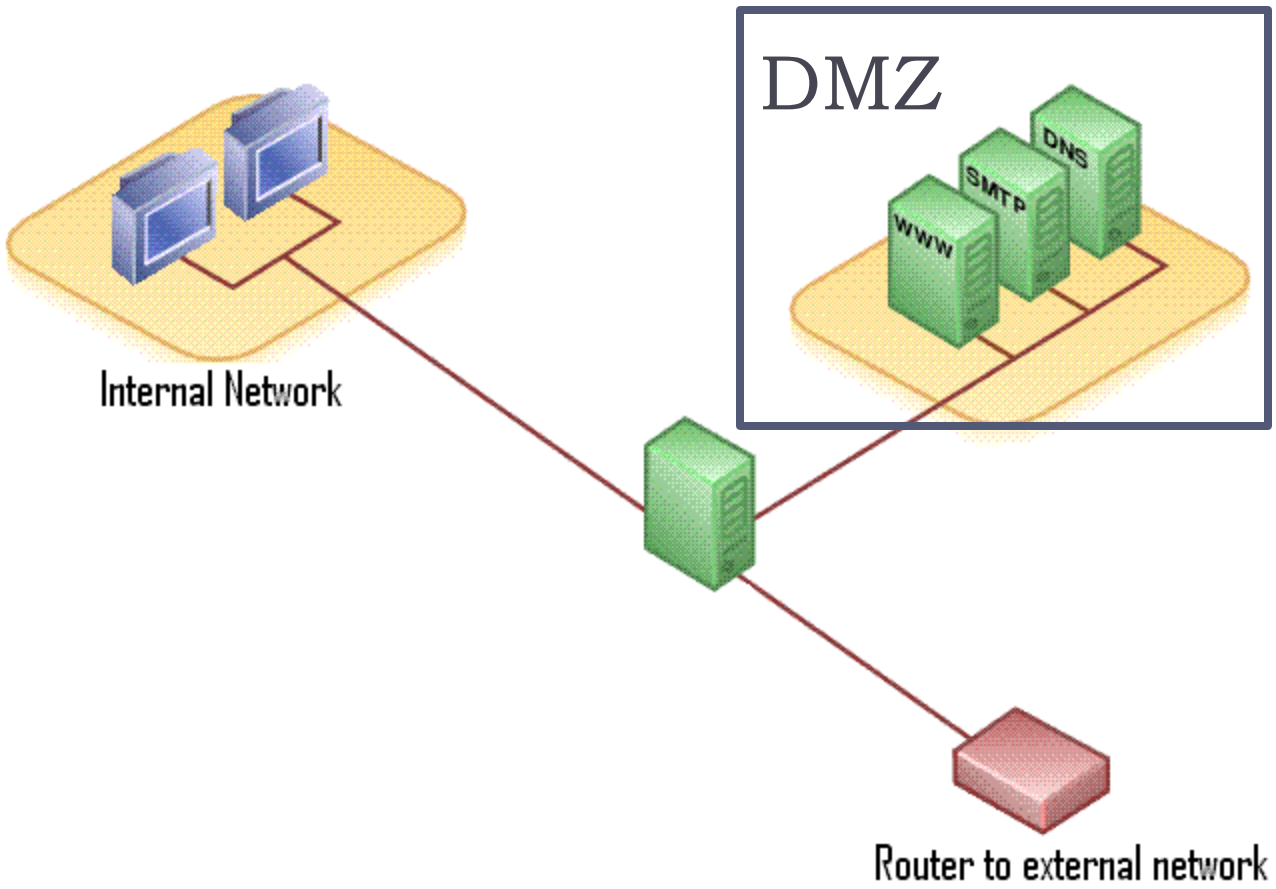
- Stateless packet filtering
  - Does not keep connection status information
  - Decision based on header values
  - Small overhead

- Stateful packet filtering
  - Keeps memory of the connection
  - Examines full packet
  - Drops packets that overload the server
  - Blocks packets from hosts not connected

Basic filtering rules

- Any outgoing packet
  - Must have a source address in your internal network
  - Must not have a destination in your internal network
- Any incoming packet
  - Must not have a source address in your internal network
  - Must have a destination in your internal network
- For
  - ICMP, UDP, TCP, IP

Usual configuration
Demilitarized Zone (DMZ)



Source: http://en.wikipedia.org/

Defenses: IDS

Intrusion Detection Systems

An Intrusion is any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource within an information system

- May or may not involve humans

- Passive: confidentiality breach
- Active: integrity and/or availability bridge

Intrusion indicators

- Actions that violate the security policy
- Reports from intrusion detection tools
- Unexplained incidents:
  - New user accounts
  - User accounts deleted
  - Unexplained change permissions to files
  - Unusual time usage
  - Unusual patterns
  - DoS

Signature analysis

- Uses "intrusion signatures"
  - Well known patterns of behavior
    - Ping sweeps, port scanning, OS fingerprinting, DoS attempts, etc.
- Examples
  - Connection attempt from a reserved IP address
  - Packet with an illegal TCP flag combination
  - Email containing a particular virus
  - Denial of service attack caused by issuing the same command thousands of times.

```
------------------------------------------------------------
X is a public SSH and IMAP(S) server. To prevent brute force
attacks only 5 connections/30 seconds are allowed from the same
source IP.
------------------------------------------------------------
```

Host-based IDS

- Monitors and analyses the internals of an individual computer
- Software based
- Inspects
  - Dinamyc behaviour: is Word modifying passwords?
  - Static Status: why is this software installed in my computer?
- Uses a database to compare the status of key files and resources
- Near Real-Time
- Keeps logs

Host-based IDS limitations

- Relatively high cost
  - ~40 $/unit
  - Expensive maintenance
- OS dependant
- Not perfect
  - Vulnerable to DoS
- If host is compromised, game over

Network-based IDS

- Monitors network traffic
  - denial of service attacks,
  - port scans
  - ...
- More than a Firewall
  - Which application is accessing what?
- Low cost (only few critical points)
- OS independent
- Detects also not-successful attacks

Network-based IDS limitations

- Cannot analyse encrypted traffic
- Generate more data in the network
- High-volume networks
- High false alarm rate
  - What is normal behaviour
  - How to train the system?

Other IDS systems

- Protocol-based intrusion detection system
  - monitors and analyzes the communication protocol.
  - e.g. HTTP protocol

- Application protocol-based intrusion detection system
  - monitors and analyzes the communication on application specific protocols
  - e.g. SQL protocol

Passive vs Reactive

- What to do when an intrusion is detected?

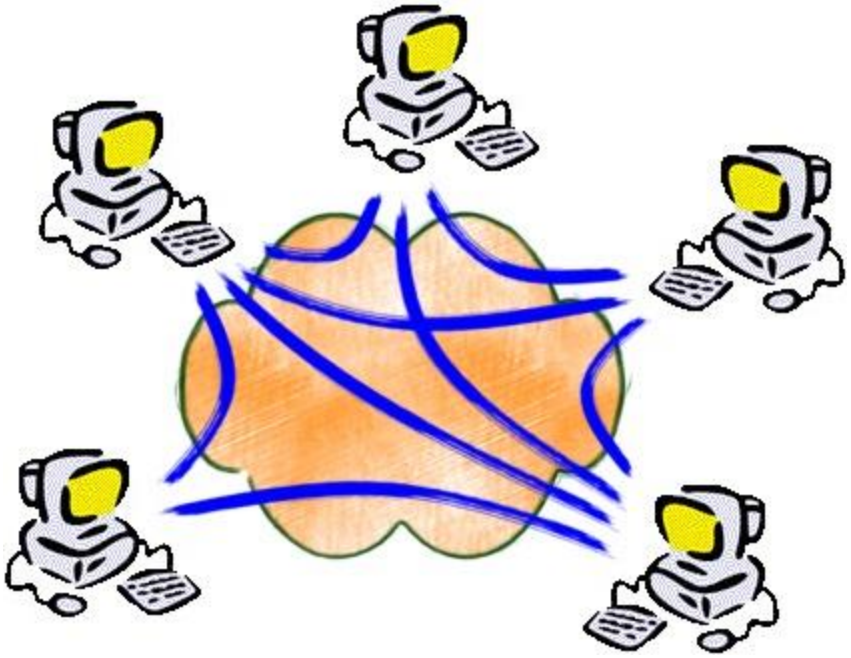
- Passive
  - Logs all information
  - Raises an alarm

- Reactive
  - Closes connection
  - Block source

Peer to peer security

Peer to Peer networks

- Partitions tasks work loads between peers.
  - Peers are equals
  - Sharing resources, censorship resistance
  - Ad-hoc connections



Source: HyperCast Project

Security issues

- Attacks
  - Sybil attack
  - Attacks in routing
- Free rider problem
  - Incentive models
- Anonymity
  - Publisher, requester, responder, mutual anonymity
  - How to achieve anonymity
  - This is other lecture... (Crowds, Salsa, ...)

Sybil attack

- P2P uses multiple entities for security reasons
  - Confidentiality: Secret sharing
  - Availability: Multiple routes
  - Integrity: Replication

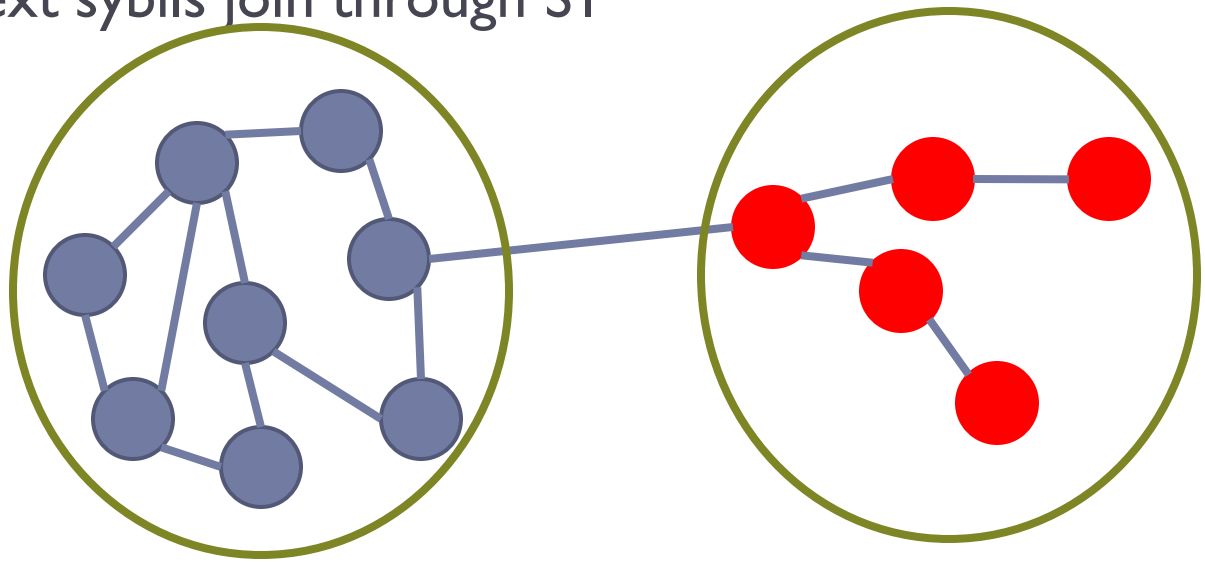
- An attacker can assume multiple identities
  - Route Table Poisoning
  - Break confidentiality
  - Attack replica set
  - In case of majority votes, be the majority.

Solutions?

- Can authentication help?
  - Only if identities can not be created cheaply.
- Limit the number of identities?
  - Use real physical identities
  - Who enters the data?
- Limit to IP address or port?
  - But many nodes behind a NAT possible. Use external identities?
- Limit to email adresses?
- A real limit?
  - Make it costly to create identity?
  - Use crypto…

Detecting sybils

- Assumption
  1. The first sybil S1 joins the P2P network through a random node
  2. Next sybils join through S1

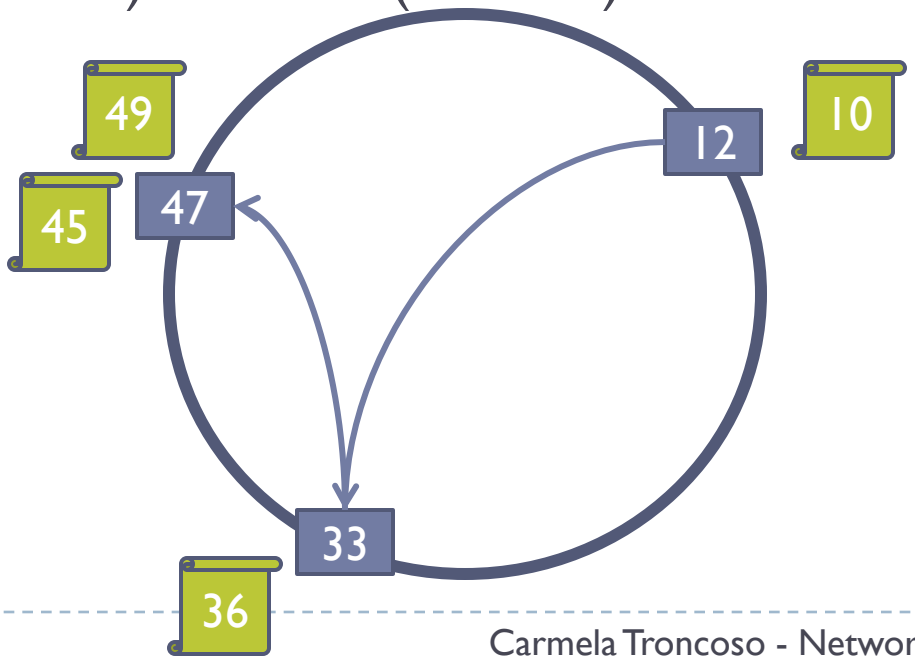


- Different pattern!
  - SybilGuard, SybilLimit, SybilInfer

Routing in P2P networks

- Central indexing (Napster)
- Neighbour search (Gnutella)

- Distributed Hash Tables
  - Contain tuple (k, content) k=hash(content)



Routing attacks

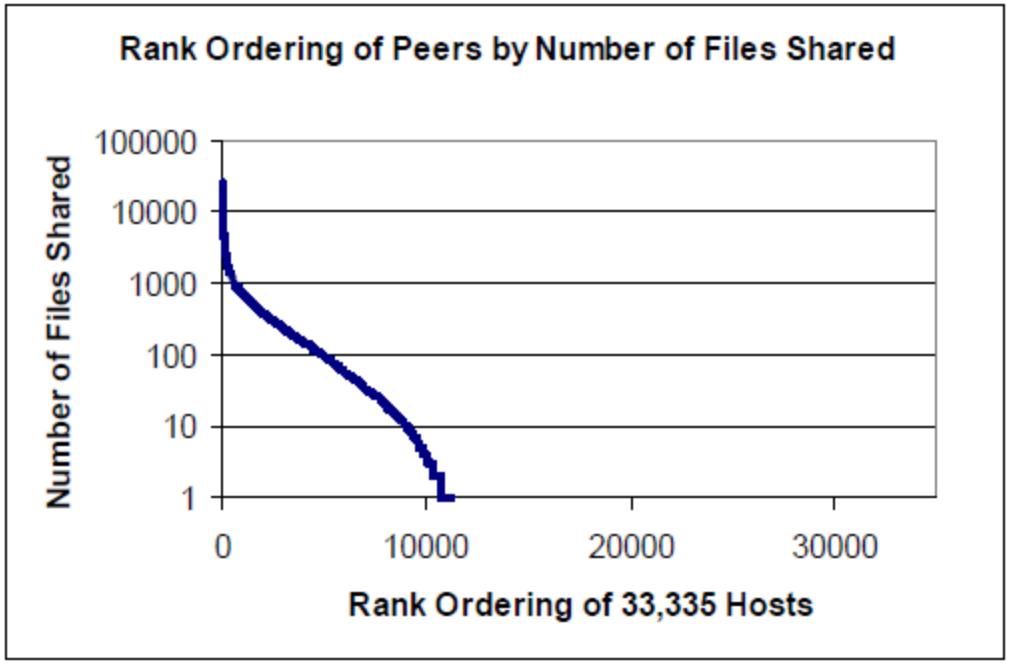
- Index Poisoning
  - Store bogus information in the DHT
  - e.g. links to nodes that do not have a file,
  - Redirect nodes requesting an item to attacker
- File Poisoning
  - Spamming the network with fake and corrupted files.
- Routing Table Poisoning
  - Add attacker nodes to the routing table of a node
  - Allows surveillance

Free riders

- Autonomous nodes need incentives to work together to
  - Forward messages, perform computations, share/store files
- But there are free riders
  - May not share any (interesting) content
  - May not forward messages
  - Reasons for not wanting to share
    - Security concerns
    - Does not want to consume its own network bandwidth/storage resources
- Consequences
  - Good peers are overloaded
  - Eventually content will not be reachable

Gnutella

- Only 30% of users share content
  - Only a 37% of this content is useful



Source: Free Riding on Gnutella by E. Adar , B. A. Huberman

Build incentives

- Tit-for-tat or Reciprocative
  - If you do something for me, I will do something for you
  - Between two nodes
  - Limited

- Shared History
  - Gets reward for services provided
  - Reputation, currency
  - Vulnerable to cheating and collusion
    - Sybil attack

Reputation vs Currency

- Reputation
  - Objective reputation
    - Everyone in the system agrees on the reputation of a node
    - Similar to currency
  - Subjective reputation
    - Each node computes reputation subjectively
    - Nodes A and B may observe different reputations for node X
    - Node A can take other trustable nodes into account for evaluating X
    - More popular scheme now
- Currency
  - A reward that is consistent in the entire system
  - Require well established infrastructure
    - How to avoid faking currency?
    - Can easily duplicate currency

Conclusions

- Network Security is a huge field
  - Firewalls
  - IDS
  - P2P
  - Botnets
  - DNS poisoning
  - Web security
  - Botnets
  - DNS poisoning
  - Web security
- Far from being there...
- ... and it only grows!
- I did not say much about it, but cryptography helps a bit

Further reading

- W. Stallins, "Cryptography and Network Security"

- William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, "Firewalls and Internet Security: Repelling the Wily Hacker."