Security Engineering
Part III – Network Security

Intruders, Malware, Firewalls, and IDSs

Juan E. Tapiador
jestevez@inf.uc3m.es
Department of Computer Science, UC3M

Intruders and Attacks

External
Internal
- masqueraders

External intrusion – common techniques
- Scan the network to find out
  - IP addresses in use
  - Operating systems
  - Open ports (network services)
- Run exploits
- Get access to shell, preferably with suid
- Install rootkits, use the system as a node in a botnet, launch further attacks from here, …

Homework:

CAPEC (Common Attack Pattern Enumeration and Classification)
- http://capec.mitre.org *(Methods of Attack)*

Firewalls

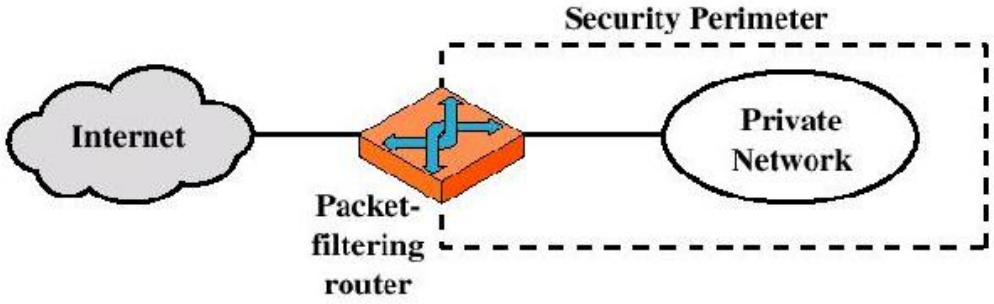
- Provide protection to a local network from network-based threats, while allowing access to the outside world

- General design principles
  - Establish a controlled link between Internet and your network
  - Provide a single choke point
  - All traffic must pass through the FW
  - Only authorised traffic, as defined by the local security policy, will pass through

- Common methodology
  - *Service control* – determine which Internet services can be accessed, inbound or outbound
  - *Direction control* – determine in which direction service traffic is allowed to flow
  - *User control* – determine who can access what
  - *Behaviour control* – determine how particular services are used

Firewalls

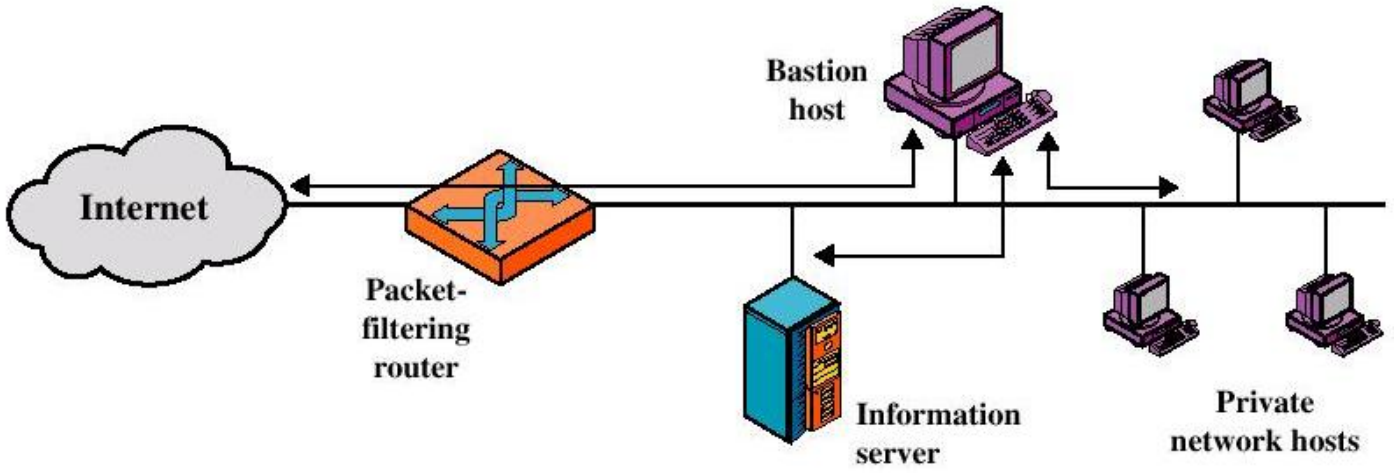
- **Types of FW** – Packet-filtering routers



- Applies set of rules to packets, then discards or forwards them
- Rules generally based on matching protocol fields
- Advantages:
  - High-speed, transparency to users, simplicity
- Disadvantages:
  - Lack of authentication, vulnerable to some attacks (IP address spoofing, fragmentation, …)

Firewalls

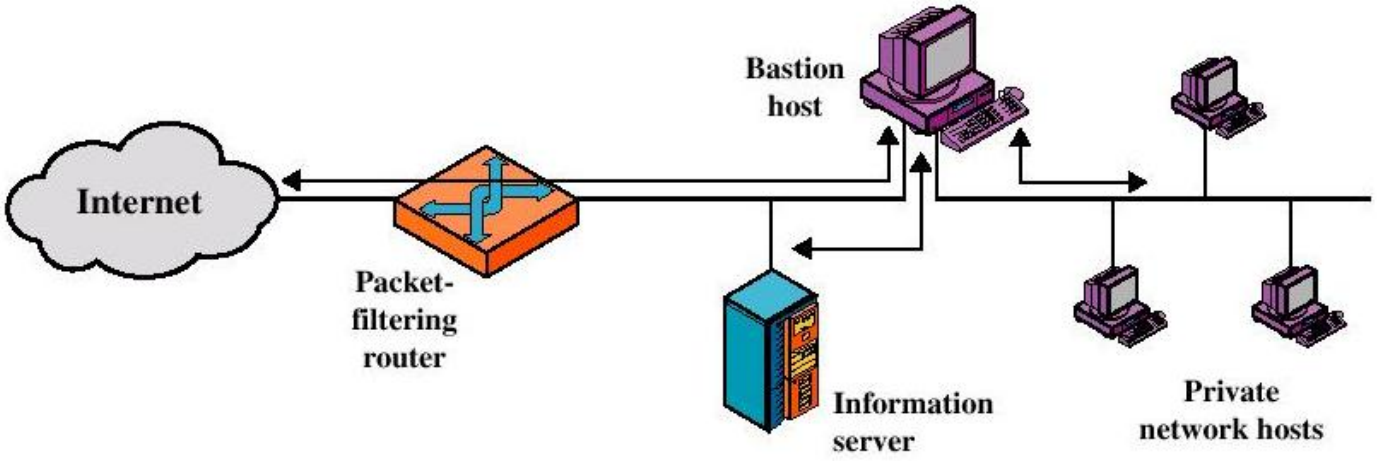
- **More complex (and secure) FW configurations**:
  - Screened host FW (single-homed bastion host)



- FW consists of 2 separate systems:
  - PF router: only packets from and to the bastion host are allowed
  - Bastion host: peforms authentication and proxy functions
- Attacker needs generally to penetrate both systems

Firewalls

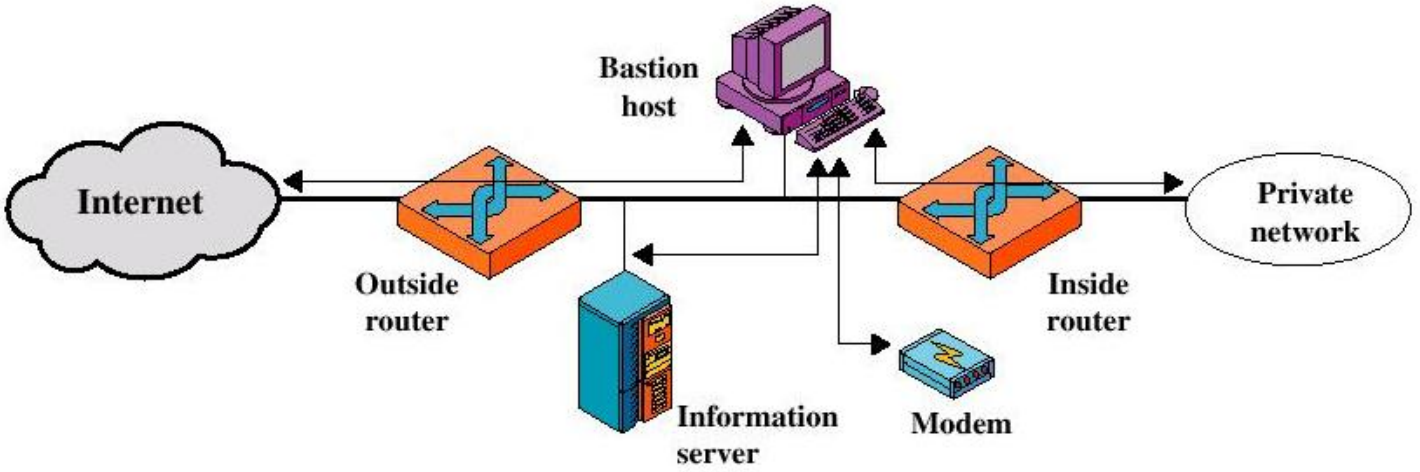
- **More complex (and secure) FW configurations**:
  - Screened host FW (dual-homed bastion host)



- Now traffic between Internet and the internal network has to physically flow through the bastion host

Firewalls

- **More complex (and secure) FW configurations**:
  - Screened subnet FW



- Most secure than previous ones
- 2 PF routers are used to create an isolated subnetwork (DMZ – Demilitarized Zone)
- External router advertises only DMZ, so internal network is “invisible”
- Internal router advertises only DMZ, so systems within private network cannot construct direct routes to Internet

Malware

- **What is a malware?**

  Code that run on your computer and make your system do something that an attacker wants it to do

- **What is good for?**
  - *Steal information*
  - *Delete files*
  - *Fraud (e.g., click fraud)*
  - *Use system as a relay*
  - *…*

- **Malware zoo**
  - Virus
  - Backdoor
  - Trojan horse
  - Rootkit
  - Worm
  - Scareware
  - Adware
  - Spyware (including keyloggers)
  - Botnets / zombies
  - …

  Terminology quite fuzzy nowadays

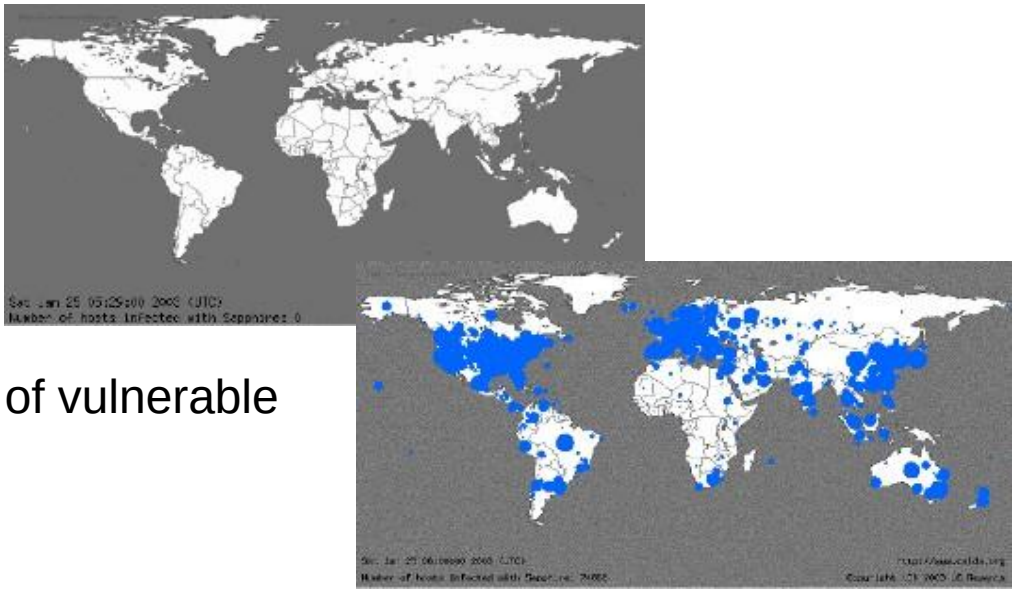
Malware

- **Virus**
  - Program that can infect other programs by modifying them to include a (possibly evolved) version of itself
  - Some types:
    - *Polymorphic*
      - Uses an engine to mutate after each infection, while keeping the engine intact
    - *Metamorphic*
      - Changes (almost) completely after each infection
- **Trojan**
  - Class of malware that appears to perform a desirable function but in fact performs undisclosed malicious actions that allow unathorised access to the victim’s computer or data

Malware

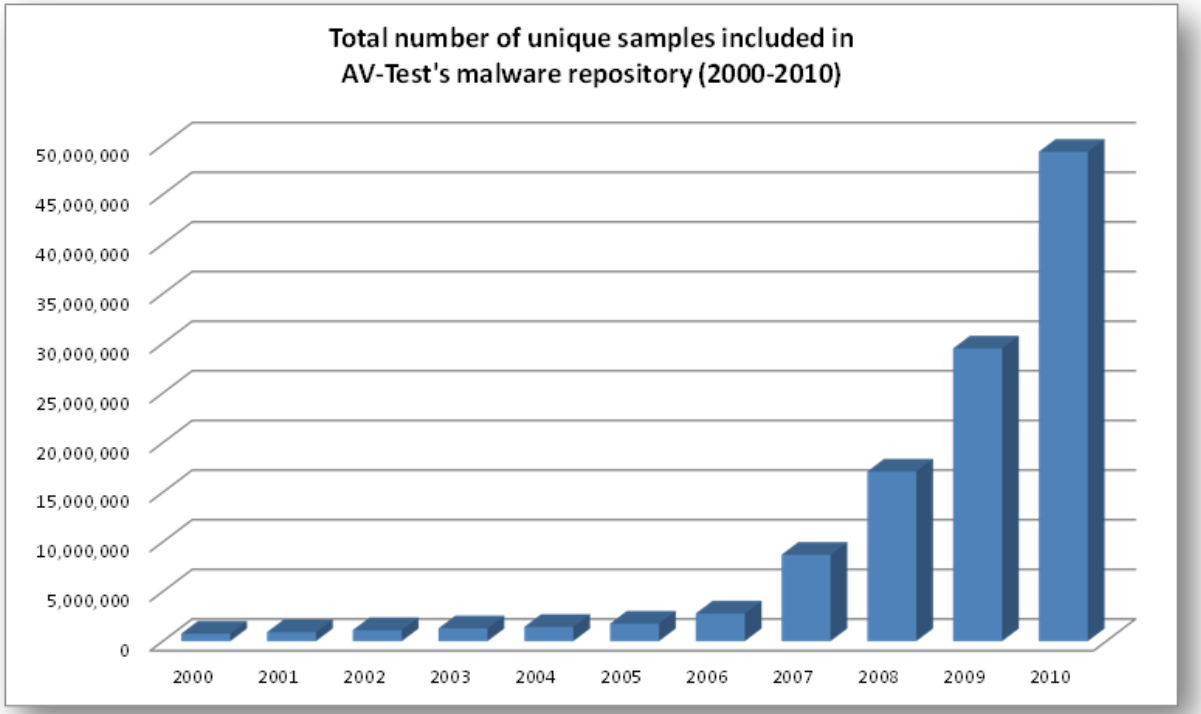
- **Rootkit**
  - Component that uses stealth to maintain a persistent presence on the system

- **Worm**
  - Self-replicating computer program that uses a network to send copies of itself to other nodes without user intervention
  - Slammer: infected most of vulnerable Internet in 10 minutes



Malware

- A problem growing beyond control…



Source: www.av-test.org

Malware

- **Infection methods:**
  - Executables
  - Interpreted files (including built-in scripting languages in applications such as Office, Acrobat, etc.)
  - Kernel & services
  - MBR
  - Hypervisor
  - …
- **Propagation methods:**
  - Exploitation of software vulnerabilities
  - Shared folders
  - Email
  - Faked software (audio/video codecs, antivirus, p2p files, games, …)
  - Bluetooth
  - USB devices
  - Social networks
  - …

Malware

- **Detection**
  - *Signatures*
    - Find a string that identifies the malware
    - Scan files, memory, etc. Detection if match occurs
    - Huge problem with poly/meta-morphism
    - Doesn't scale well
  - *Heuristics*
    - Analyze program behaviour: files opened, network access, attempts to delete files or modify the boot sector, etc.
  - Checksums
  - Sandbox analysis
    - Run executable in a VM
    - Observe behaviour and extract file activity, network accesses, memory usage, etc.

- **See also:**
  - http://cme.mitre.org
  - http://maec.mitre.org

Malware

- **Example of costs due to malware**
  - *Morris worm (1988)*
    - $10 million in downtime and cleanup
    - Internet down
  - *Slammer (2003)*
    - ATMs unavailable, phone network overloaded (no 911!), planes delayed, …
  - Cryptovirus
  - Real costs of most malware remain unknown to the general public
- **Some current trends**
  - Annual growing rate: 175%
  - Smartphones are one the hottest targets
  - Most current malware have characteristics of worms (autonomy, etc.)
  - Advanced features: AV deactivation, jumping out of the sandbox, multiple infection vectors, …
  - **Cyberwarfare:** Stuxnet

Intrusion Detection Systems

- **Where to look for signs of ongoing attacks?**
  - Host-based
  - Network-based
  - Application-based
- **Detection techniques:**
  - Signatures
  - Anomaly detection
- **Network-wide (distributed) detection:**
  - Event correlation techniques
  - Coordination and cooperation among different domains
- **20+ years of research, many experimental and commercial systems, lots of experience gained and…**
  - Still many open questions
  - Pressure towards autonomic response systems
  - Sophisticated evasion techniques increasingly worrying