System Security

Module-VI

Contents

Intrusion Detection System

Firewalls

Malicious software

Wireless Security, Blockchain Cryptocurrencies and the Dark Web

Intrusion Detection

Intrusion and Intrusion Detection

- Intrusion : Attempting to break into or misuse your system.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

Intrusion Detection Systems (IDS)

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

Intrusion Detection Systems (IDS)

- Different ways of classifying an IDS

  IDS based on

  - anomaly detection
  - signature based misuse
  - host based
  - network based

Anomaly based IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
  - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

Signature based IDS

- This IDS possess an attacked description that can be matched to sensed attack manifestations.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
  - E.g DNS, FTP etc.

Signature based IDS (contd.)

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets,as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the ``phf" in ``GET /cgi-bin/phf?"), it identifies those network packets as vehicles of an attack.

Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms
- Have to programmed again for every new pattern to be detected.

Host/Applications based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

Drawbacks of the host based IDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

Stack based IDS

- They are integrated closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.
- This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

Commercial ID Systems

- ISS – Real Secure from Internet Security Systems:
  - – Real time IDS.
  - – Contains both host and network based IDS.
- Tripwire – File integrity assessment tool.
- Bro and Snort – open source public-domain system.

Future of IDS

- To integrate the network and host based IDS for better detection.
- Developing IDS schemes for detecting novel attacks rather than individual instantiations.

Firewalls

Outline

- Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls
  - Firewall Configurations

Firewalls

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet

Firewall Design Principles

- The firewall is inserted between the premises network and the Internet
- Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point

Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security police) will be allowed to pass

Firewall Characteristics

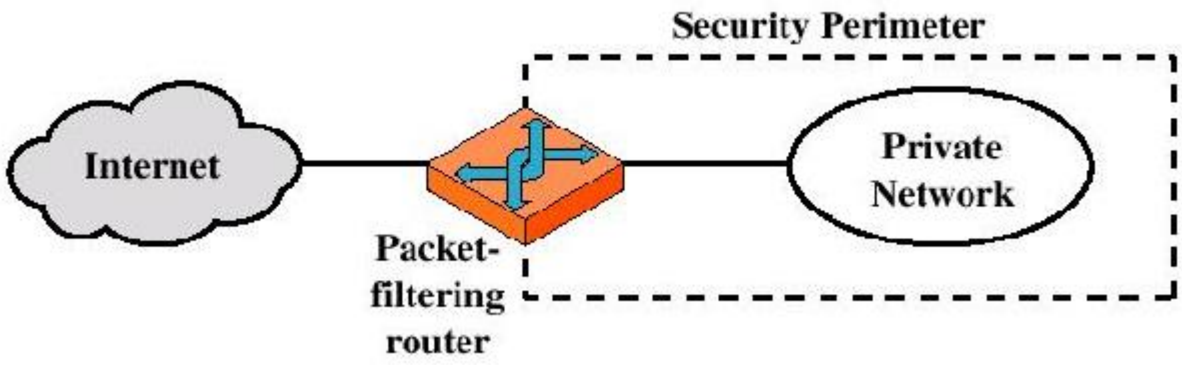
- Design goals:
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways

Types of Firewalls

- Packet-filtering Router

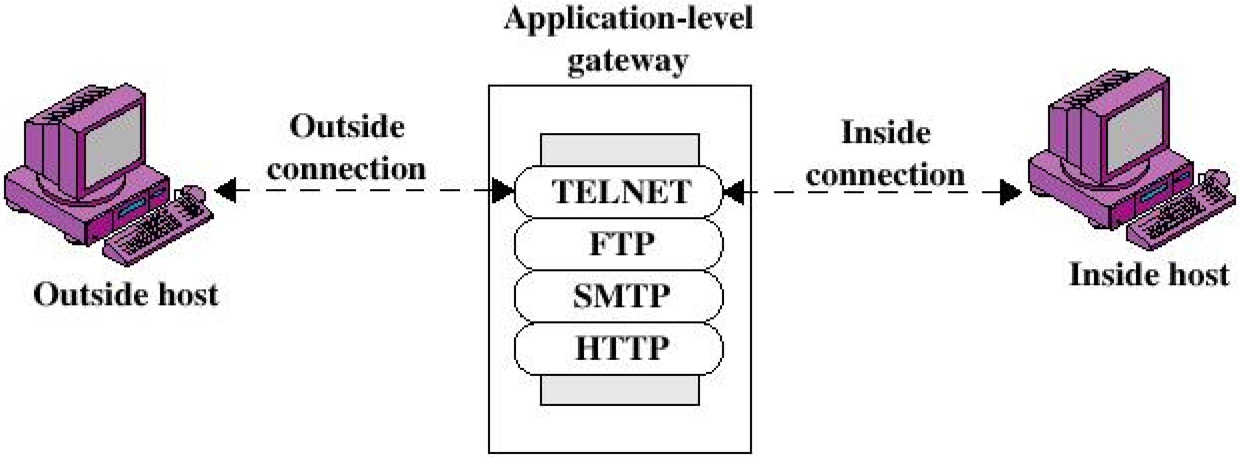


Types of Firewalls

- Packet-filtering Router
  - Applies a set of rules to each incoming IP packet and then forwards or discards the packet
  - Filter packets going in both directions
  - The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
  - Two default policies (discard or forward)

Types of Firewalls

- Application-level Gateway



Types of Firewalls

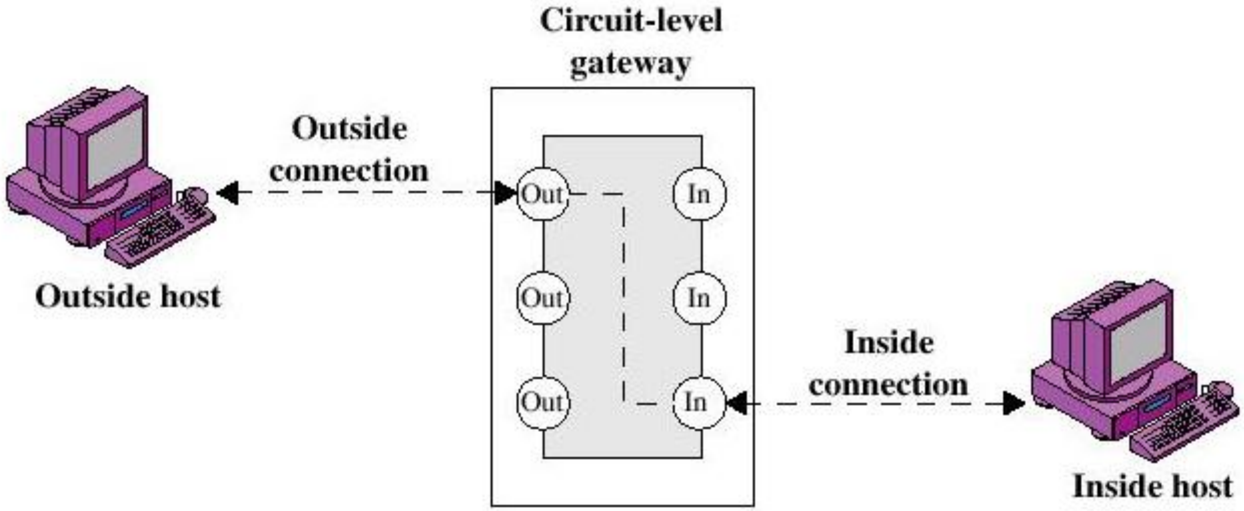
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

Types of Firewalls

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Types of Firewalls

- Circuit-level Gateway



Types of Firewalls

- Circuit-level Gateway
  - Stand-alone system or
  - Specialized function performed by an Application-level Gateway
  - Sets up two TCP connections
  - The gateway typically relays TCP segments from one connection to the other without examining the contents

Malicious Software

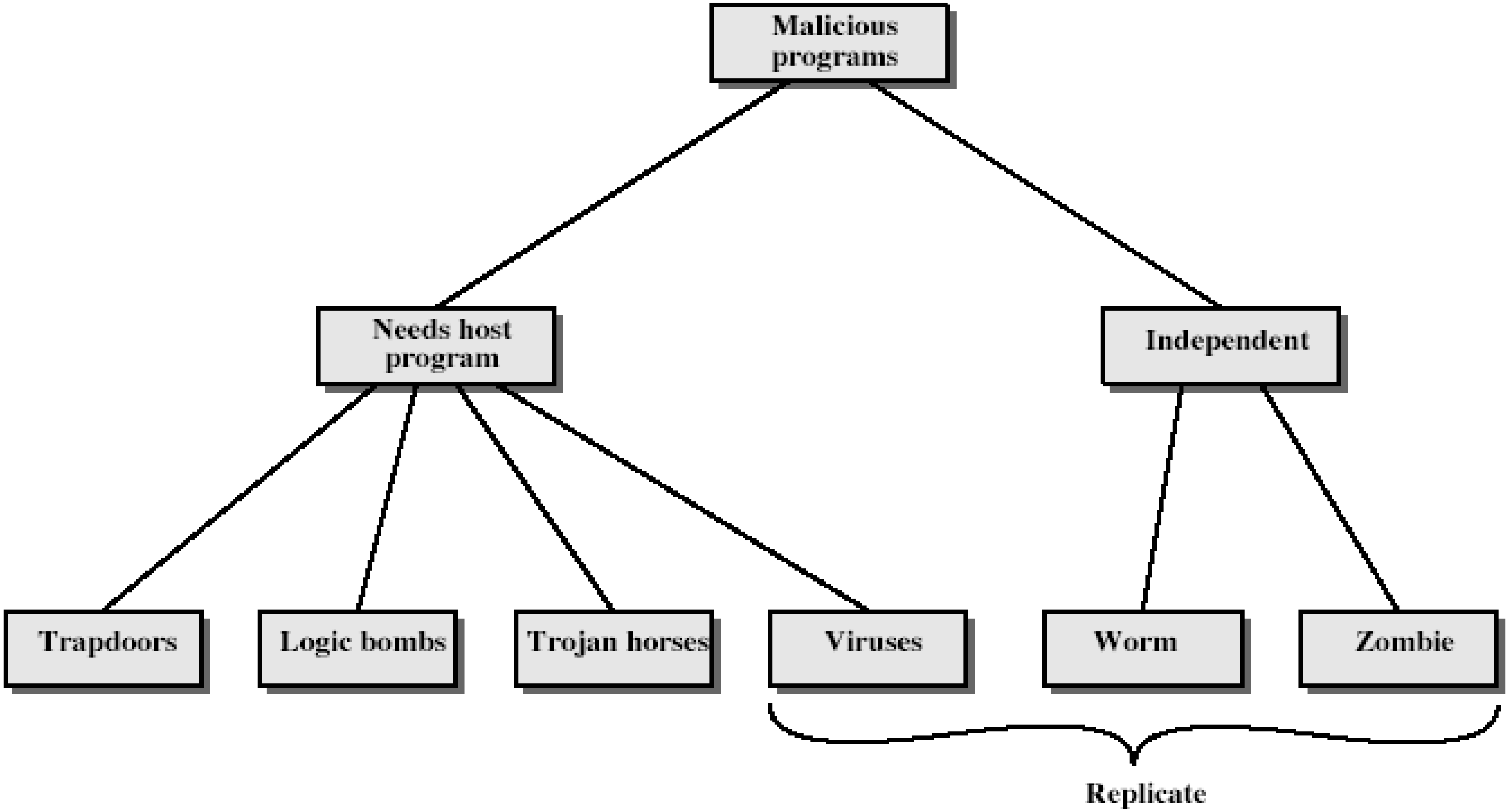
What is the concept of defense: The parrying of a blow. What is its characteristic feature: Awaiting the blow.

—*On War,* Carl Von Clausewitz

Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

Malicious Software



Trapdoors

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks

Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data

Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

Viruses

- a piece of self-replicating code attached to some other code
  - cf biological virus
- both propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

Virus Operation

- virus phases:
  - dormant – waiting on trigger event
  - propagation – replicating to programs/disks
  - triggering – by event to execute payload
  - execution – of payload
- details usually machine/OS specific
  - exploiting features/weaknesses

Types of Viruses

- can classify on basis of how they attack
- parasitic virus
- memory-resident virus
- boot sector virus
- stealth
- polymorphic virus
- macro virus

Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder
- classic trade-off: "ease of use" vs "security"

Email Virus

- spread using email with attachment containing a macro virus
  - cf Melissa
- triggered when user opens attachment
- or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Worms

- replicating but not infecting program
- typically spreads over a network
  - cf Morris Internet Worm in 1988
  - led to creation of CERTs
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create **zombie PC's**, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

Worm Operation

- worm phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

Morris Worm

- best known classic worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pw file
  - exploit bug in finger daemon
  - exploit debug trapdoor in sendmail daemon
- if any attack succeeds then replicated self

Recent Worm Attacks

- new spate of attacks from mid-2001
- **Code Red**
  - exploited bug in MS IIS to penetrate & spread
  - probes random IPs for systems running IIS
  - had trigger time for denial-of-service attack
  - 2nd wave infected 360000 servers in 14 hours
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor

Virus Countermeasures

- viral attacks exploit lack of integrity control on systems
- to defend need to add such controls
- typically by one or more of:
  - **prevention** - block virus infection mechanism
  - **detection** - of viruses in infected system
  - **reaction** - restoring system to clean state

Thank you