Network Security

Hijacking, flooding, spoofing and some honey

Overview of Today's Lecture:

- Threat Models
- Communication Models
- Protocol Design Principles
- IPSec
- SSL/TLS
- DNS
- Firewalls
- IDS
- Honeypots

Introduction:

- Networks
- Data sent from one node to another
- Network protocols - transmission and its problems
- OSI security architecture
- Access Control – Firewalls
- Intrusion Detection Systems

Threat Models:

- Passive attackers
  - eavesdropping / wiretapping / sniffing
  - Traffic Analysis
- Active attackers
  - Spoofing attacks (Phishing, e-mail)
    e.g. messages come from false sender
  - Squatting attacks (Phishing)
    e.g. attacker claims to be at victim's location

Communication Models:

- In formal protocol analysis (Traditional perspective)
  - *internet – cloud*
  - *messages can be seen/modified by anyone*
- Not best model for all security issues
- In security analysis
  - Adversary can only read messages directly addressed to him/her
  - can spoof addresses

Examples of Security Analysis:

- TCP SYN flooding
  - attacker initiates genuine connection but immediately breaks it
  - attacker never finishes 3 way handshake
  - victim is busy with the timeout
  - attacker initiates large number of SYN requests
  - victim reaches its half-open connection limit
  - Denial of service

Protocol Design Principles:

- Open Systems Interconnection model
- Framework for layering network protocols
- 7 layers

OSI model
Application
Presentation
Session
Transport
Network
Link
Physical

Background on IP Security:

- IP connectionless and stateless
- provides a best-effort service
- no guaranteed delivery of packets
- no mechanism for maintaining order
- NO security protection (IPv4)
- In IPv6 – security architecture - IPsec

IP Security:

- Optional in IPv4 and mandatory for IPv6
- 2 major security mechanisms
  - IP Authentication Header
  - IP Encapsulation Security Payload
- Does not contain mechanism to prevent traffic analysis

IP Security – Authentication Header:

- Protects the integrity and authentication of IP packets
- Does not protect confidentiality

IP Security – Authentication Header:

- Protects the integrity and authentication of IP packets
- Does not protect confidentiality

IP Security – Encapsulating Security Payloads:

Provides:

- confidentiality
- data origin authentication
- some replay protection
- limited traffic flow confidentiality
- Achieved by encryption of payload

IP Security – Encapsulating Security Payloads:

- transport mode
  - a protocol frame is encapsulated
  - and encrypted
  - provides end-to-end protection of packets
  - end hosts need to be IPsec aware

IP Security – Encapsulating Security Payloads:

- tunnel mode
  - entire datagram treated as new payload
  - can be thought of as IP within IP
  - can be performed at security gateways
  - host need not be IPsec aware
  - provides traffic flow confidentiality

IP Security:

- IPsec services use encryption
- But are not tied to one particular key management protocol
- Considers possibility of future flaws

Summary

- IPsec provides transparent security for everyone using IP, without changing interface of IP
- Provides host-to-host security but with an overhead

Secure Socket Layer/ Transport Layer Security:

- TCP – a stateful connection oriented protocol
- Performs address based entity authentication
- Vulnerable to attacks – hijacking (OLD), flooding
- Lacks strong cryptographic mechanisms
- These were introduced in SSL by Netscape
- TLS identical to SSL v.3

Secure Socket Layer/ Transport Layer Security:

SSL

- Sits between application layer and TCP
- Relies on properties guaranteed by TCP
- Stateful and connection oriented
- Contains handshake protocol where client and server agree on cipher suite
- This is then used for secure transmisison
- Most widely used Internet security protocol

Domain Name System (Background):

- www.nottingham.ac.uk – Domain name
- 128.243.40.30 – IP address
- Translation of domain name to IP address – DNS
- Information maintained by DNS servers
- DNS lookup – name -> IP address
- DNS reverse lookup – IP address -> name

Domain Name System – Security Issues:

- Attacker can corrupt DNS information
- thus can redirect users to fake sites
- or make sites seem unavailable – DoS attack
- This gets even worse when corruption is propagated between DNS servers

- Work on secure DNS service (DNSEC) underway

Introduction to Firewalls:

- *Cryptographic mechanisms* – confidentiality and integrity
- *Authentication protocols* – verify sources of data
- Access control at network level – *firewalls*

Firewall

"A network device controlling traffic between two parts of a network"

Firewalls:

- Generally installed between LAN and Internet
- or between different LANs
- or on individual hosts
- Should control traffic to and from a protected network
- But ALL traffic has to go through it in order for it to be effective
- e.g. issues with Wifi LANs and Mobile Ad Hoc Networks

Firewalls:

- Defend a protected network against parties accessing services that should only be available internally
- Can also restrict access from inside to outside services (e.g. IRC, P2P)

- Virtual Private Network
  - A secure connection between two gateways
- Network Address Translation
  - hides internal machines with private addresses

Firewalls:

Packet filters:

- Specify which packets are allowed or dropped
- Rules based on source and destination IP address
- and TCP and UDP port numbers
- possible for both inbound and outbound
- Can be implemented in a router examining packet headers

Firewalls:

-*Packet filters - Issues:*

- Only crude rules enforced
- Certain common protocols are difficult to handle
- We can have blanket rules (e.g. block all port 21 traffic)
- We cannot have dynamically defined rules

-*Stateful Packet filters:*

- Consider FTP example
- Understand requests and replies
- e.g. FTP client (connect to 21, receive from 20)
- Can support policies for a wider range of protocols than simple packet filters

iptables – a Linux implementation

Firewalls:

Application-Level Proxies:

- Client - > Server
- Client -> Proxy -> Server-> Proxy -> Client
- Another instance of controlled invocation

e.g. Mail proxy – filters emails for spam, viruses, etc…

- Proxy server – only entity seen by the outside world
- Transparent to users

Firewalls:

Application-Level Proxies:

- Typically run on a hardened PC
- Provide close control over content
- Offer high level of security

Issues

- Large overhead per connection
- More expensive than packet filters
- Configuration complex
- A separate proxy server required for each service to be protected

Firewalls:

Policies:

Permissive – allow everything except dangerous services

- easy to make a mistake or forget something

Restrictive – block everything except designated useful services

- More secure but if blocked something that is needed – DoS

Firewalls:

- Location of firewall important

But there are inherent firewall issues

- No protection against insider threats
- Encrypted traffic cannot be examined

Intrusion Detection Systems -- Background:

- Cryptographic mechanisms help, but…
- Impossible to prevent all attacks
- DoS attacks
- Insider Attacks
- Badly configured firewalls
- Already happening attacks not detectable

-> Intrusion Detection Systems

Intrusion Detection Systems:

- Consists of a number of sensors (network or host)
- Sensors collect various data
- Data is analysed
- Intrusion reported
- and possibly reactions triggered

Intrusion Detection Systems:

- Misuse Detection
  - looks for attack signatures
  - signatures – patterns of network traffic
  - e.g. no. of failed login attempts
  - only as good as its database of attack signatures
  - new attacks -> signature needs to be created
  - IDS needs to update its database

Intrusion Detection Systems:

- Anomaly Detection
  - Statistical / Behaviour-based detection
  - uses statistical techniques
  - first 'normal' behaviour is established as baseline
  - during operation if behaviour of monitored system deviates from baseline and exceeds a threshold ->
  -> alarm is issued

Intrusion Detection Systems:

- Anomaly Detection
  - Possibility of detecting novel attacks
  - However only detects anomalies
  - Anomaly is not necessarily an attack
  - Attack is not necessarily anomalous
  - False positives (false alarm)
  - False negatives (attack detected as normal)

Intrusion Detection Systems:

- Network based IDS
  - attack signatures of network traffic
  - e.g. SNORT, Firestorm
- Host Based IDS
  - attack signatures from system activity

Most effective IDS systems to date combine the two.

Vulnerability Assessment and Honeypots:

- Vulnerability Assessment
  - examines the security state of a network or a host
  - info on open ports, package version, etc..
- Honeypots
  - a resource to track attackers and to learn and gather evidence about their activities
  - designed to mimic real systems
  - low and high interaction honeypots

Summary:

- Networking Protocols
- Firewalls
- Intrusion Detection