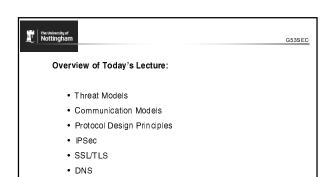


Network Security

Hijacking, flooding, spoofing and some honey



| The Universality of Nottingham

Introduction:

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

The University of Nottingham

G53SEC

Threat Models:

FirewallsIDSHoneypots

- 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

The University of Nottingham

G53SEC

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

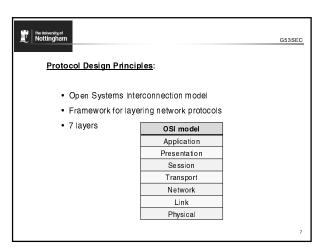
The University of Nottingham

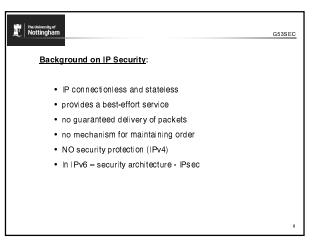
G53S F

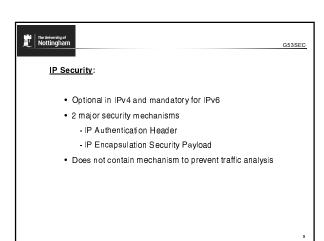
Examples of Security Analysis:

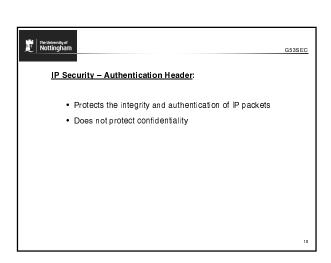
- TCP SYN flooding
- attacker initiates genuine connection but immediately breaks it
 - attacker never finishes 3 way handshake
 - $\ensuremath{\text{victim}}$ is busy with the timeout
 - attacker initiates large number of SYN requests
 - victim reaches its half-open connection limit
 - Denial of service

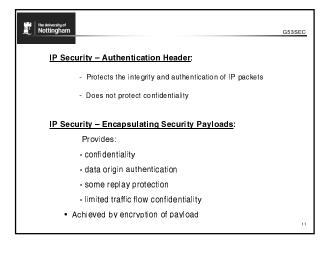
6

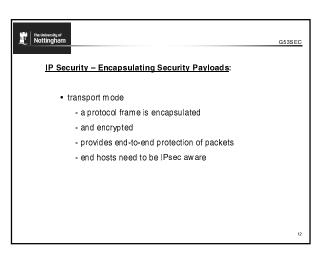














G53SEC

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

13



G53SEC

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

14



G53SEC

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



G53SEC

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

.



G53SEC

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

The University of Nottingham

G53SEC

<u>Domain Name System - Security Issues:</u>

- 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

18



G53SEC

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



G53SEC

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
- · e.g. issues with Wifi LANs and Mobile Ad Hoc Networks



G53SEC

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



G53SEC

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



G53SEC

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

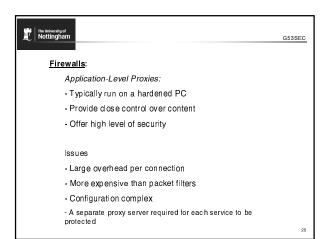
The University of Nottinghan

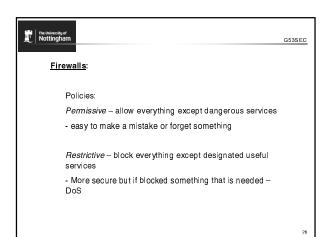
G53SEC

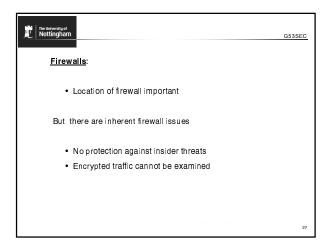
Firewalls:

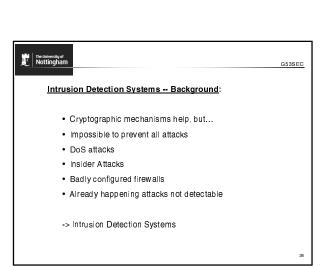
Application-Level Proxies:

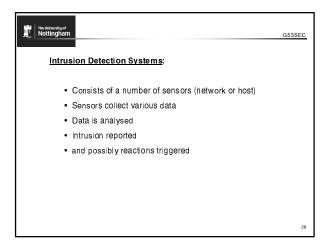
- Client > Server
- Client -> Proxy -> Server-> Proxy -> Client
- Another instance of controlled invocation
- e.g. Mail proxy filters emails for spam, viruses, etc...
- Proxy server only entity seen by the outside world
- Transparent to users

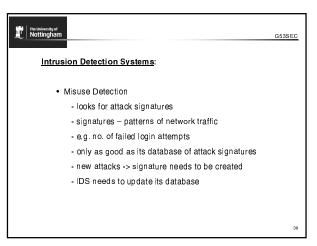














G53SE

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

31



G53SEC

Intrusion Detection Systems:

- An omaly 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)

32



GESSEC

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.

33



G53SEC

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

.



G53SEC

Summary:

- Networking Protocols
- Firewalls
- Intrusion Detection

35