Tutorial 8

Aims

- To understand the major threats and challenges in networks
- To examine the efficacy of major network security equipment

Questions

1. What are the major issues (vulnerabilities) created by connecting to a network?

   Hardware:

   - LAN: Data not confined to the local computer but travel through paths accessible by others

     Wired: vulnerable to tapping, wireless: open access
   - MAN, WAN:
     - Data path may not be known
     - Network perimeter may not be known

   Software:

   - External access to the computer

     People or software
   - Many possible origins (source nodes) of attack

2. How are the basic Internet protocols addressing the security requirements of LANs and of the Internet?

   Protocol: Message formats and exchange rules for interoperability

   They are optimised for

   Efficiency/speed: minimum overhead

   Reliable delivery: Protection against transmission errors

   Security is addressed by different protocols (TLS/SSL/https, IPsec, DNSsec etc)

3. What types of attacks can be repelled by a

   (a) packet filter

   (b) proxy server?

   Compare the performance and detection abilities of the two types of firewall and those of intrusion detection systems.

   Packet filter

   - Examines packets, and passes or blocks them.
   - Fast
   - Can detect and block malicious content and attacks directed against specific IP addresses, e.g. denial-of-service attacks.
   - Stateful filters can also pair up requests with replies, and can repel injected packets, intrusion probes (e.g. port scanning)

   Drawbacks

   - Can be difficult to configure
   - Can default to pass when faulty
   - Decision made on limited information

Proxy

- Intercepts traffic for certain applications
- Analyses content, generates a new message with the same content

Drawbacks

- Slow
- A proxy is needed for each application

Firewall: preventive device (first line of defence)
Intrusion detection system: reactive device (second line of defence)

4. Discuss the following attacks targeting a network connection.
   (a) Host compromise (e.g. spyware, web page defacing)
   (b) Person in the middle, session hijacking
   (c) Denial of service

(a) Host compromise
Attacks the operation locally
May affect individual users, user groups, individual systems in different ways (e.g. tampering with data or with access rights)
May affect external systems (use the host for attacking other systems)

(b) Person in the middle, session hijacking
Attacks the communication
Interferes with the information communicated

(c) Denial of service
Attacks a single target
Affects availability