Security in Computing & Information Technology

Lecture 8

Network Security

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

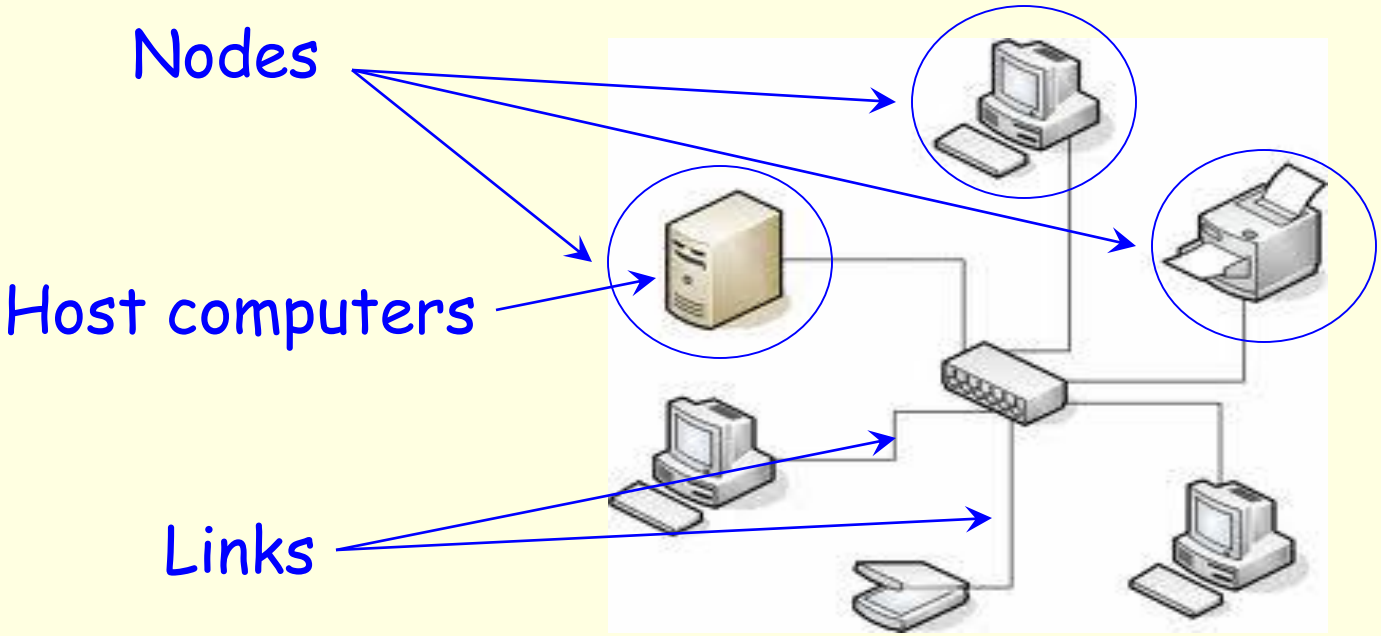
11. Privacy
12. Internet banking

Lecture Topics

- Security of the communication medium
- Traffic security
- Intrusions and their detection

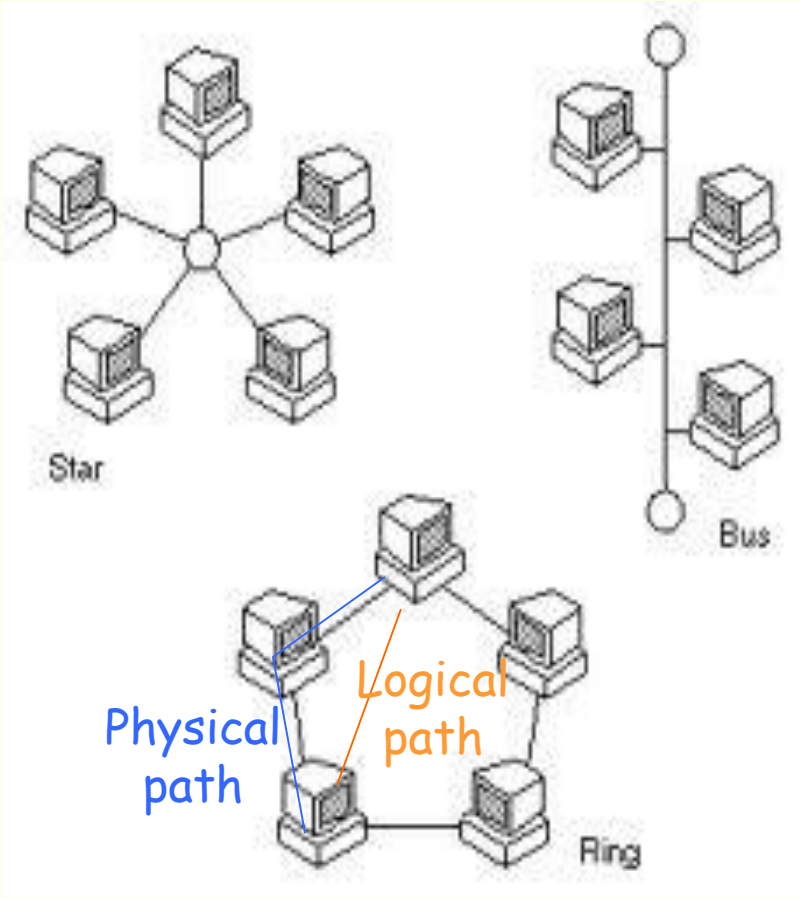
Computer Networks

- Interconnected computers
- Provide communication between nodes
- Components



Network Configurations

- Topology
  - Layout of the network
    - Physical topology
      - Interconnection of cables (e.g. bus, ring)
    - Logical topology
      - Data transfer paths
      - May or may not be the same as physical topology



Wired Networks

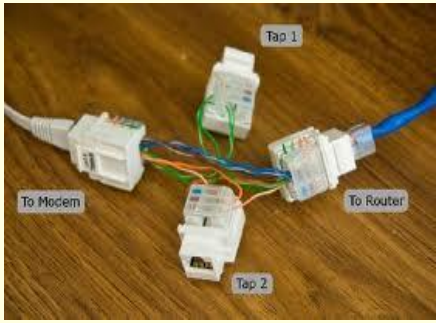
- Communication medium is cable
  - Advantage
    - Signal confined to the cable

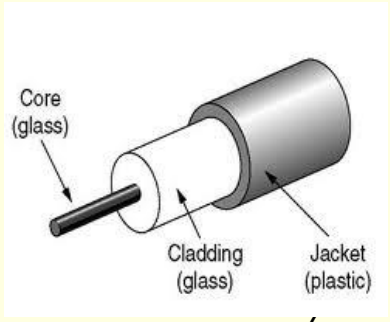
  - Disadvantage
    - Cabling costs

Wired Media Security

Cable paths may be publicly accessible

- Cable
  - Coaxial cable: very easy to tap unnoticed
    - Detect the electromagnetic field radiated around the cable
  - Twisted pair: fairly easy to tap, hard to notice
    - Low radiation: Connection may need to be interrupted
- Optical fibre
  - Can be tapped unnoticed after removing outer protection (cladding & jacket)

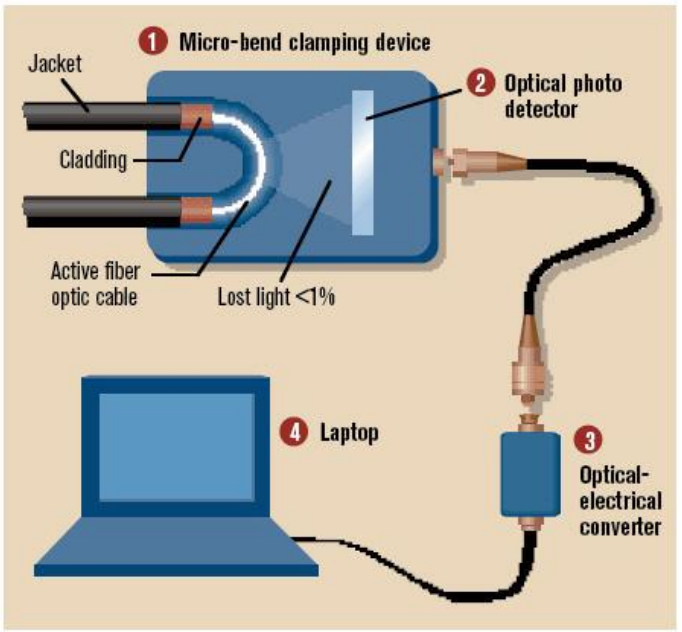




Cable Security – Wiretapping Tools

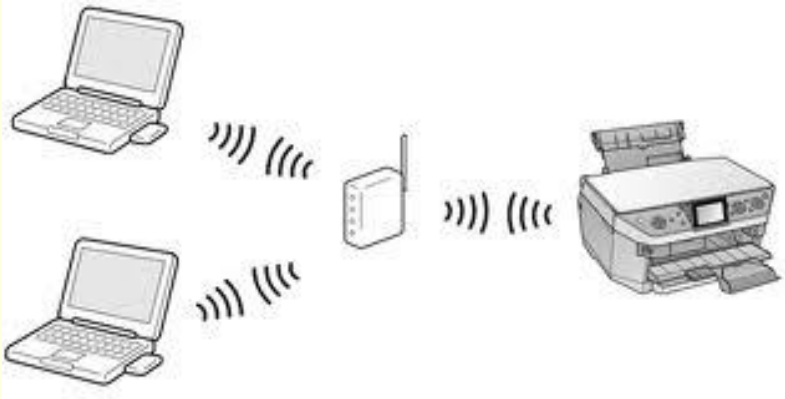
- Copper cable

- Optical cable



Wireless Networks

- Communication medium is air
  - Advantage
    - No Cabling cost



  - Disadvantage
    - Reduced range (fast signal attenuation)
    - Lack of security

Wireless Media Security

Transmission medium is openly accessible

- Eavesdropping

  Confidentiality (secrecy) problem

  - Anyone in the vicinity can receive the signal
  - Intrusion cannot be detected
  - War driving: searching for wireless networks by driving around in a car

- Easy to interfere with

  Data integrity problem

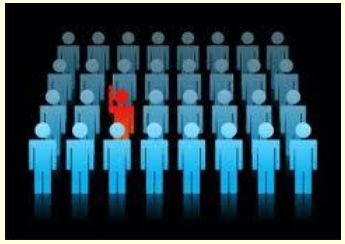
  - Anyone in the vicinity can transmit
  - Signal interference may corrupt the signal (jamming)

Network Vulnerabilities

- Anonymity

  On the Internet no-one knows you are a dog

- Many points of attack
  - Source can be anywhere
  - Huge range of targets



- Unknown perimeter
  - The Internet spans the whole world
- Unknown communication path
  - Message routes optimised for fast delivery

Node Addressing

- MAC address
  - "Physical" address of a node
  - Assigned by equipment manufacturer
  - Cannot be changed
- IP address
  - Address assigned by the network
  - Can change/be reassigned as network conditions require
- Human-understandable names
  - Domain name system (DNS)
- Mapping between
  - IP addresses and MAC addresses: Address Resolution Protocol (ARP)
  - names and IP addresses: DNS name resolution

Seven-Layer OSI Model

Layer	*Function*	*Security support*
Application	User process	Yes
Presentation	Data formats, encryption	Yes
Session	Connection management	
Transport	End-to-end data transfer	
Network	Logical addressing, determining paths	Yes
Data link	Physical addressing, sending packets	Yes (can be messy)
Physical	Medium interface, transmitting bits	Yes

Internet Protocols

- Communication protocol
  - Rules for exchanging messages
  - Description of message formats
- Essential Internet protocols (TCP/IP)
  - Use basic information
    - Source address
    - Destination address
  - Optimise
    - For speed
    - For reliable message delivery
  - Information protection
    - Limited protection against transmission errors
    - No protection against malicious use or interference

Securing the Network

- Physical security
  - Protecting the wires (cables)
    - Telecommunication companies provide basic network protection
- Traffic protection
  - Firewalls
    - Site manager's responsibility
    - The more restrictive, the stronger the protection
- Secure protocols
  - Security-aware protocols
    - Require the installation & support of additional software

Firewalls

- Function: protect computers and networks
  - First line of defence
  - Preventive tool
- Operation
  - Traffic screening
    - Block unwanted communication
    - Repel certain attacks
  - Device protection
    - Single host protection
      - Installed in workstations
    - Network segment or a whole network protection
      - Installed at
        - network entry/exit points
        - computer connections

Firewall Implementation

- Firewall software
  - Uses a rule base to make decisions
  - Purpose-built software
    - Kits are available for different operating systems
- Firewall solutions
  - Dedicated hardware
    - Fast
    - Should not run any other application software
    - Has advanced management features
  - Software running on the protected device
    - Cheaper
    - Less secure
      - Application software can interfere with the operation
      - Vulnerable to insider attacks
    - Implements better-than-nothing (BTN) security

Firewall Types

- Packet filters
  - Look at the message and take action (filter)
  - Filtering
    - can be based on protocol type, source/destination address, content (packet payload), time of day, etc
    - can be performed at one layer or across several layers
    - results in passing or discarding the message
  - Processing is fast
- Proxies
  - Interpret the message
  - Generate a new message with the same content
  - Processing is slower

Secure Protocols

- Additional protocols operating over the existing ones
- Are not part of the standard TCP/IP protocol set
- Are implemented at different layers
- Can provide
  - Authentication
  - Confidentiality/secrecy
- Examples

  IPsec, DNSsec, TLS (SSL)

Attacks

- Targeting a node
  - Host compromise
  - Denial of service
- Targeting a connection
  - Person-in-the-middle
  - Session hijacking
  - Traffic diversion
- Targeting a whole network
  - Interfering with network administration

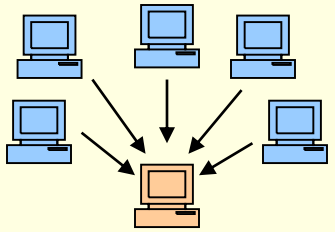
Host Compromise

- Aims
  - Collect sensitive data from target
  - Use compromised computer to launch further attacks
- Methods
  - Using automated tools

    E.g. Viruses, worms, etc
    - Used for mass infection/intrusion
  - Manually

    Hackers bypassing access control
    - Used for accessing large systems (e.g. databases)

Denial of Service (DoS)

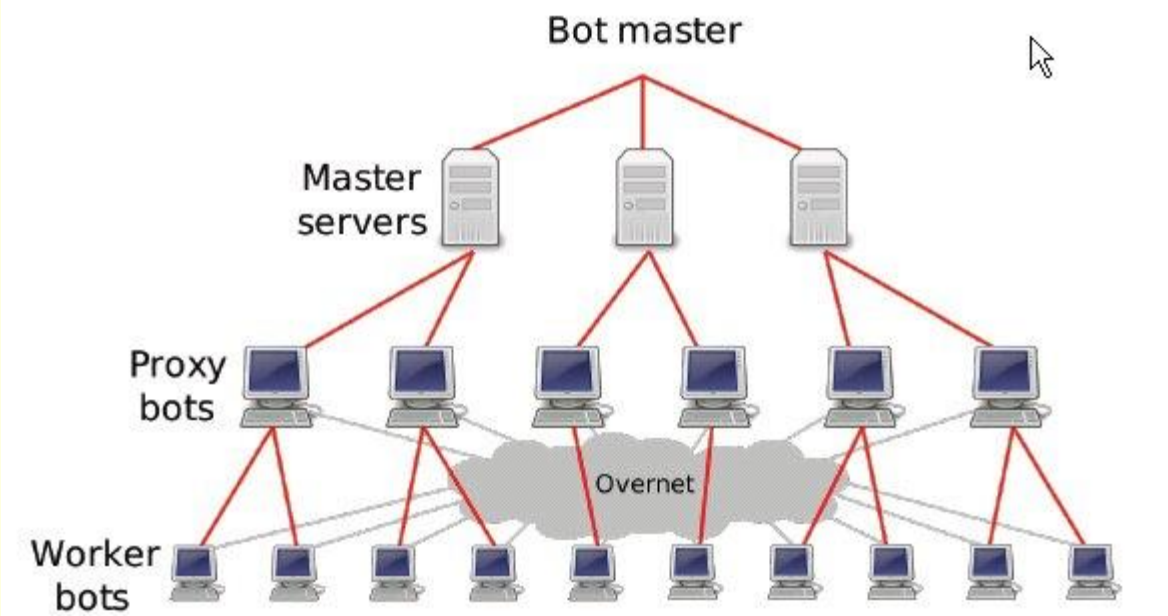


- Aims
  - Block external access to the site
  - Bring the site down (crash it)
- Methods
  - Direct flooding
    - Traffic via established connections
    - Legitimate connection requests
    - Malformed/unfinished connection requests
  - Indirect flooding
    - Directing responses to maliciously formed queries to the victim (e.g. DNS amplification attack)

Distributed DoS

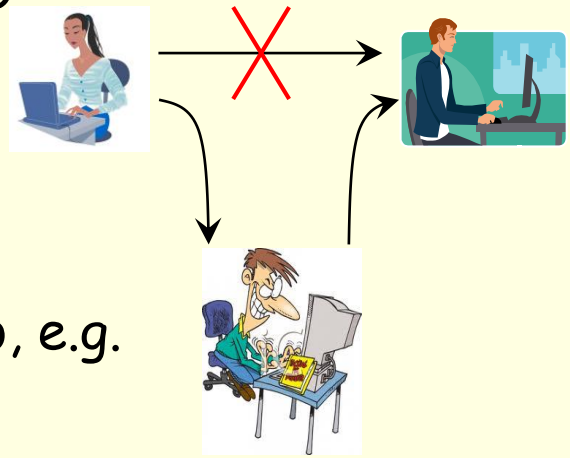
- Using a large number of compromised computers for the attack
- The Storm botnet

Image source: Kanich et al, Spamalytics: An Empirical Analysis of Spam Marketing Conversion



Person-in-the-Middle

Active eavesdropping ("unauthorised proxy")



- Aim
  - To intercept messages
  - To modify/inject messages
- Method
  - Splits the original connection into two, e.g.
    - One between client and attacker
    - One between attacker and server
  - Attacker can read and modify all messages
  - Can be done over an https connection as well
    - Tools can
      - Intercept browser messages
      - Allow the operator to modify those messages (e.g. HTML)
- Traffic diversion
  - Redirecting messages to the attacker so that the intended recipient may not even receive it

Session Hijacking

An unauthorised entity takes over a valid, legitimate connection

- Session fixation
  - Attacker tricks the victim into connecting to a server with a session ID set by the attacker

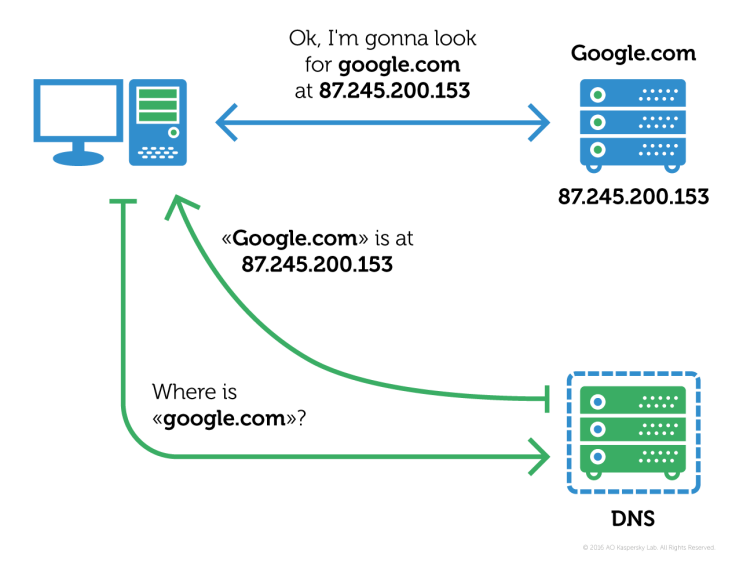
    or
  - Communication uses a predictable session token
- Session sidejacking (sniffing)
  - Attacker acquires an existing, valid session ID, and takes over the connection
- Cross-site scripting (XSS)
  - Attacker tricks the user's computer to run malicious code (and e.g. steal a session token)
  - Details will be discussed in next week's lecture

Attacks on Network Administration

- Attack on the authentication database
  E.g. password file attack
- Attack on network security devices
  E.g. firewall attack
- Attack on web servers
  E.g. defacing
- Rogue secondary certificate authorities (CA)
  E.g. secondary CA
  - has a certificate from a trustworthy CA
  - issues certificates to less reliable subjects

Attack Example: DNS Switching

Normal operation



Hijacked DNS server

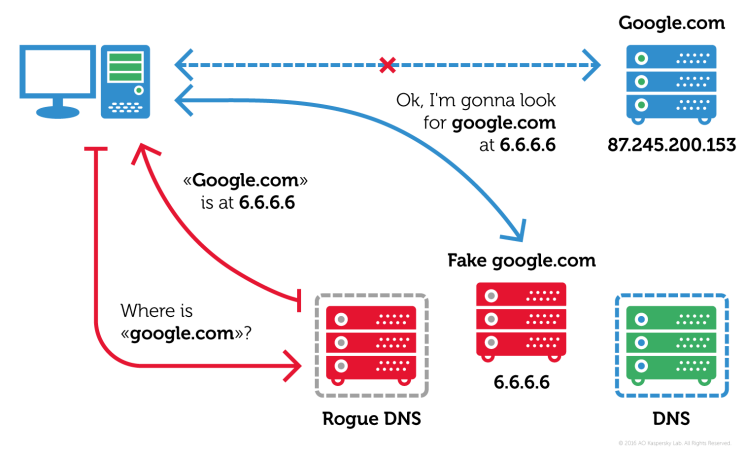


Image source: https://blog.kaspersky.com/switcher-trojan-attacks-routers/13771/

Intrusion Detection Systems

- IDS Function: protect computers and networks
  - Second line of defence
  - Reactive tool
- Operation
  - Monitors the operation
    - Stealth mode: not visible to other hosts
  - Looks for evidence of unauthorised activity
  - Raises alarm
    - False positive: alarm generated by legitimate operation
    - False negative: genuine attack missed

Logs and Audit Trails

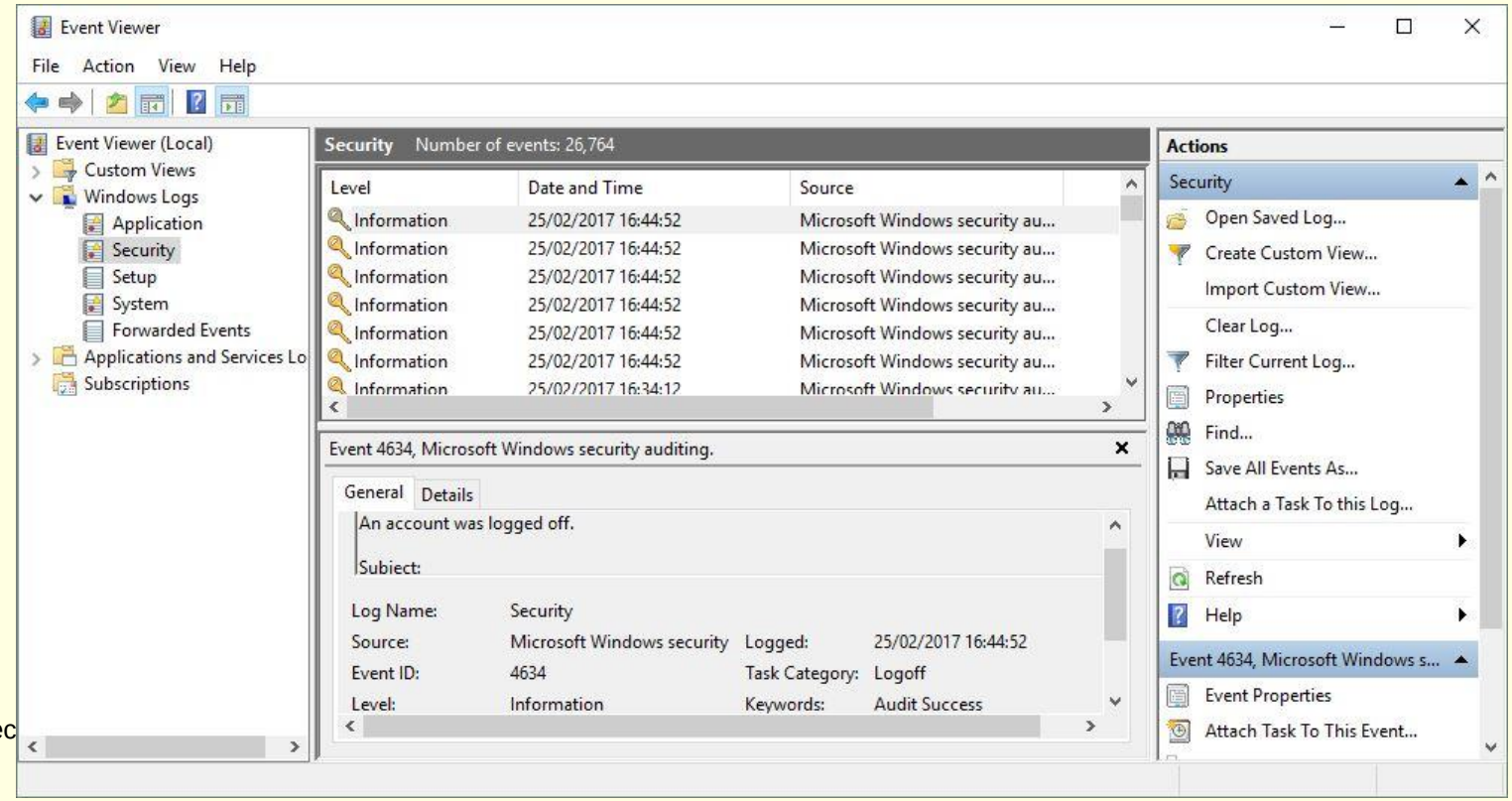
- Logs
  - Traces of operation
  - Generated by system and application programs
  - Kept in a file

    Easy to access, easy to review
- Audit trails
  - A protected collection of information about system activities
  - Contains detailed information
    - Better chances to detect anomalies
    - More data to store & analyse

Audit Trail Example

Event list (MS Windows)

- Generated by
  - Applications
  - System programs



IDS Types

- Network based
  Network devices (e.g. routers) checking all traffic
  - Advantage: few devices can protect a large network
  - Disadvantages
    - Cannot cope with current, high network speeds
    - Cannot analyse encrypted packets
- Host based
  Dominant approach: system integrity verification
  - Advantage: Can analyse encrypted traffic
  - Disadvantage: performance penalty borne by the host
- Application based
  Monitors data used by running applications (event logs etc.)
  - Advantage: can observe user interaction
  - Disadvantage: tied to a particular application
- Target based
  Targets monitor their own data (e.g. cryptographic hash)

Detection Approaches

- Misuse detection
  - Looking for known attack patterns ("misuse signature")
  - Based on pattern matching
    - E.g. code pattern in memory
- Anomaly detection
  - Looking for deviation from normal (expected) system behaviour ("strange event")
  - Based on behaviour analysis
    - E.g. number/frequency of resource access

Misuse Detection

- Detects known events only
  - Database has to be updated periodically
  - Protection becomes available only after the threat's appearance
- Race between hackers & security people

  E.g. a virus encrypts itself when propagating and uses unpredictable encryption keys (virus signature varies) $\Rightarrow$ new detection methods emerge
- Typical example: Antivirus software

Anomaly Detection

- Can detect new, unknown events
- Protection is available potentially when the threat appears
- Description of normal behaviour
  - Statistics based

    E.g. system calls, network traffic
    - System has to be trained what constitutes normal behaviour
  - Specification based

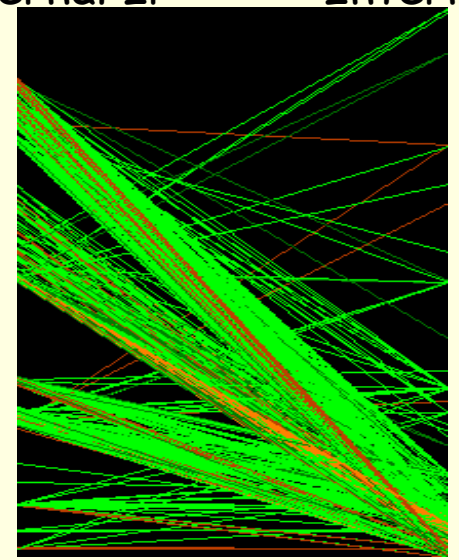
    E.g. logic-based rules
    - Similar to misuse detection, but evaluates data rather than matching against known patterns

Visual Intrusion Detection

- Attack visualisation
  - Showing traffic (e.g. packet traces)
  - Relies on human processing
    - More capable
    - Prone to human errors (tiredness)

Occlusion

External IP Internal port



Jamming

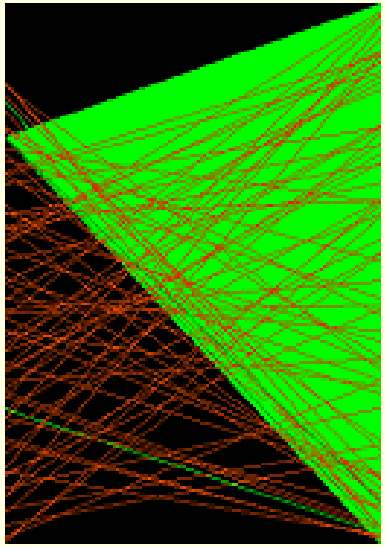


Image source: http://www.rumint.org/gregconti/publications/20060303_BH_Europe.ppt

Incident Handling

- Detection
  - Investigate incident candidates
  - Identify attack
- Containment
  - Stop the spread of malware
  - Prevent further damage
- Eradication
  - Removal of malware
- Recovery
  - Restore damaged items
  - Restart the operation

Summary

- Networks have many points of attack
- Traffic security is a major concern
- Protection
  - First line: firewalls
  - Second line: intrusion detection systems