COMPUTER SECURITY

Securing access to resources

Lecture 3

4th stage – (2021-2022)

Dr. Moceheb Lazam Shuwandy

WHAT IS COMPUTER SECURITY?

- **Securing Access to resources**
  - **Two steps:**
    - **Authenticate = establish identity of the requestor**
    - **Authorize = grant or deny access**

SECURING ACCESS

- TO:
  - Something you have
  - Something you know
  - Something you are

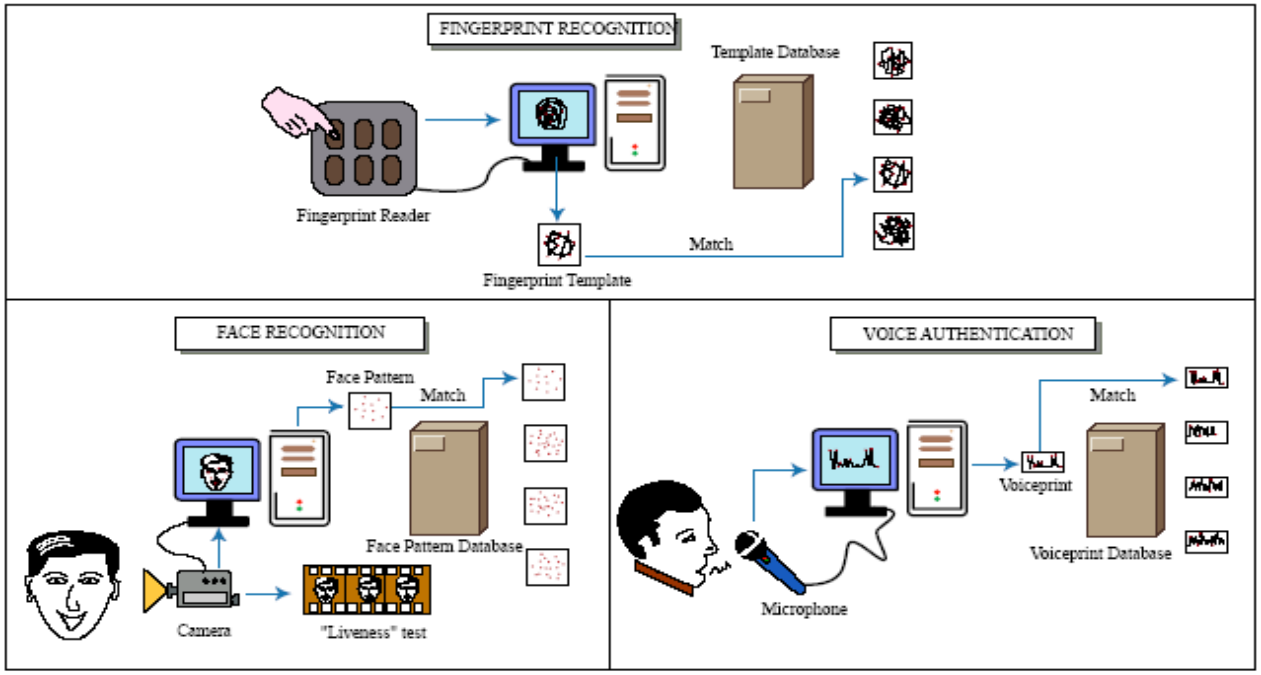
SMART CARDS "SOMETHING YOU HAVE"

- Several subcategories
- One of interest here is cryptographic smart cards:
  - Store user's digital certificate and/or private key
  - Used to prevent private keys from being "hacked" from user's computer
  - What happens if a smart card is stolen?

SYSTEM ACCESS CONTROLS "SOMETHING YOU KNOW…"

- Login procedures
  - Usually something you know
- Password leaks
  - Commonly used password
  - Explicitly told
    - Voluntarily
    - Trojan horse
  - Trial and error
  - Intercepted communication
    - paper, camera, wiretap, file on disk, emanations, password sniffing on networks
- Passwords are inconvenient
  - In client/server environment, user doesn't want to enter password for every service she connects to

ENTER BIOMETRICS…
“SOMETHING YOU ARE…”



SNEAKING THROUGH THE BACKDOOR…

- Strategies whose goal is to gain control by bypassing access control defenses
- Exploit "vulnerability" in applications that connect our machine to the network
  - Viruses
  - Buffer overflow attacks

VIRUSES AND WORMS

- Programs that run on machines where they're not wanted
- Transmitted through I/O channels
- Disguise themselves
  - How?
- Often don't act right away
  - Why not?
- Why hasn't anyone written a definitive virus eliminator?

MALWARE: SPYWARE, ADWARE

- Programs that are (usually) added to your computer without your knowledge and that do things you don't want, such as:
  - Display unwanted ads in pop-up windows
  - Subreptitiously send information about your computer and your actions to someone else
  - Change toolbars, homepages, etc.
- Common sources:
  - "Free" software you download and install
  - Some web pages

DENIAL OF SERVICE ATTACKS

- Flood a server with fake messages (with "spoofed" IP addresses) so that no legitimate messages can get through
  - Flood someone's mailbox
  - Recent attacks on eBay, Yahoo, etc.
- Difficult to trace since fake messages are sent from a variety of "hijacked" machines

DEFENSIVE MEASURES

- Virus scanners and removers
- Malware scanners and removers
- Firewalls
- Intrusion Detection Systems

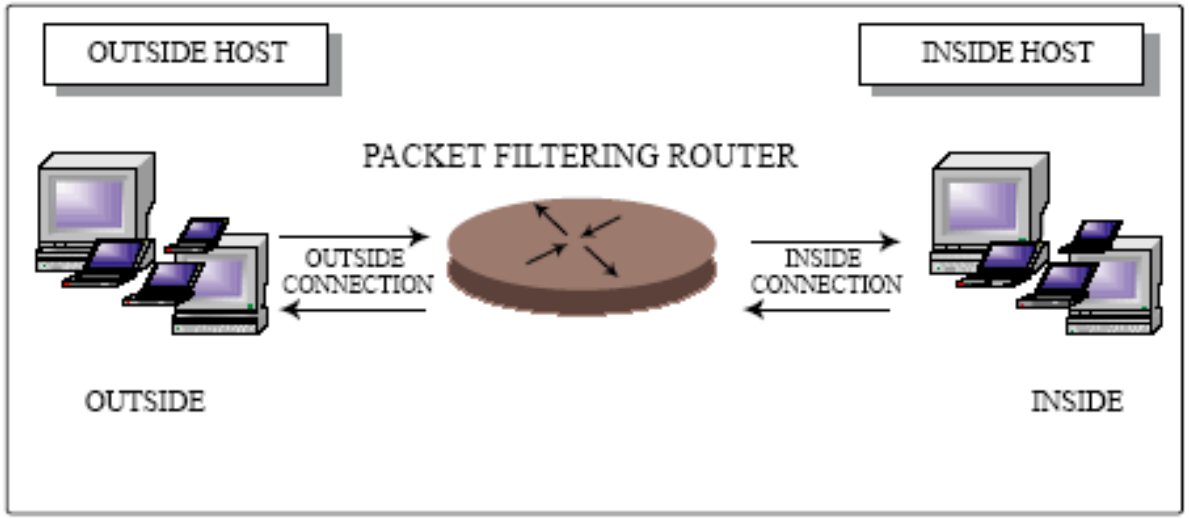
FIREWALLS – WHAT THEY DO

- Hides the structure of the network by making it appear that all transmissions originate from the firewall.
- Blocks all data not specifically requested by a legitimate user of the network.
- Screens data for source and destination address so you receive data from only trusted locations like people on your approved guest list.
- Screens the contents of data packets for known hacker attacks

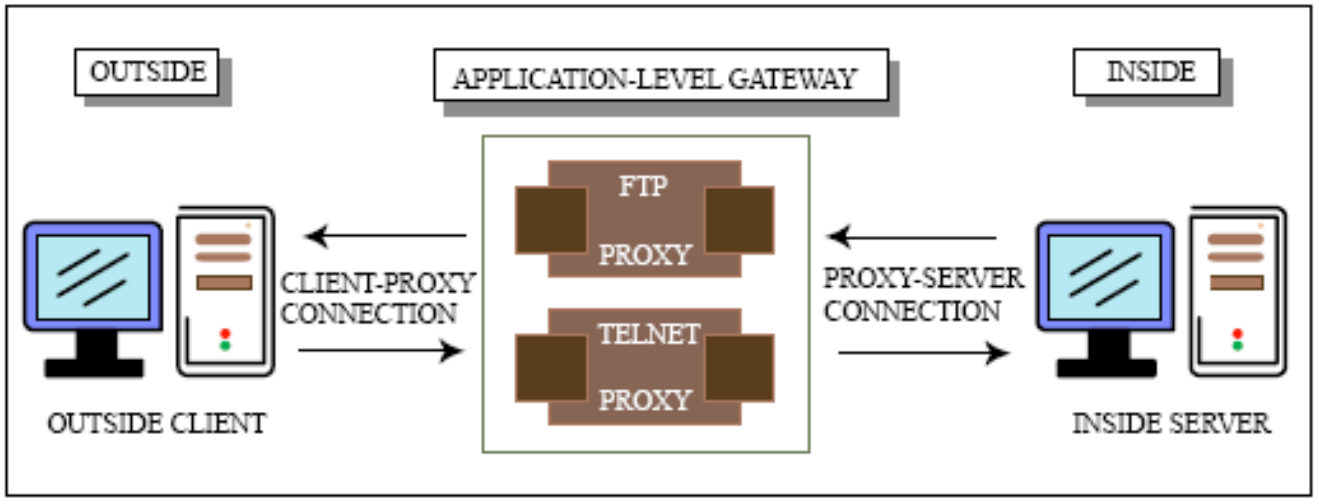
TYPES OF FIREWALLS

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.
  - Stateless
  - Stateful
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses

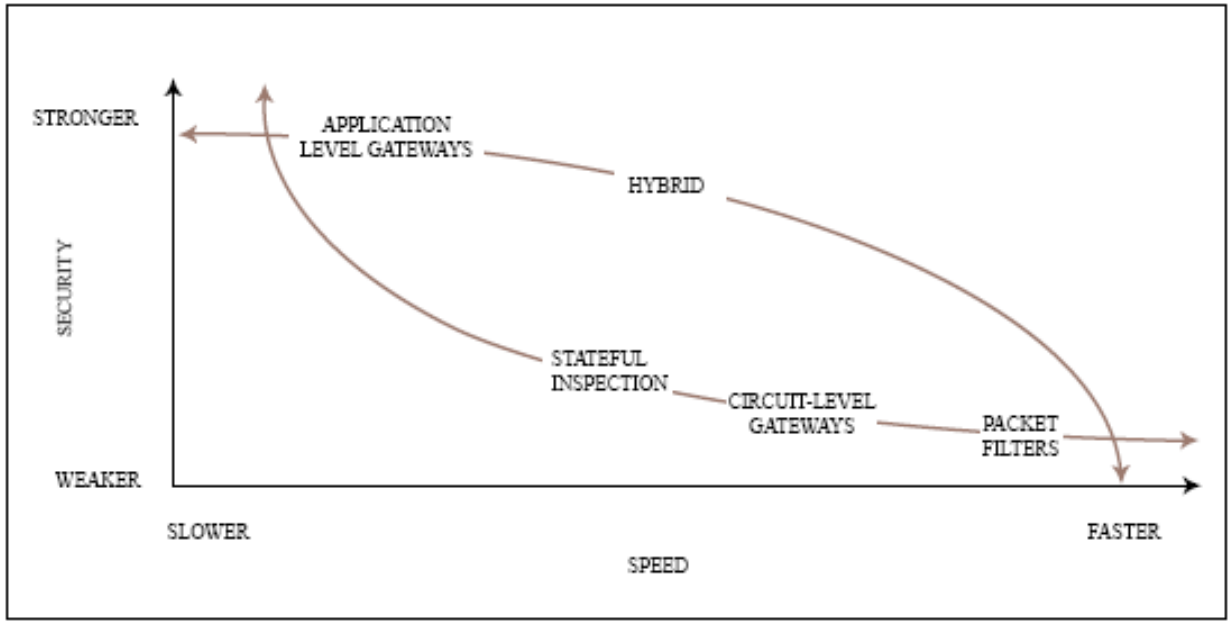
PACKET-LEVEL FIREWALLS



APPLICATION-LEVEL GATEWAYS



FIREWALL PERFORMANCESECURITY TRADEOFFS



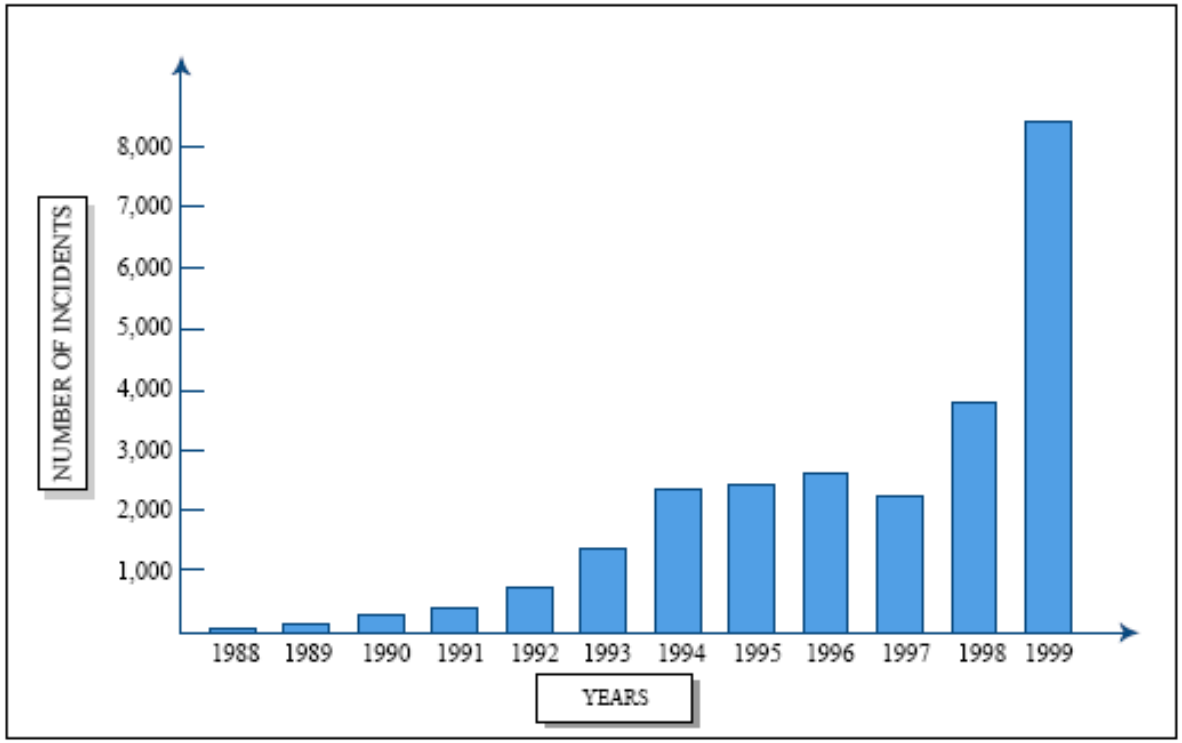
HOW DO INTRUSION DETECTION SYSTEMS WORK?

- IDS uses data mining techniques to uncover and report suspicious activities
- Two main strategies:
  - Pattern recognition
  - Anomaly detection

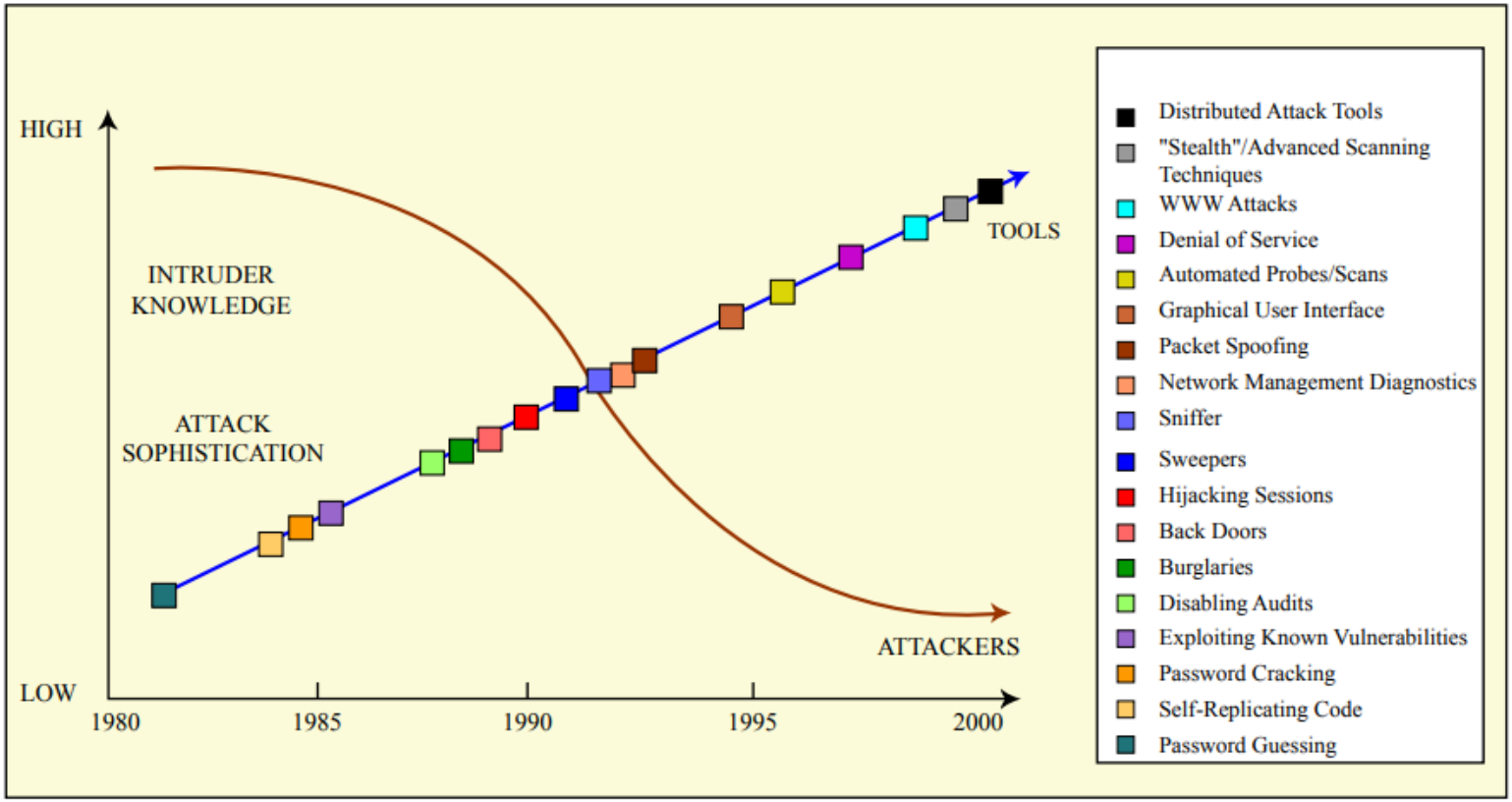
OTHER PREVENTION MEASURES

- Stay current on patch levels for Microsoft's OS and web server.

HOWEVER, ATTACKS ARE ON THE RISE



…AND REQUIRE FAR LESS TECHNICAL EXPERTISE



SECURITY RESOURCES

- www.microsoft.com/security
  - Advisories
  - Patches
  - IIS Security Checklist
- www.securityfocus.com
  - Bugtraq Mailing List
  - Tools, Books, Links
  - Vulnerabilities and Fixes

Q&A