15.561
Information Technology Essentials

# Sessions 9 & 10
# Computer Security

Acknowledgments:
Adapted from Chris Dellarocas, U. Md..

# What is computer security?

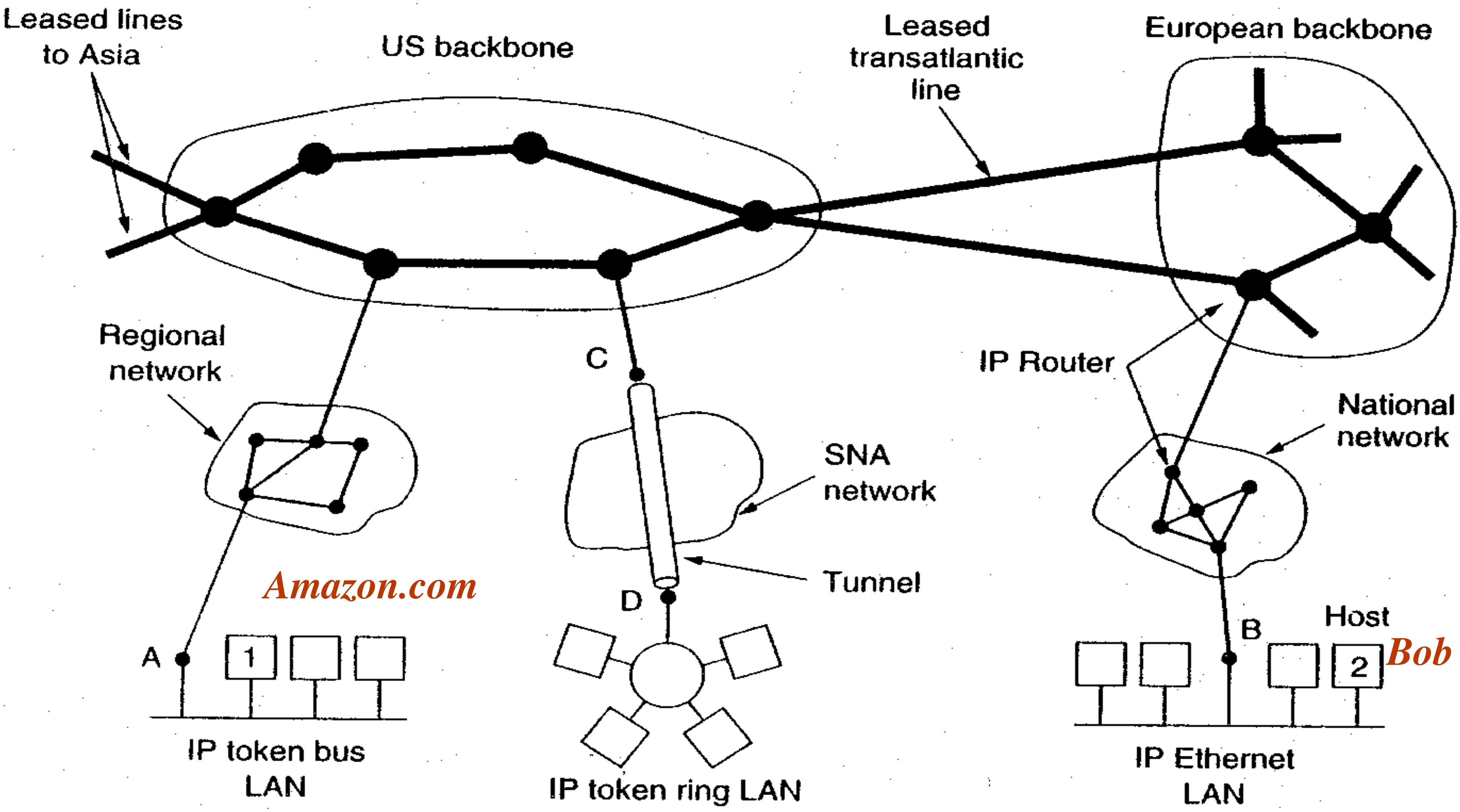
- Securing communications
  - Three steps:
    - Secrecy = prevent understanding of intercepted communication
    - Authentication = establish identity of sender
    - Integrity = establish that communication has not been tampered with

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

# Topic 1: Securing communications

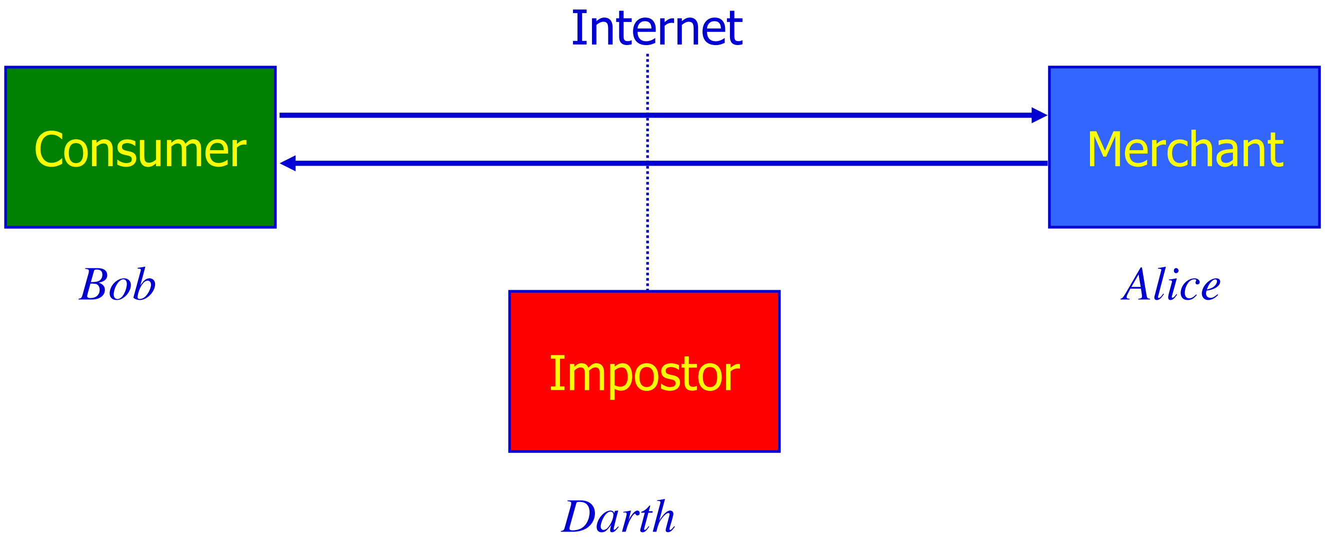
- What can go wrong?

# A bird's eye view of the Internet



# Communication security issues

- **Encryption - How do I ensure the secrecy of my transactions?**
- **Authentication - How do I verify the true identity of my counterparts?**
- **Integrity - How can I be sure the message hasn’t been altered?**



# Traditional cryptography

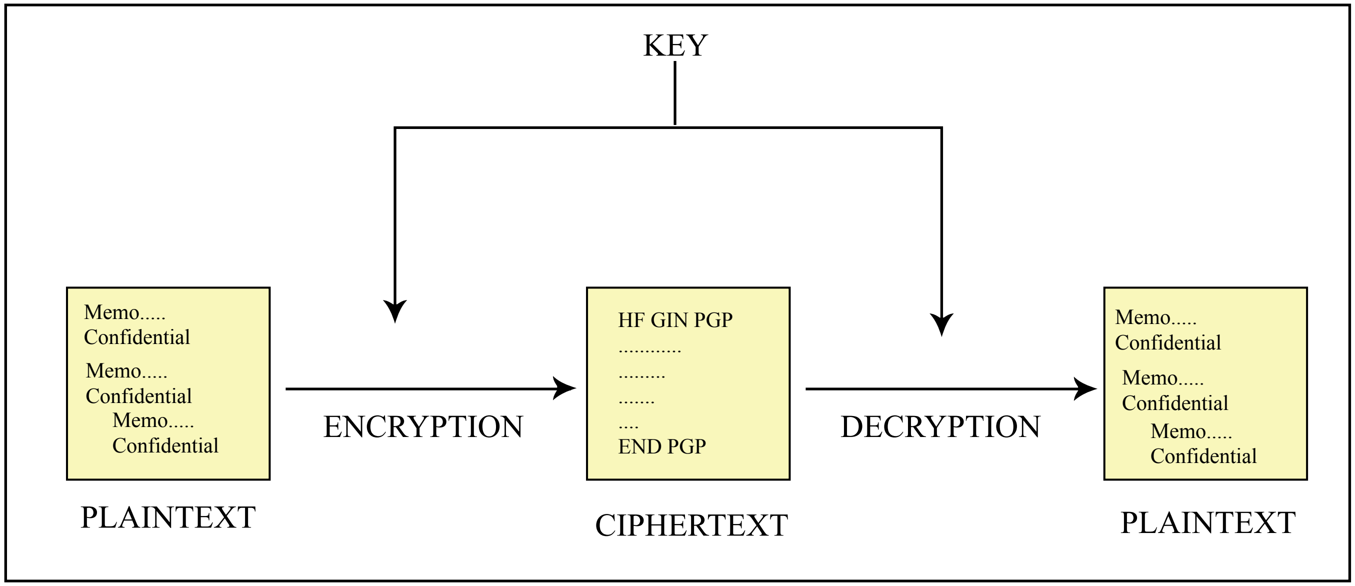
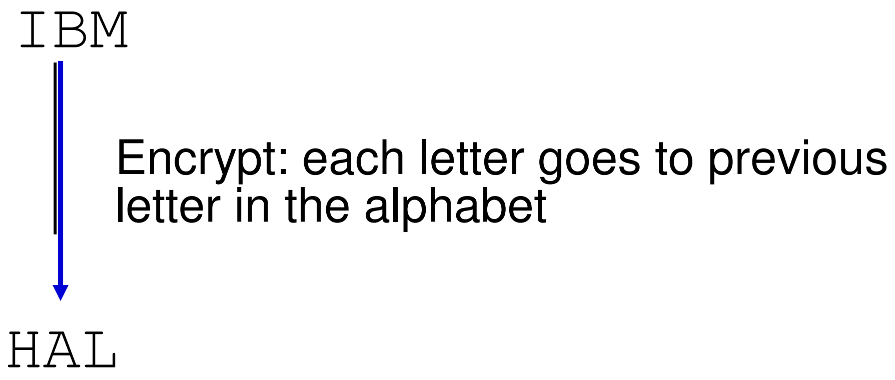


Figure by MIT OCW.

# Ceasar’s Cipher: Encryption by Substitution

- Substitute for each letter (block of bits)



IBM

Encrypt: each letter goes to previous letter in the alphabet

HAL

- How can you crack a substitution cipher?
  - I.e., how can you guess the key?

# Public-key cryptography

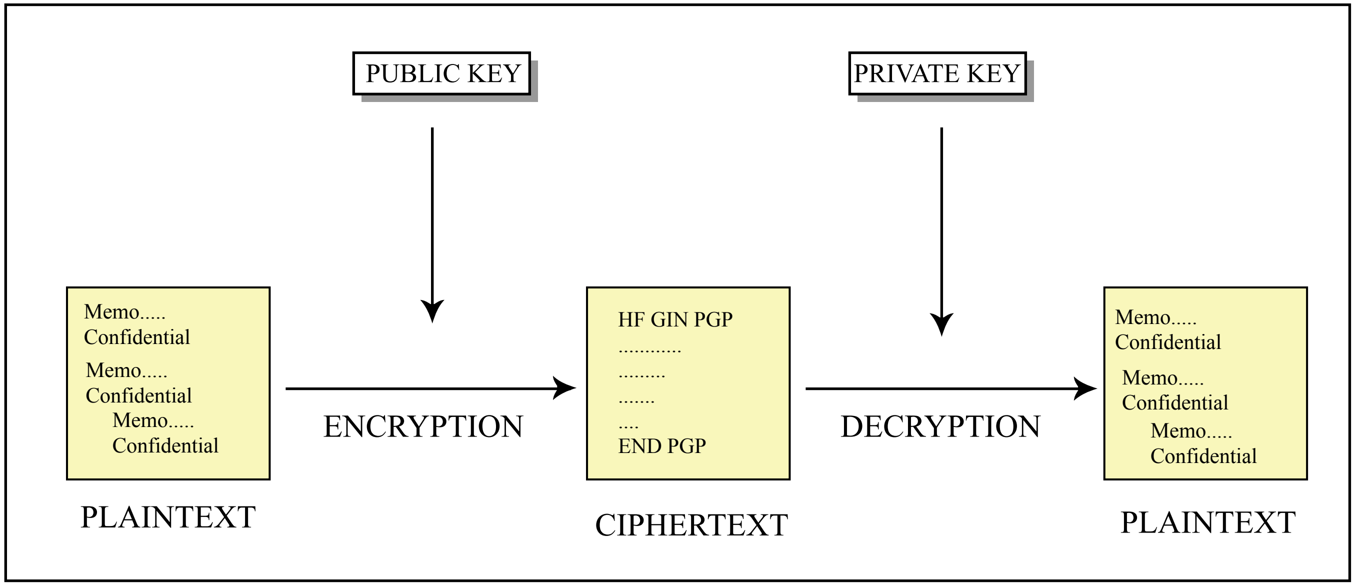
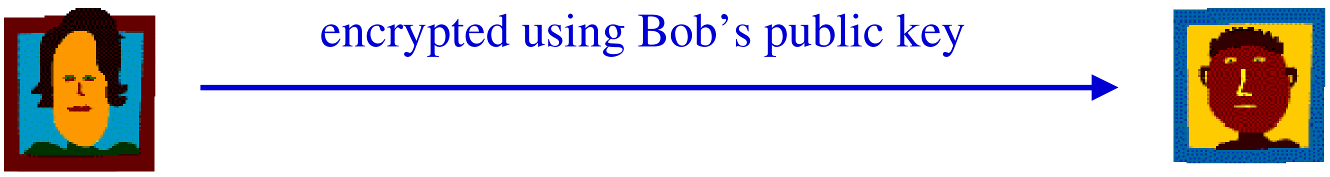


Figure by MIT OCW.

# Public key cryptography

- Secret key cryptography: Based on a secret key
  - Same secret key used for encryption and decryption
  - Problem: How to transmit key securely on the Internet???

- Public key cryptography: Two keys used
  - Public key known to everybody. Used for encryption.
  - Private key known only to owner. Used for decryption.



{Message}
encrypted using Bob's public key

Alice

Bob

Only Bob
who knows the
corresponding
private key
can decrypt

# Public key cryptography works if…

- Private key remains secret
  - Never leaves the owner’s computer
  - Typically encrypted and password-protected
- Difficult to guess private key from knowledge of public key
  - Boils down to trying all different key combinations
  - Difficulty of “breaking” the code rises exponentially with the bit length of the key
  - 1024-bit keys require more time than the life of the universe in order to be “broken”
- Reliable public key distributed
  - This is the most difficult problem!

# Encryption is not enough: Spoofs

- Pretending to be someone else
- Hard to login without someone’s password
- But can send out communications with someone else’s name on it
  - email
    - 1993: Dartmouth sent a message saying midterm exam was cancelled
    - Message appeared to come from the Professor!

# Needed: Message Authentication

- Make sure Bob gets the message unaltered
- Don’t let Alice deny sending the message

~~Plausible Deniability~~

- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

# Digital Signatures

- Key property: Public and private keys can be applied in either order

- Alice has message M
  - She applies her private key to it
  - She sends encrypted message to Bob

- Bob decrypts it with Alice's public key
  - gets back original message
  - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)

- In that way, encrypting a message with one's private key acts as a digital signature!

# Public Key Management

- Public key cryptography works as long as
  - ✓ Private key is really kept secret
  - ✓ Hard to compute private key from public key
  - – Get the correct public key from some trusted source

- Bob can send public key over insecure communication channel

- But how do you know Darth didn't send you his key instead?

# A central key distributor

- Alice asks the distributor for Bob's public key
- The distributor sends it to Alice and "digitally signs" it
- Alice knows the key came from the distributor
  - Now just have to be sure that the distributor is honest and got Bob's key from Bob, not Darth
- Requires one secure communication per user
  - Bob sends public key to distributor when he joins the system
- Secret keys require secure communication between every pair of users

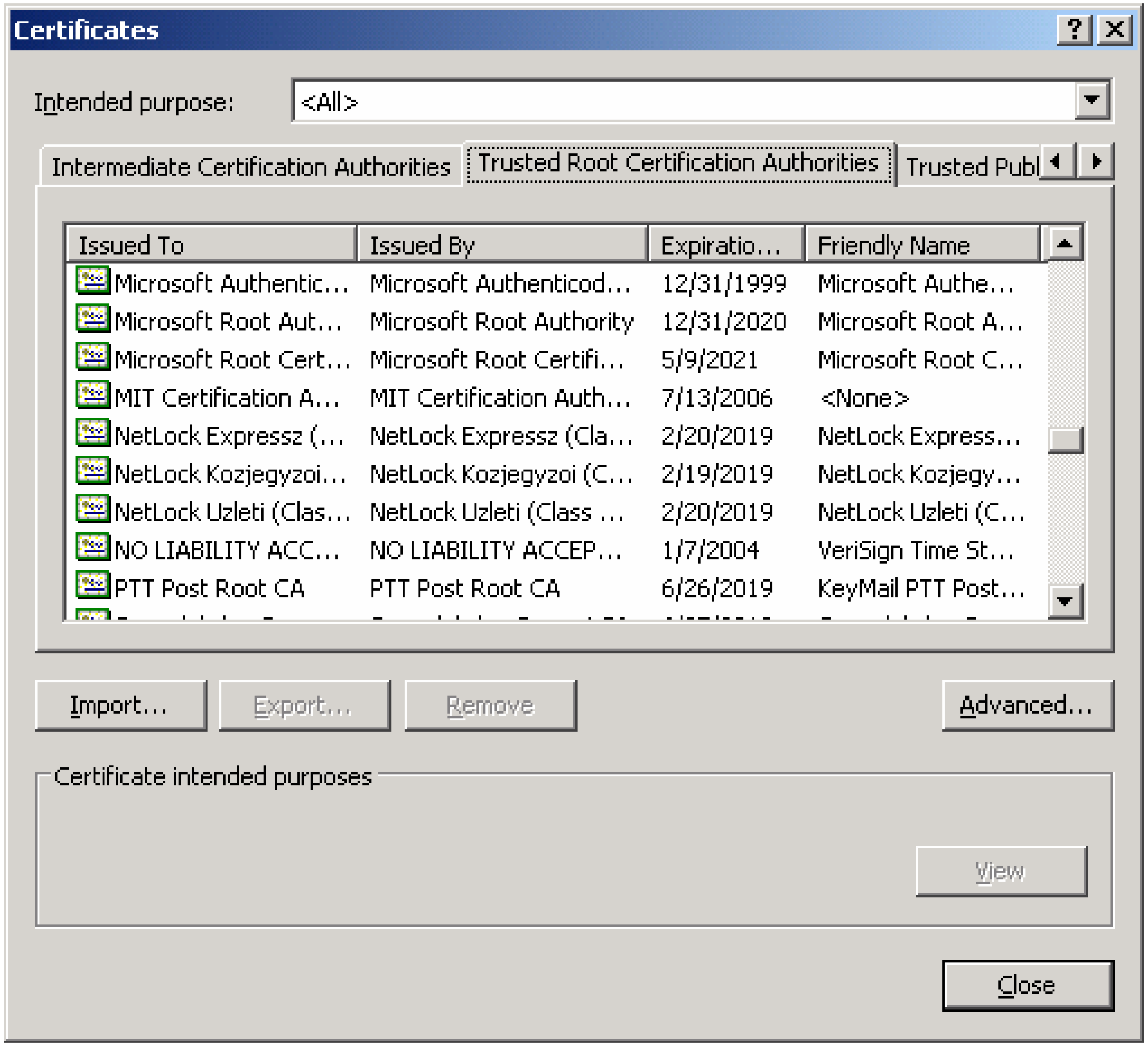
# Public Key Infrastructure (PKI)

- Certificate Authorities are Trusted Third Parties charged with the responsibility to generate trusted certificates for requesting individuals organizations
  - Certificates contain the requestors public key and are digitally signed by the CA
  - Before a certificate is issued, CA must verify the identity of the requestor
- These certificates can then facilitate automatic authentication of two parties without the need for out-of-band communication

# Certificates

- Used to certify a user’s identity to another user
  - The certificate issuer's name
  - Who the certificate is being issued for (a.k.a the subject)
  - The public key of the subject
  - Some time stamps
- Digitally signed by issuer
- Issuer must be a trusted entity
- All users must have a reliable public key of the issuer
  - in order to verify signed certificate

# Web browsers come with a number of certificates already installed



Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| Microsoft Authentic... | Microsoft Authenticod... | 12/31/1999 | Microsoft Authe... |
| Microsoft Root Aut... | Microsoft Root Authority | 12/31/2020 | Microsoft Root A... |
| Microsoft Root Cert... | Microsoft Root Certifi... | 5/9/2021 | Microsoft Root C... |
| MIT Certification A... | MIT Certification Auth... | 7/13/2006 | <None> |
| NetLock Expressz (... | NetLock Expressz (Cla... | 2/20/2019 | NetLock Express... |
| NetLock Kozjegyzoi... | NetLock Kozjegyzoi (C... | 2/19/2019 | NetLock Kozjegy... |
| NetLock Uzleti (Clas... | NetLock Uzleti (Class ... | 2/20/2019 | NetLock Uzleti (C... |
| NO LIABILITY ACC... | NO LIABILITY ACCEP... | 1/7/2004 | VeriSign Time St... |
| PTT Post Root CA | PTT Post Root CA | 6/26/2019 | KeyMail PTT Post... |

# PKI Industry

- Main players: trusted third party CAs
  - Verisign
  - Entrust
  - Cybertrust
  - RSA

- Revenue from
  - products (PKI servers for intranets and extranets)
  - services (certificate services for individuals and organizations)

# Applications: eCommerce Security

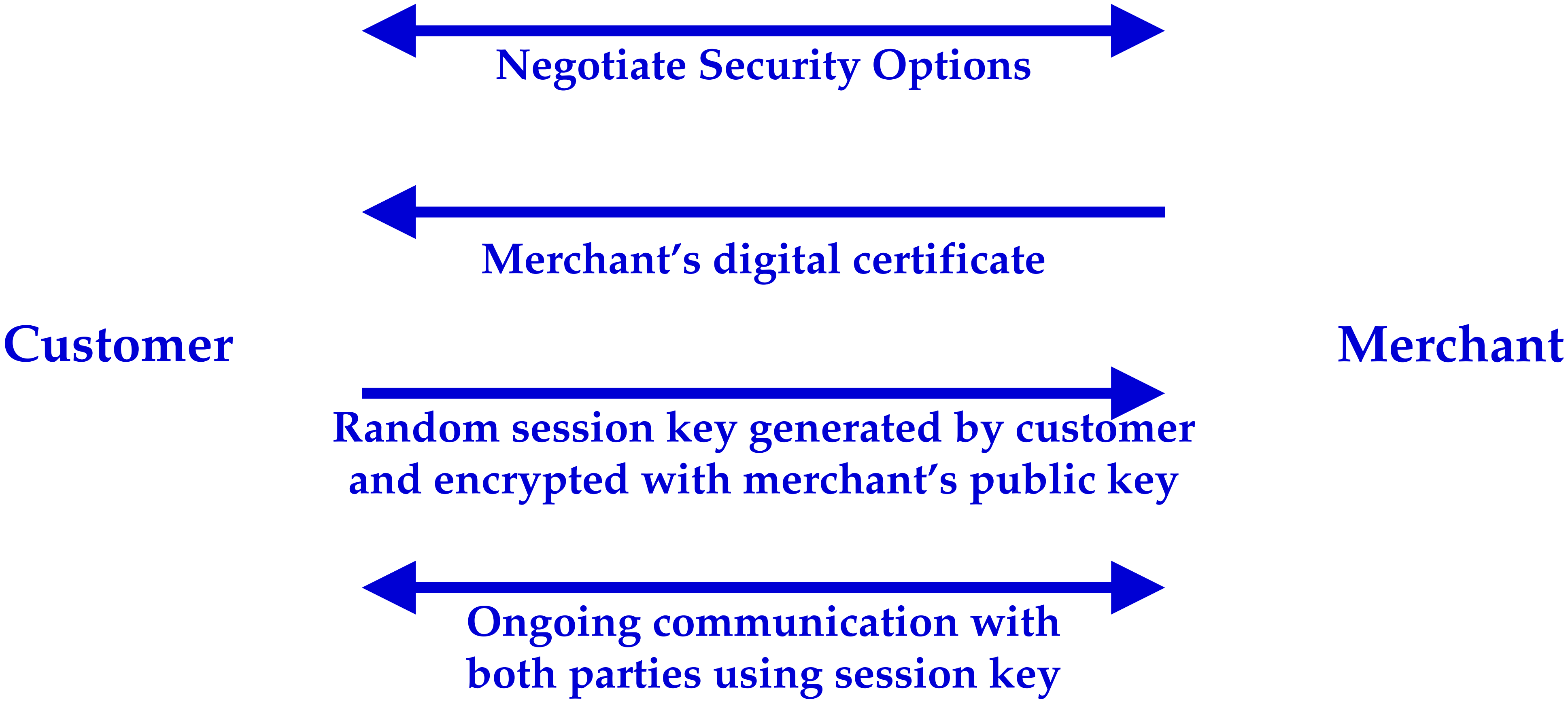
- Needed to transmit sensitive information through the Web
  - credit card numbers
  - merchandise orders

- Requirements
  - sender and receiver must authenticate each other before sending any “real” data
  - all “real” data must flow encrypted through the network
  - no intercepted communication can be used to an intruder’s advantage

# SSL / TLS

- Secure Sockets Layer / Transport Layer Security
- Provides reasonable level of security
- Often used for transactions between consumers and merchants

# SSL / TLS



Negotiate Security Options

Merchant's digital certificate

Customer

Merchant

Random session key generated by customer and encrypted with merchant's public key

Ongoing communication with both parties using session key

# Applications: Virtual Private Networks (VPNs)

- Secure, private networks that operate over a public network (like the Internet).
  - Messages are confidential
  - Only authorized users can access network

- “Tunneling” -- encrypted messages from one protocol are packaged inside another protocol.

# Topic 2: Access Control

- 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…"

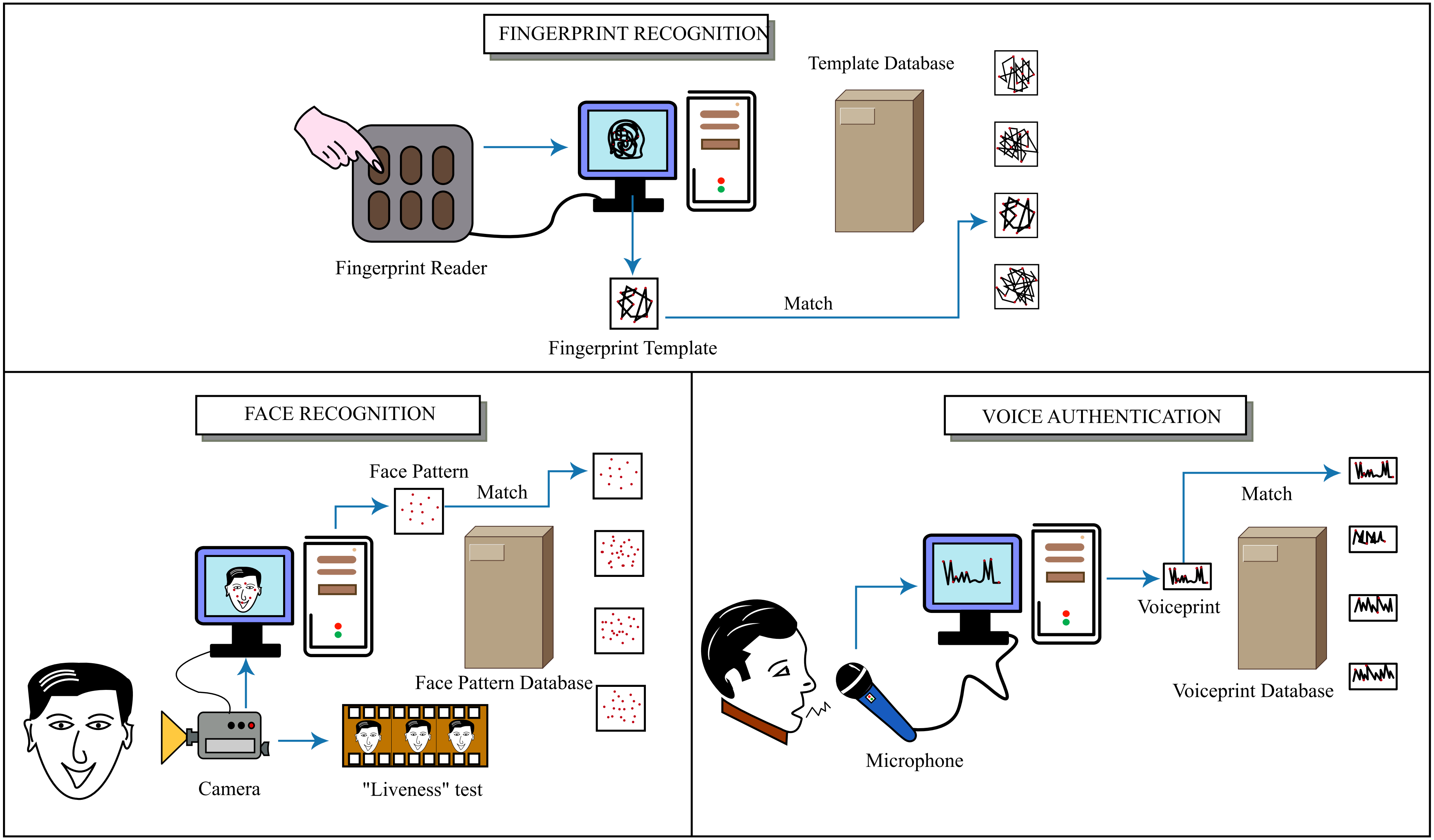


Figure by MIT OCW.

# Sneaking through the backdoor…

- Strategies whose goal is to gain control by bypassing access control defenses

- Exploit "holes" 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?

# Spyware, Adware, Malware

- 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
  - Surreptitiously 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 a firewall does

- 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

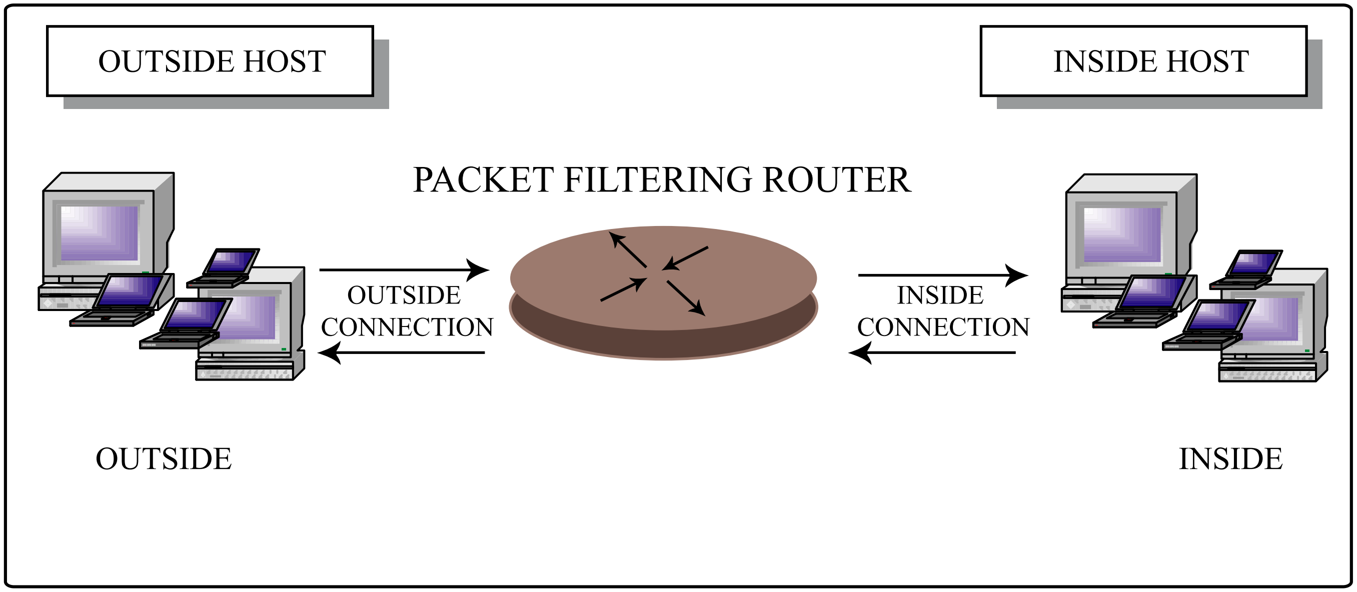


Figure by MIT OCW.

# Application-level gateways

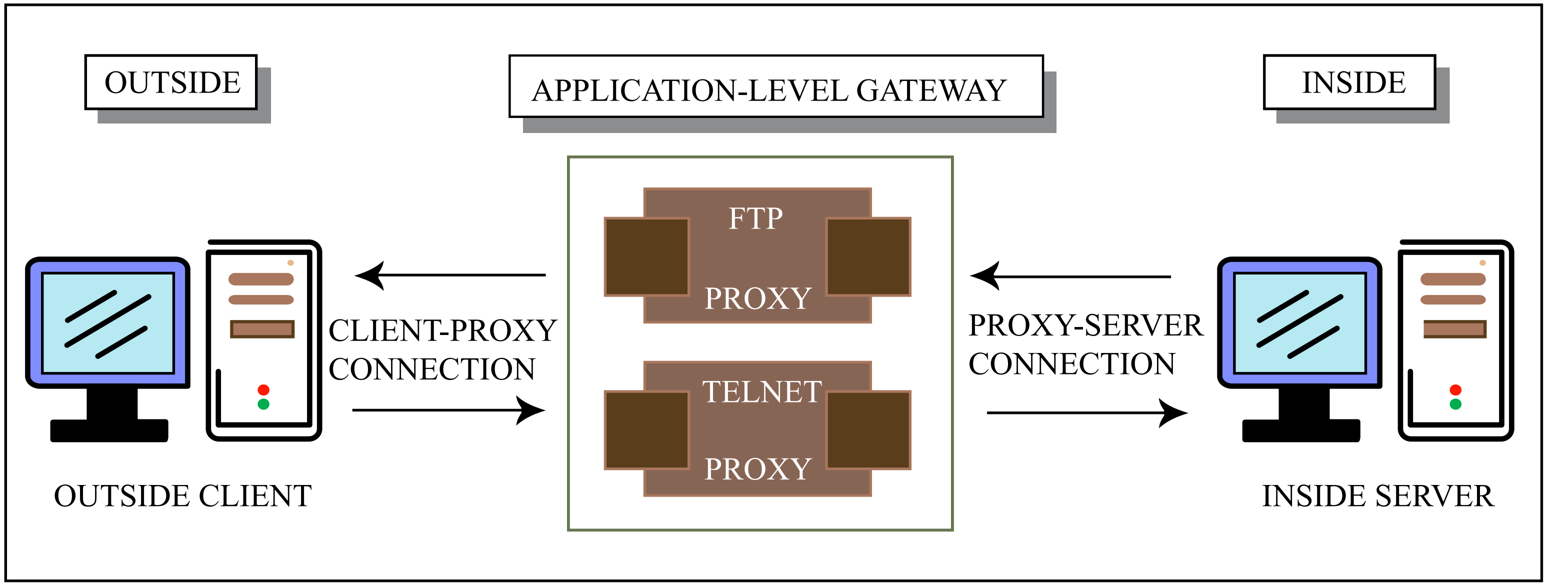


Figure by MIT OCW.

# Firewall performance/security tradeoffs

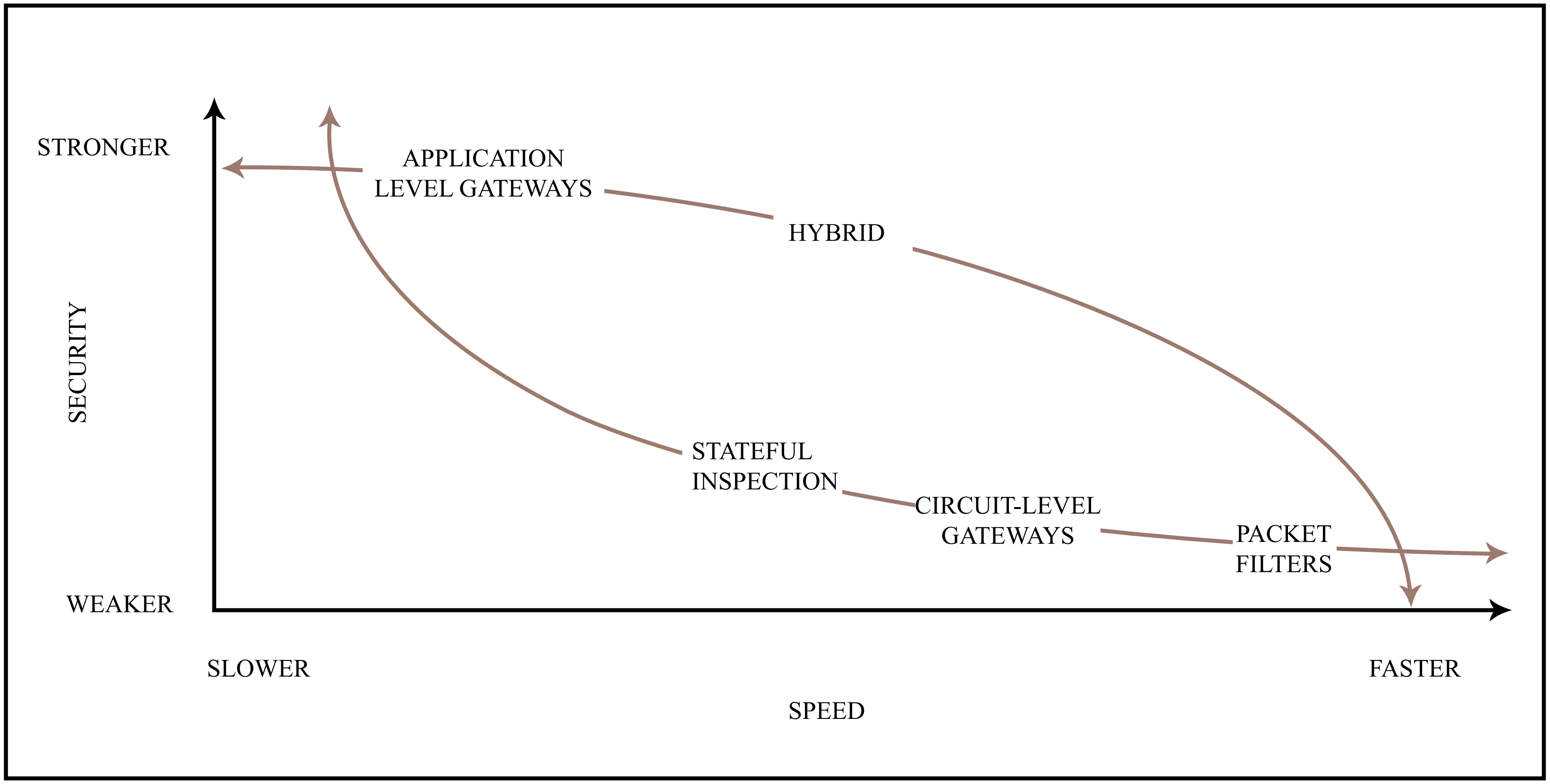


Figure by MIT OCW.

# 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.

# Despite all that… security breaches are on the rise

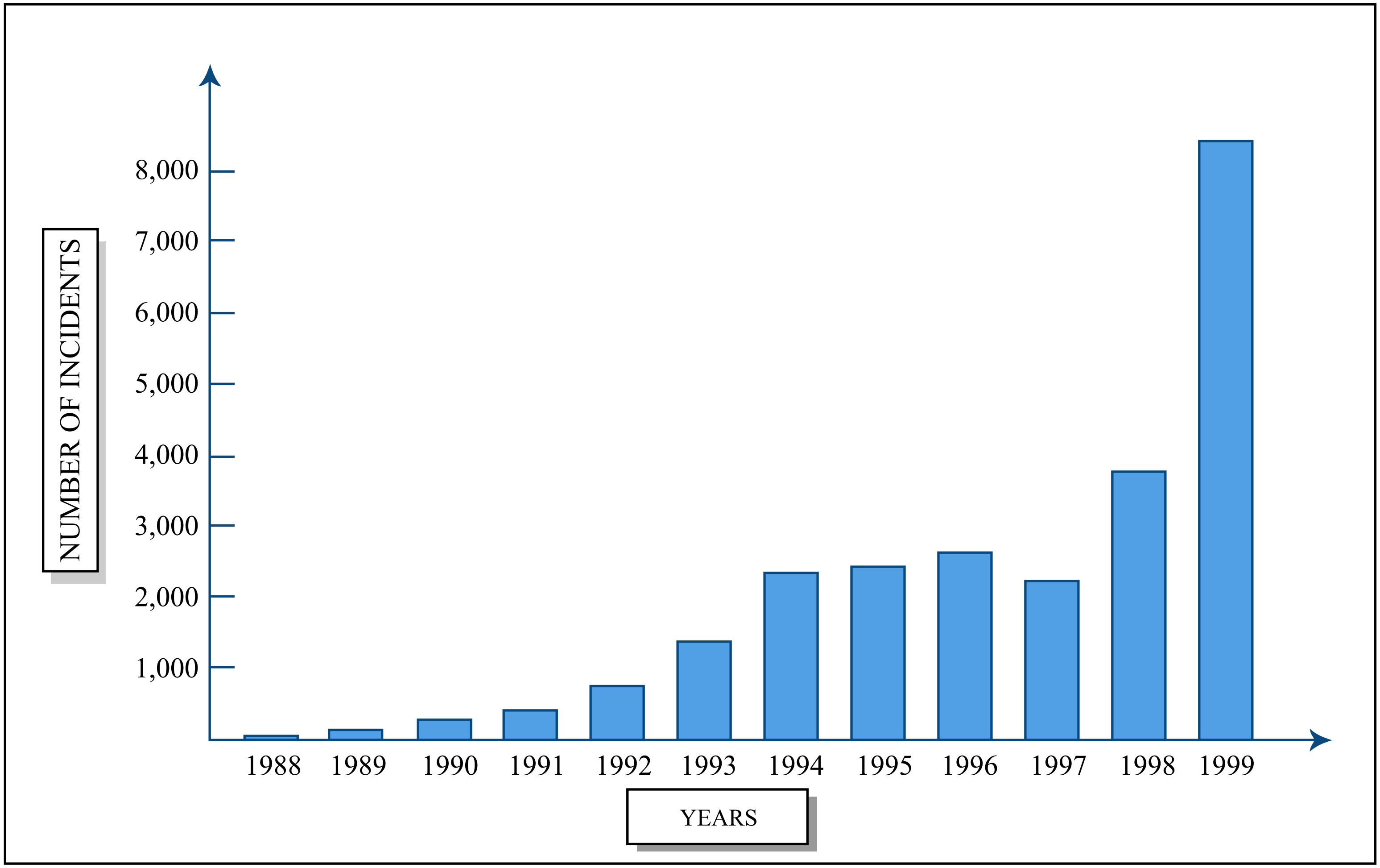


Figure by MIT OCW.

# .. and require far less technical expertise

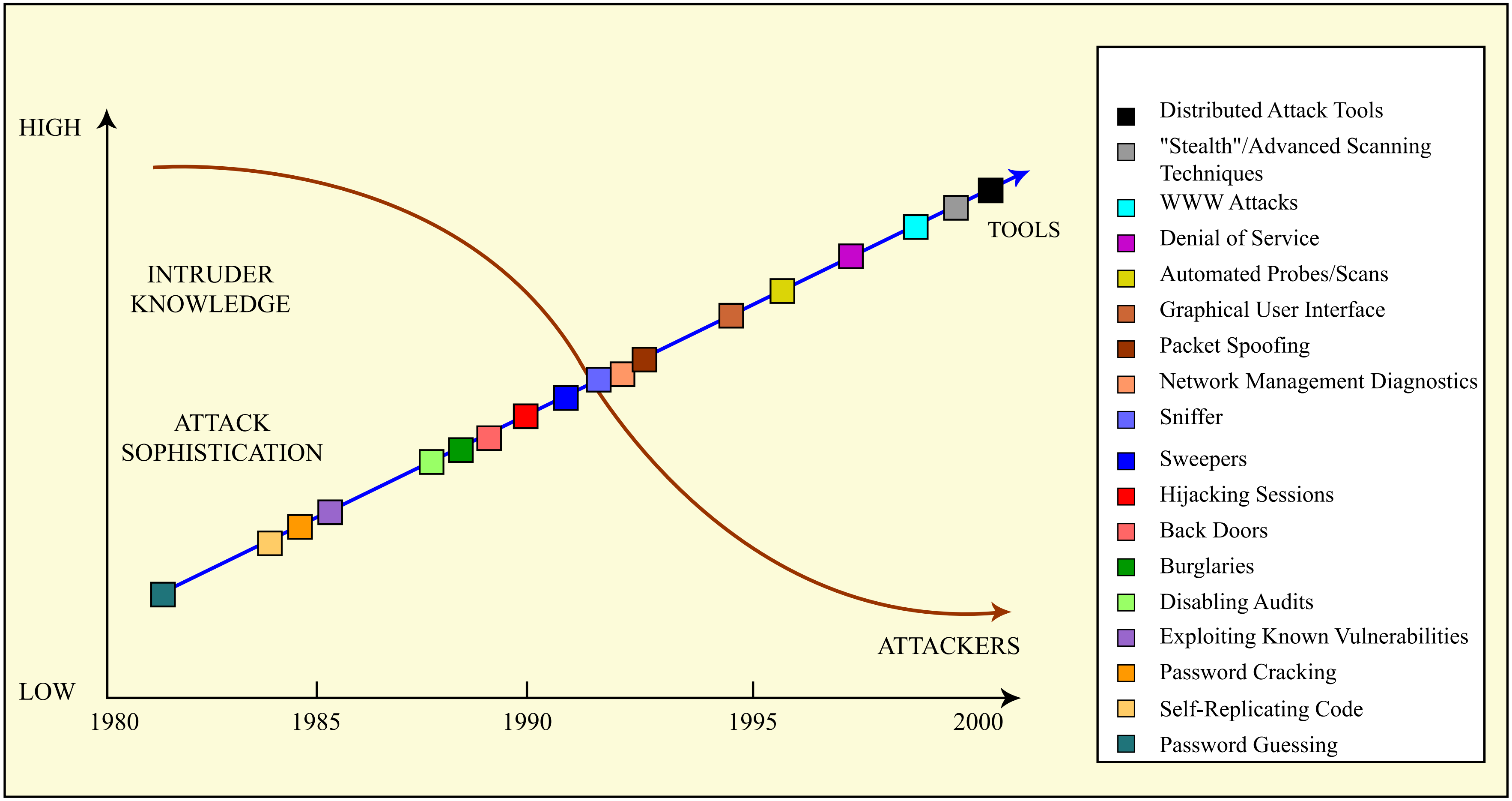


Figure by MIT OCW.

# Security Resources

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