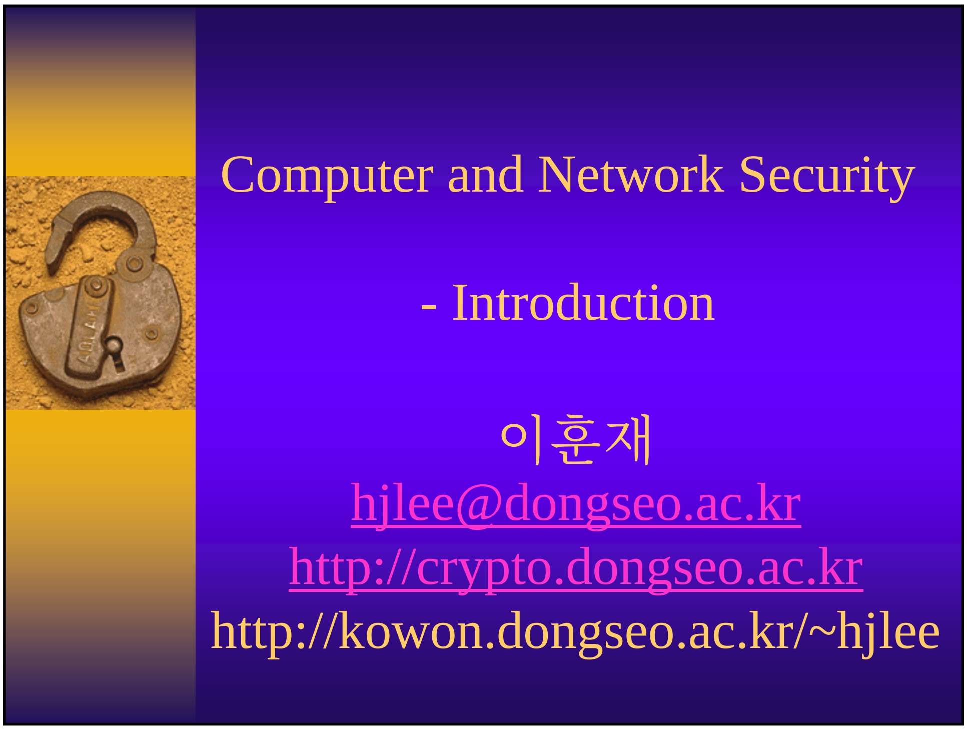
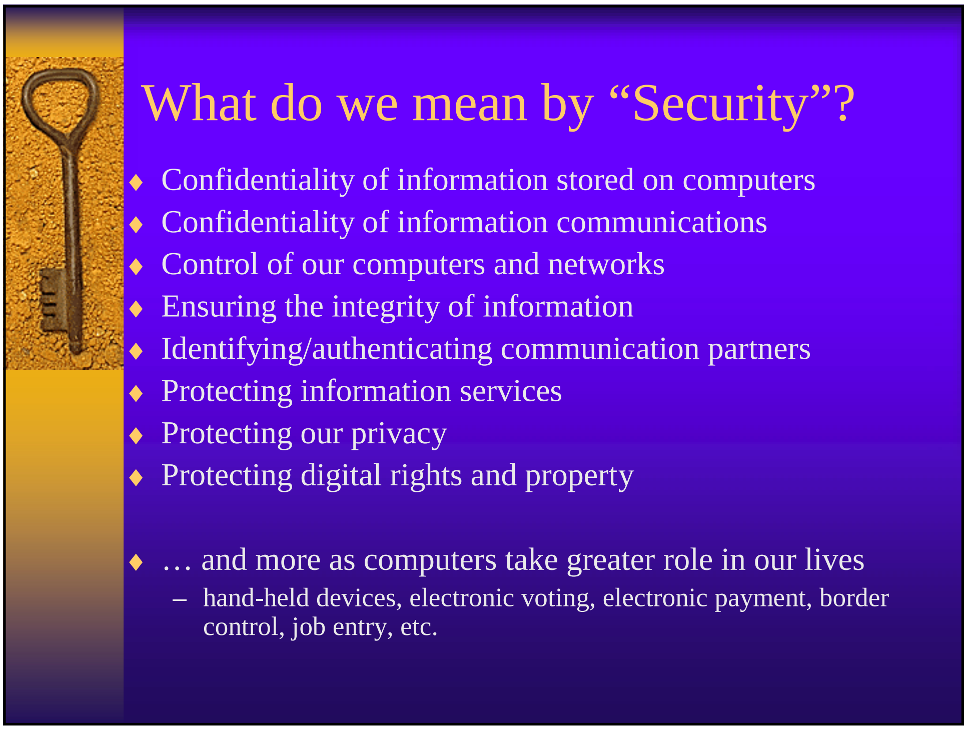


Computer and Network Security

- Introduction

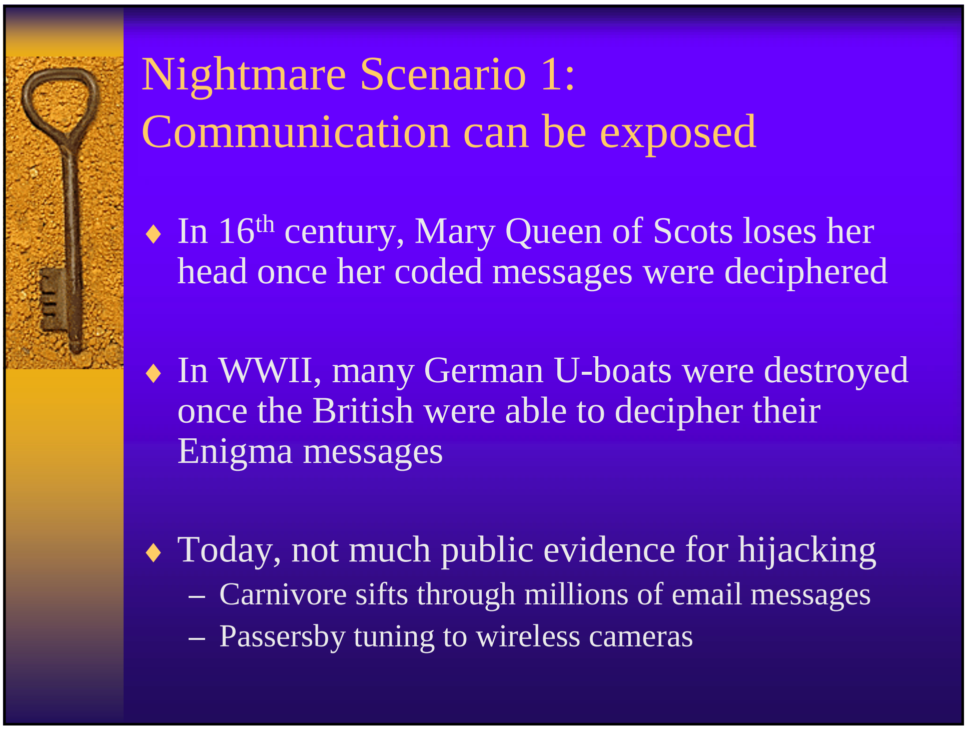
이훈재
hjlee@dongseo.ac.kr
http://crypto.dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee



What do we mean by “Security”?

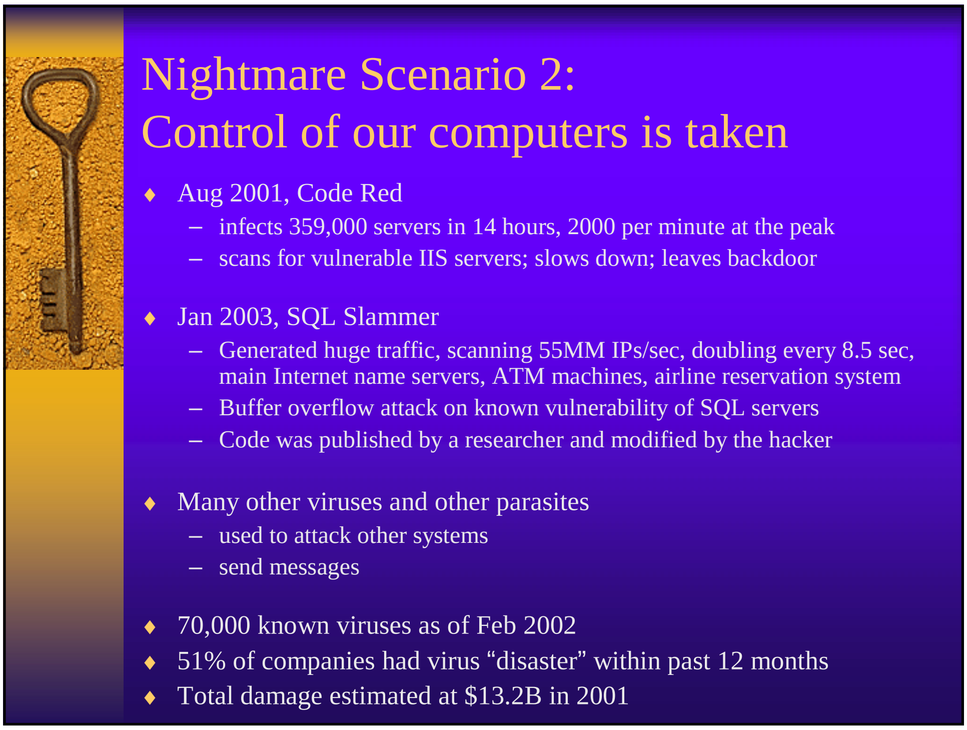
- Confidentiality of information stored on computers
- Confidentiality of information communications
- Control of our computers and networks
- Ensuring the integrity of information
- Identifying/authenticating communication partners
- Protecting information services
- Protecting our privacy
- Protecting digital rights and property

- … and more as computers take greater role in our lives
  - hand-held devices, electronic voting, electronic payment, border control, job entry, etc.



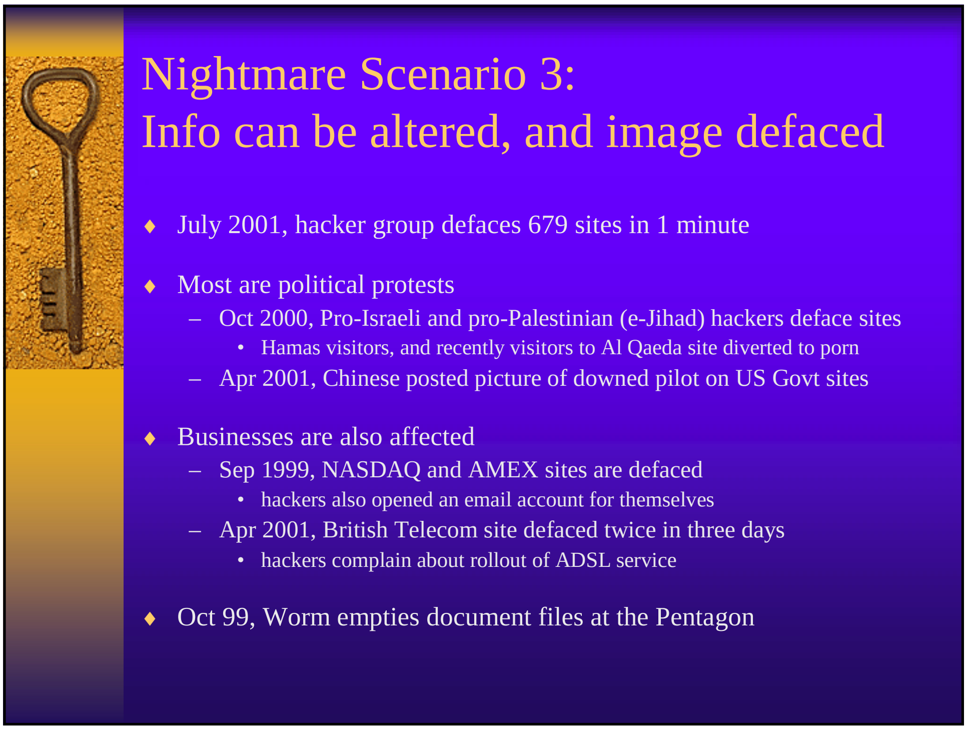
Nightmare Scenario 1: Communication can be exposed

- In 16th century, Mary Queen of Scots loses her head once her coded messages were deciphered
- In WWII, many German U-boats were destroyed once the British were able to decipher their Enigma messages
- Today, not much public evidence for hijacking
  - Carnivore sifts through millions of email messages
  - Passersby tuning to wireless cameras



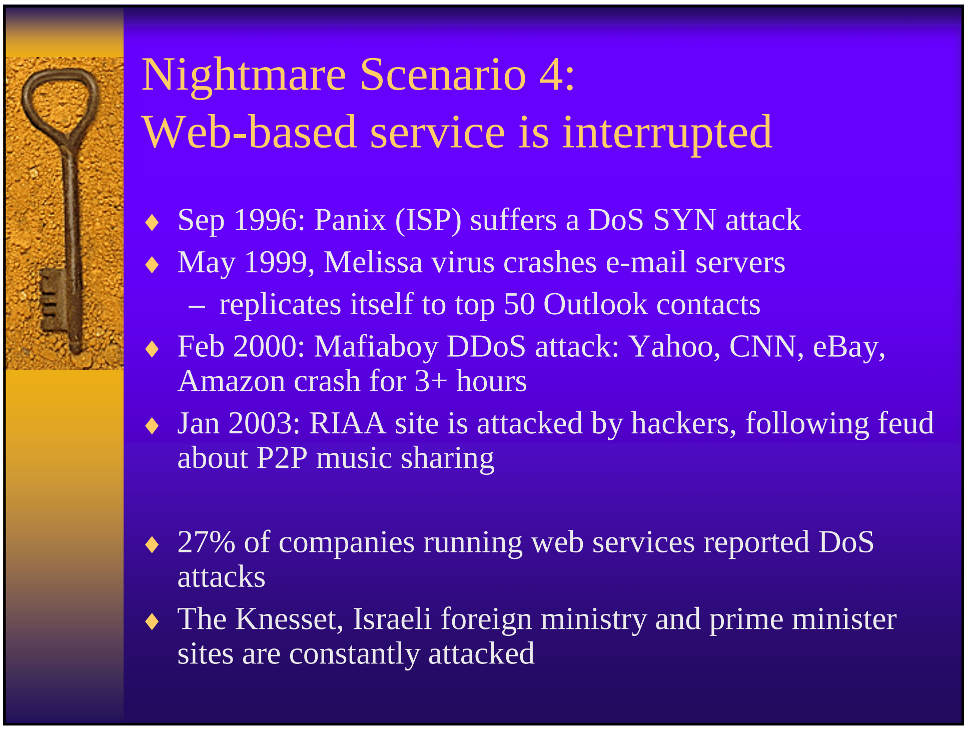
Nightmare Scenario 2: Control of our computers is taken

- Aug 2001, Code Red
  - infects 359,000 servers in 14 hours, 2000 per minute at the peak
  - scans for vulnerable IIS servers; slows down; leaves backdoor
- Jan 2003, SQL Slammer
  - Generated huge traffic, scanning 55MM IPs/sec, doubling every 8.5 sec, main Internet name servers, ATM machines, airline reservation system
  - Buffer overflow attack on known vulnerability of SQL servers
  - Code was published by a researcher and modified by the hacker
- Many other viruses and other parasites
  - used to attack other systems
  - send messages
- 70,000 known viruses as of Feb 2002
- 51% of companies had virus “disaster” within past 12 months
- Total damage estimated at $13.2B in 2001



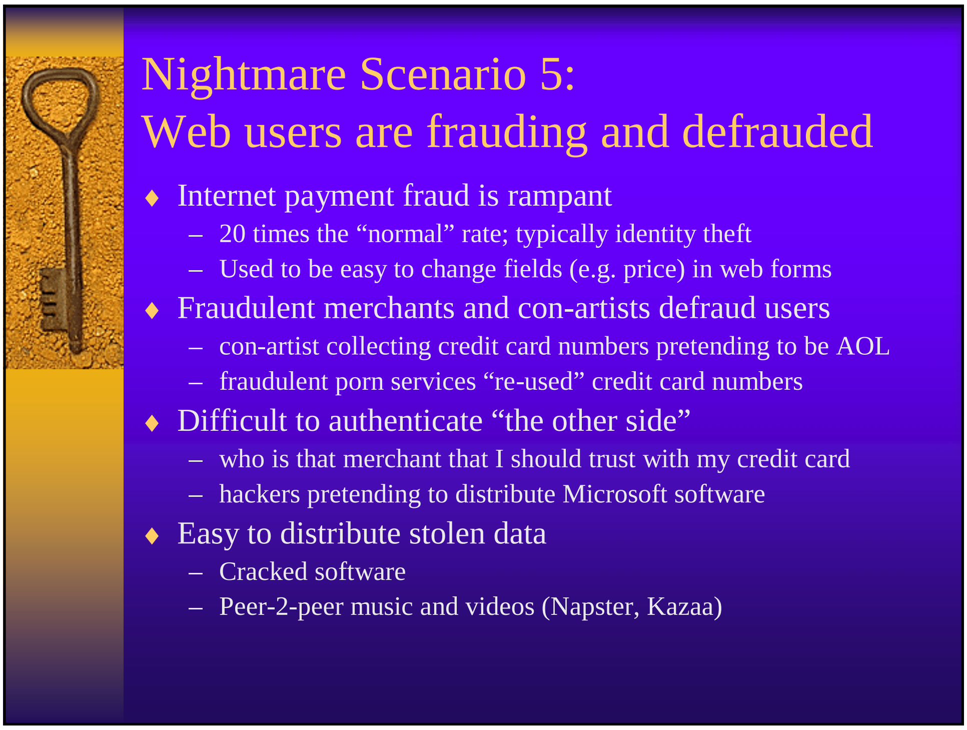
Nightmare Scenario 3: Info can be altered, and image defaced

- July 2001, hacker group defaces 679 sites in 1 minute
- Most are political protests
  - Oct 2000, Pro-Israeli and pro-Palestinian (e-Jihad) hackers deface sites
    - Hamas visitors, and recently visitors to Al Qaeda site diverted to porn
  - Apr 2001, Chinese posted picture of downed pilot on US Govt sites
- Businesses are also affected
  - Sep 1999, NASDAQ and AMEX sites are defaced
    - hackers also opened an email account for themselves
  - Apr 2001, British Telecom site defaced twice in three days
    - hackers complain about rollout of ADSL service
- Oct 99, Worm empties document files at the Pentagon



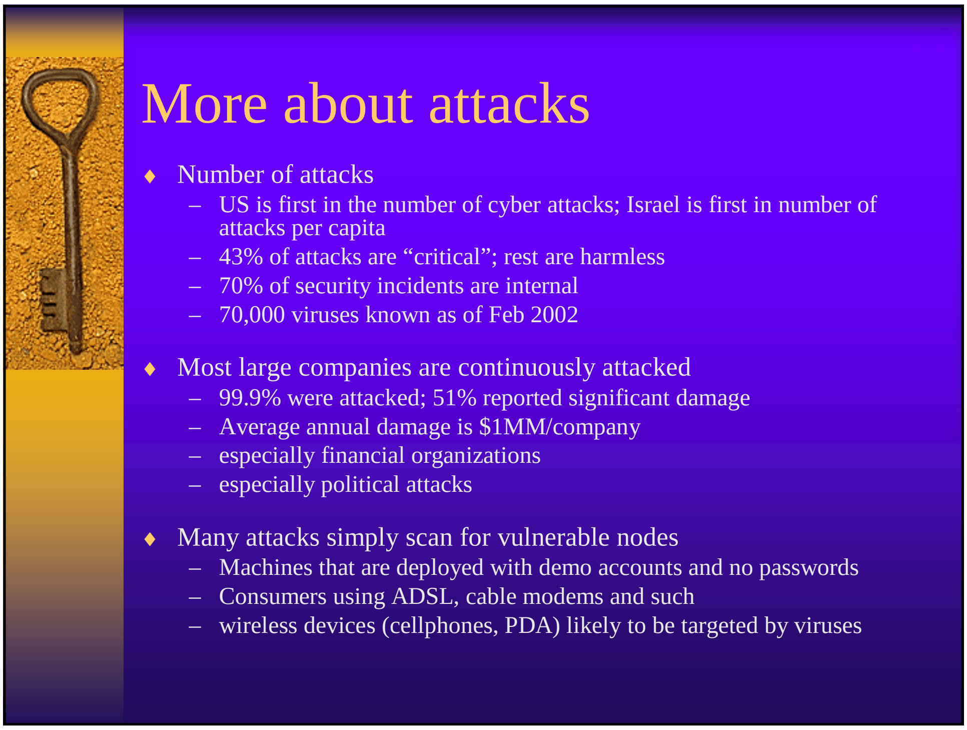
Nightmare Scenario 4: Web-based service is interrupted

- Sep 1996: Panix (ISP) suffers a DoS SYN attack
- May 1999, Melissa virus crashes e-mail servers
  - replicates itself to top 50 Outlook contacts
- Feb 2000: Mafiaboy DDoS attack: Yahoo, CNN, eBay, Amazon crash for 3+ hours
- Jan 2003: RIAA site is attacked by hackers, following feud about P2P music sharing
- 27% of companies running web services reported DoS attacks
- The Knesset, Israeli foreign ministry and prime minister sites are constantly attacked



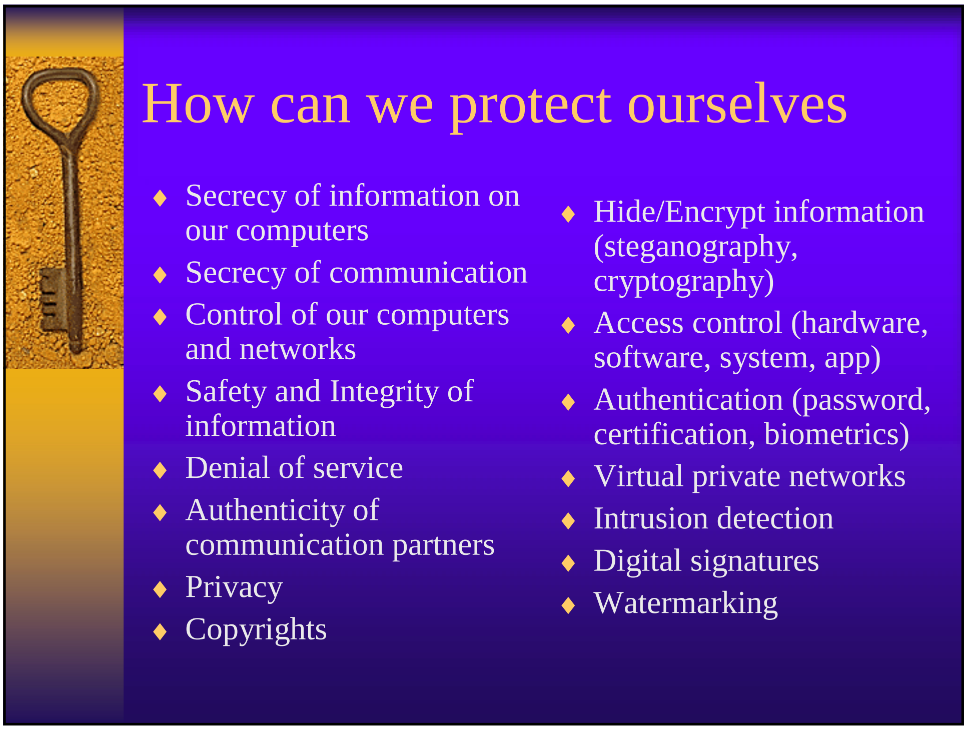
Nightmare Scenario 5: Web users are frauding and defrauded

- Internet payment fraud is rampant
  - 20 times the “normal” rate; typically identity theft
  - Used to be easy to change fields (e.g. price) in web forms
- Fraudulent merchants and con-artists defraud users
  - con-artist collecting credit card numbers pretending to be AOL
  - fraudulent porn services “re-used” credit card numbers
- Difficult to authenticate “the other side”
  - who is that merchant that I should trust with my credit card
  - hackers pretending to distribute Microsoft software
- Easy to distribute stolen data
  - Cracked software
  - Peer-2-peer music and videos (Napster, Kazaa)



More about attacks

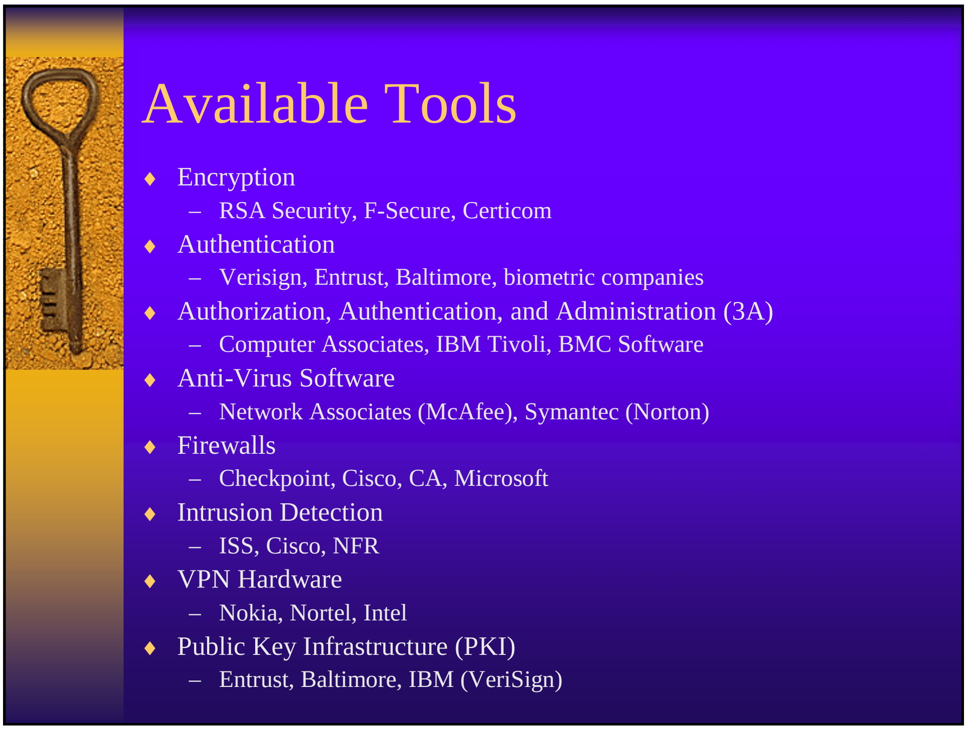
- Number of attacks
  - US is first in the number of cyber attacks; Israel is first in number of attacks per capita
  - 43% of attacks are “critical”; rest are harmless
  - 70% of security incidents are internal
  - 70,000 viruses known as of Feb 2002
- Most large companies are continuously attacked
  - 99.9% were attacked; 51% reported significant damage
  - Average annual damage is $1MM/company
  - especially financial organizations
  - especially political attacks
- Many attacks simply scan for vulnerable nodes
  - Machines that are deployed with demo accounts and no passwords
  - Consumers using ADSL, cable modems and such
  - wireless devices (cellphones, PDA) likely to be targeted by viruses



How can we protect ourselves

- Secrecy of information on our computers
- Secrecy of communication
- Control of our computers and networks
- Safety and Integrity of information
- Denial of service
- Authenticity of communication partners
- Privacy
- Copyrights

- Hide/Encrypt information (steganography, cryptography)
- Access control (hardware, software, system, app)
- Authentication (password, certification, biometrics)
- Virtual private networks
- Intrusion detection
- Digital signatures
- Watermarking

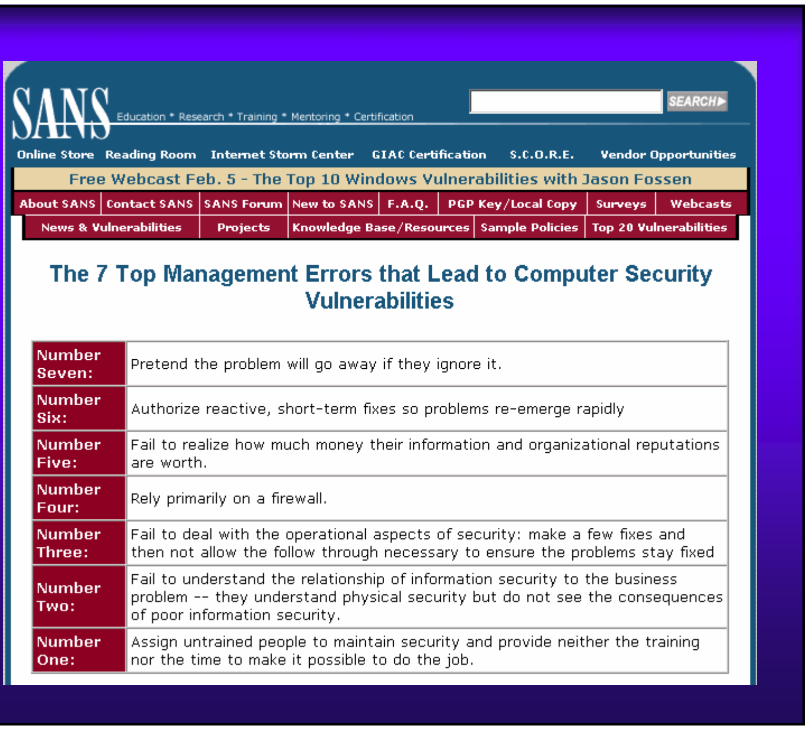


Available Tools

- Encryption
  - RSA Security, F-Secure, Certicom
- Authentication
  - Verisign, Entrust, Baltimore, biometric companies
- Authorization, Authentication, and Administration (3A)
  - Computer Associates, IBM Tivoli, BMC Software
- Anti-Virus Software
  - Network Associates (McAfee), Symantec (Norton)
- Firewalls
  - Checkpoint, Cisco, CA, Microsoft
- Intrusion Detection
  - ISS, Cisco, NFR
- VPN Hardware
  - Nokia, Nortel, Intel
- Public Key Infrastructure (PKI)
  - Entrust, Baltimore, IBM (VeriSign)

In the end, its People

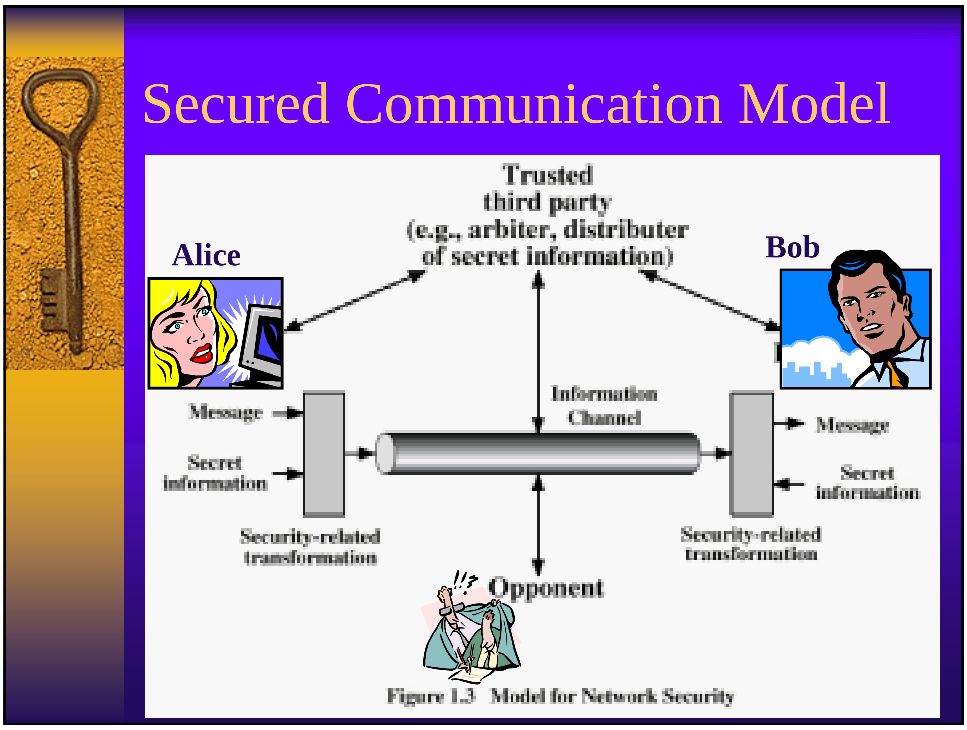
- People, not technology, are often the weakest link in any security system
- Create business processes that educate and involve people
  - Organizational policy
    - Perform risk analysis - different resources are at different risk
    - Create and enforce a clear provisioning policy for privileges
    - Enforce Separation of Duty principles
    - Update patches, and protective software regularly
  - Protect the people that protect resources
    - Educate service people not to fall prey to social engineering
    - Choose good passwords and protect them
- Treat security an important part of doing business. It is not less important than features and performance (Bill Gates)



The 7 Top Management Errors that Lead to Computer Security Vulnerabilities

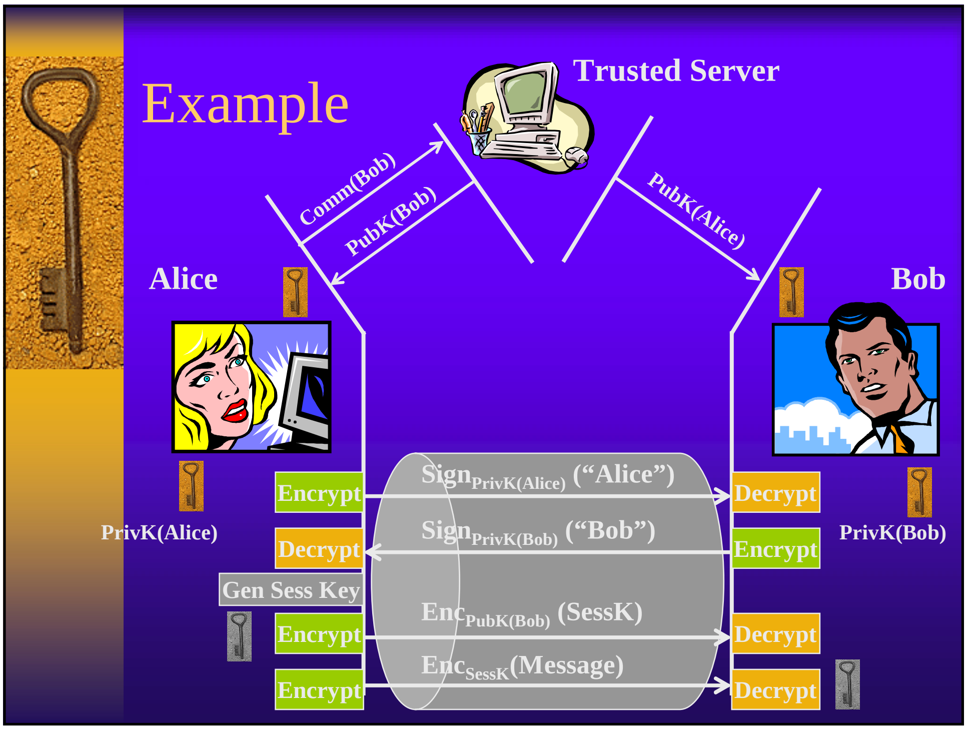
Number Seven:	Pretend the problem will go away if they ignore it.
Number Six:	Authorize reactive, short-term fixes so problems re-emerge rapidly
Number Five:	Fail to realize how much money their information and organizational reputations are worth.
Number Four:	Rely primarily on a firewall.
Number Three:	Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed
Number Two:	Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
Number One:	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Computer Security:
An Overview



Secured Communication Model

Figure 1.3 Model for Network Security



Example

Trusted Server

Comm(Bob)

PubK(Bob)

PubK(Alice)

Alice

Bob

PrivK(Alice)

PrivK(Bob)

Encrypt

Decrypt

Gen Sess Key

Encrypt

Encrypt

$\text{Sign}_{\text{PrivK(Alice)}}$ (“Alice”)

$\text{Sign}_{\text{PrivK(Bob)}}$ (“Bob”)

$\text{Enc}_{\text{PubK(Bob)}}$ (SessK)

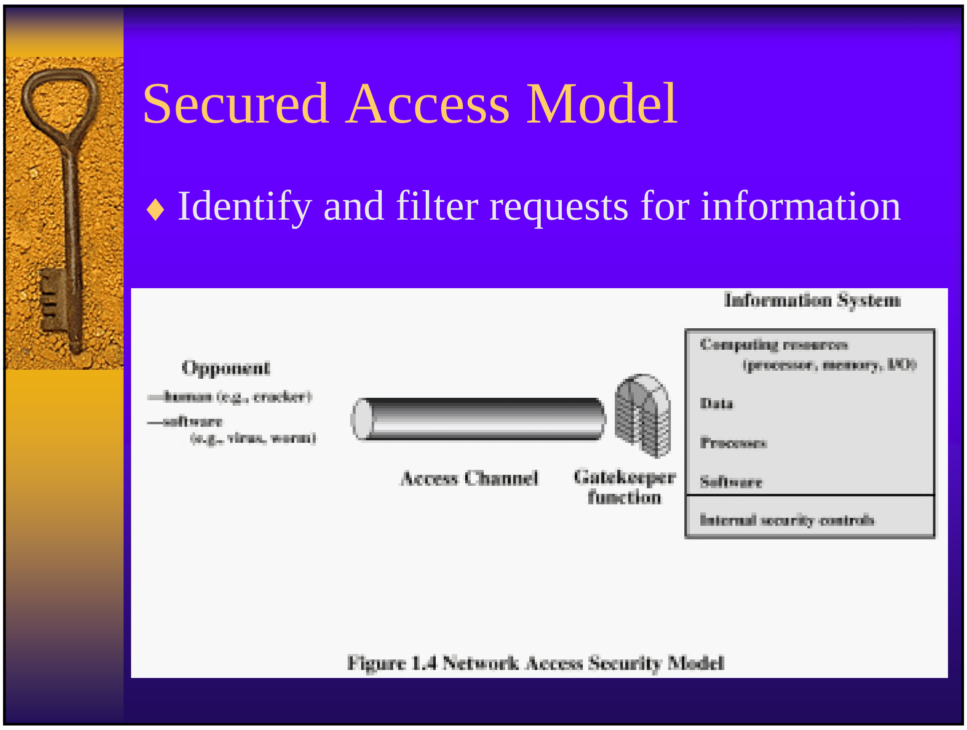
$\text{Enc}_{\text{SessK}}$(Message)

Decrypt

Encrypt

Decrypt

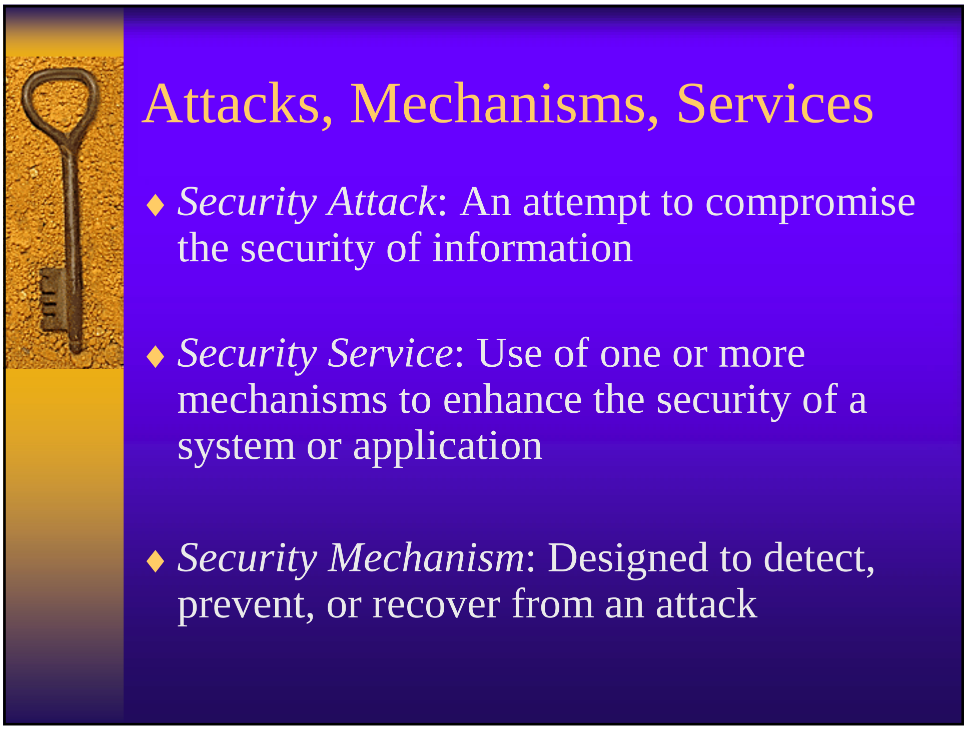
Decrypt



Secured Access Model

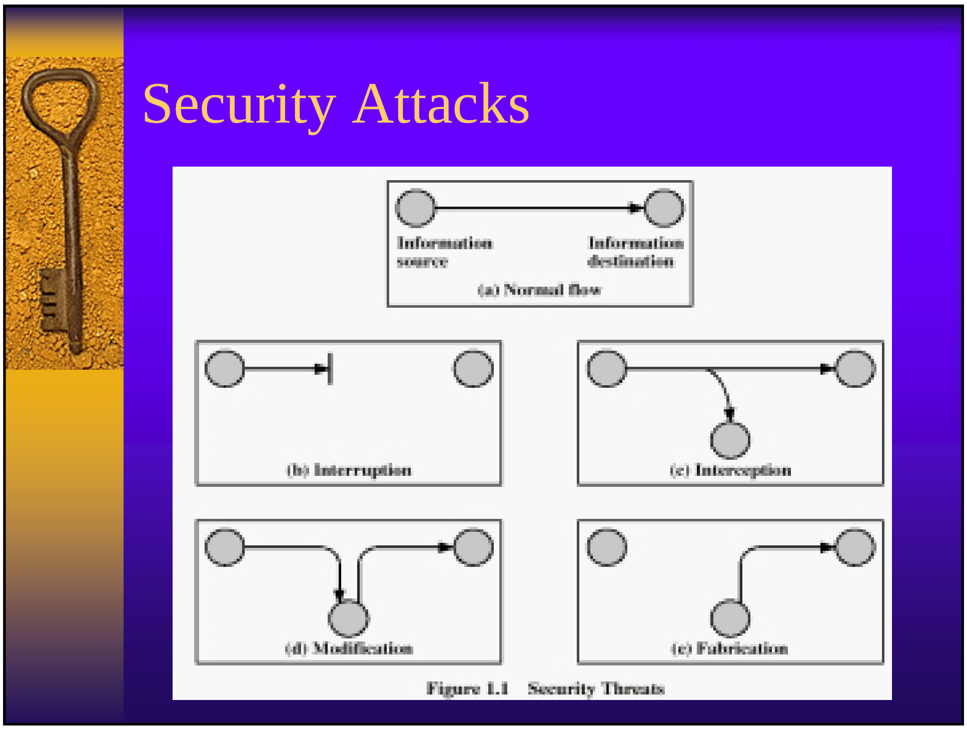
- Identify and filter requests for information

Figure 1.4 Network Access Security Model



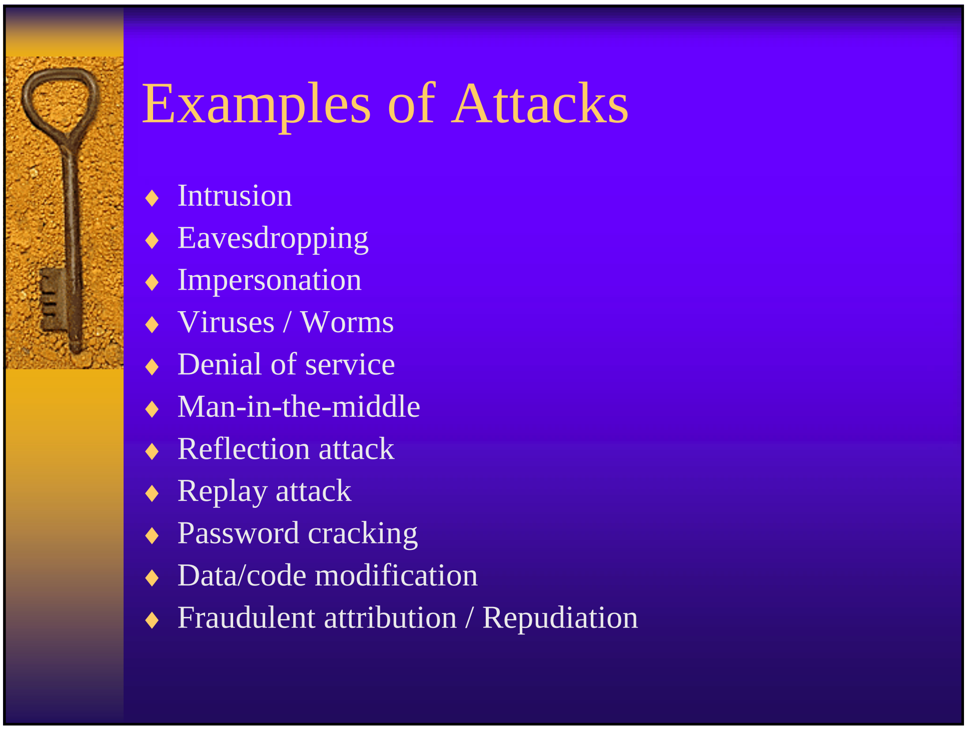
Attacks, Mechanisms, Services

- ♦ *Security Attack*: An attempt to compromise the security of information
- ♦ *Security Service*: Use of one or more mechanisms to enhance the security of a system or application
- ♦ *Security Mechanism*: Designed to detect, prevent, or recover from an attack



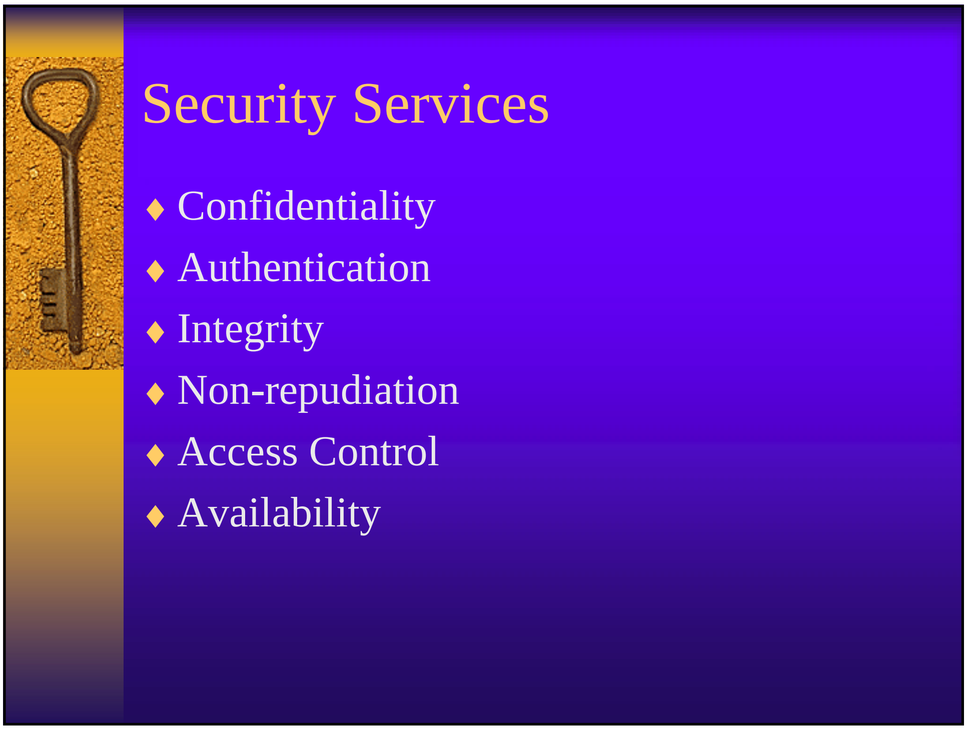
Security Attacks

Figure 1.1 Security Threats



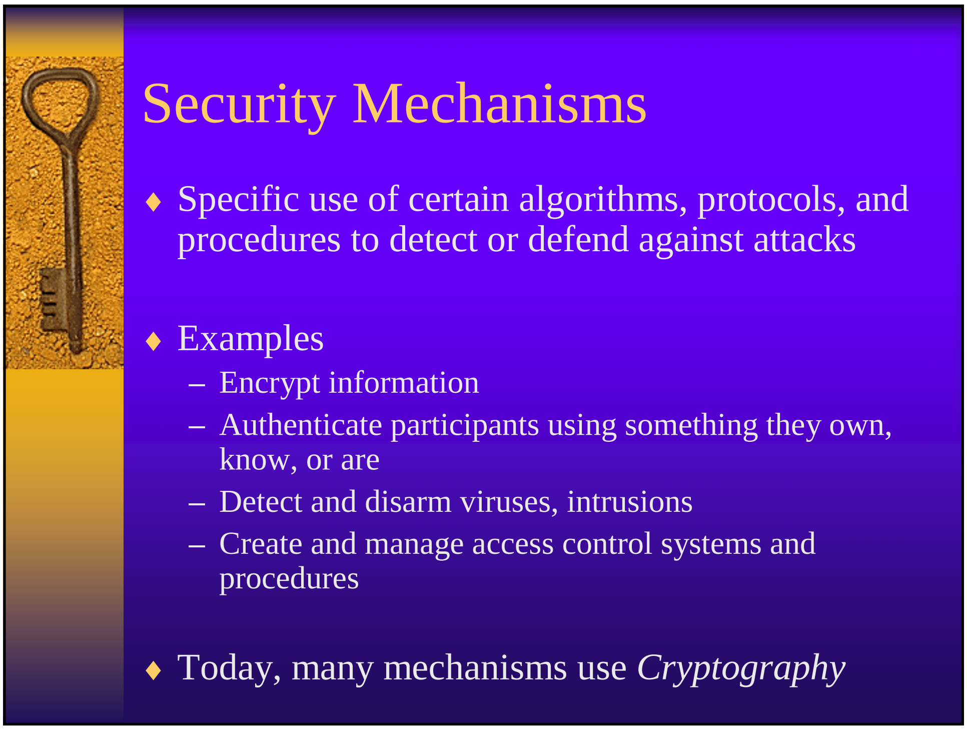
Examples of Attacks

- Intrusion
- Eavesdropping
- Impersonation
- Viruses / Worms
- Denial of service
- Man-in-the-middle
- Reflection attack
- Replay attack
- Password cracking
- Data/code modification
- Fraudulent attribution / Repudiation



Security Services

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Access Control
- Availability



Security Mechanisms

- Specific use of certain algorithms, protocols, and procedures to detect or defend against attacks
- Examples
  - Encrypt information
  - Authenticate participants using something they own, know, or are
  - Detect and disarm viruses, intrusions
  - Create and manage access control systems and procedures
- Today, many mechanisms use *Cryptography*