Web Technologies and Applications

Winter 2001

CMPUT 499: Security Issues

Dr. Osmar R. Zaïane

University of Alberta

Course Content

- Introduction
- Internet and WWW
- Protocols
- HTML and beyond
- Animation & WWW
- Java Script
- Dynamic Pages
- Perl Intro.
- Java Applets
- Databases & WWW
- SGML / XML
- Managing servers
- Search Engines
- Web Mining
- CORBA & SOAP
- **Security Issues**
- Selected Topics
- Projects

Objectives of Lecture 16

Security Issues

- Introduce the basic concepts and basic security mechanisms
- Get an overview of computer security as it applies to the Web environment.
- Understand the mechanism behind firewalls.
- Understand the issues pertaining to securing a web application and web transactions

Outline of Lecture 16

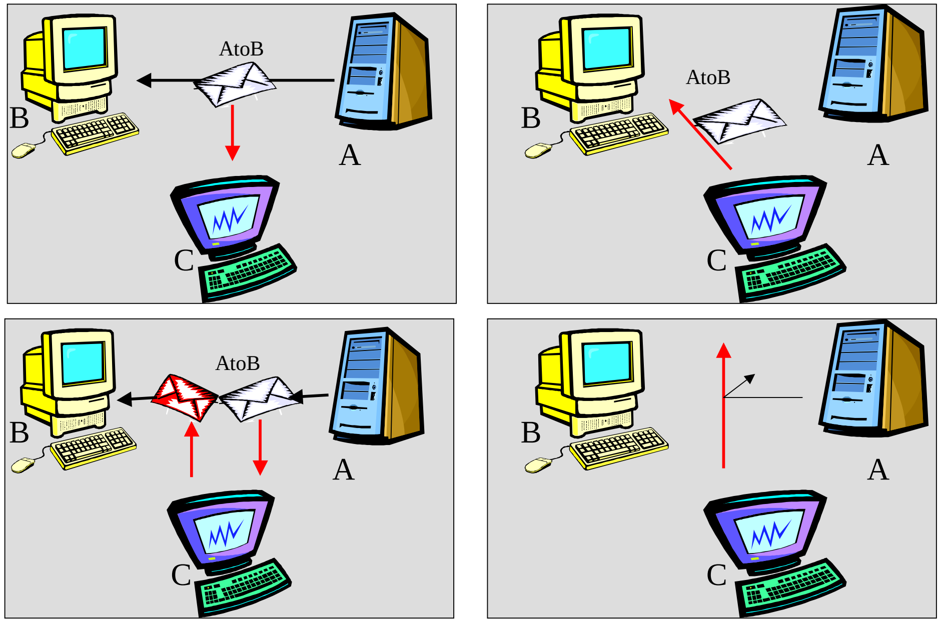
- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

What are the Risks?

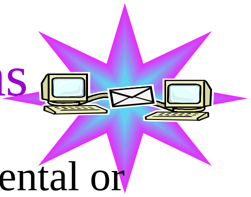
- Information intercepted:
  - Leakage of information
  - Privacy and confidentiality
  - Illegitimate use of data
- Information tempered:
  - Integrity of data
  - Jeopardize the application, communication, trust,…
- Illegal access
  - Integrity of data
  - Denial of service
  - viruses

What to Consider?

- **Data Integrity**: refers to protection from change: Is the data received exactly the same as the data that was sent?
- **Data Availability**: refers to protection against disruption of service: Does the data remain available for legitimate use?
- **Data Confidentiality**: refers to protection against unauthorized data access: Is data protected against unauthorized access?
- **Privacy**: refers to the ability of the sender to remain anonymous: Is the sender's identity revealed?

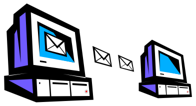


Integrity Mechanisms

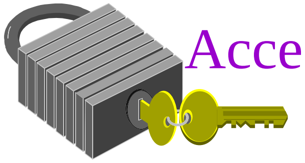


- Ensure data integrity against accidental or intentional damage using parity bits, checksum and cyclic redundancy checks (CRC).
- The sender computes a integer value as a function of the data in a packet.
- The receiver re-computes the integer from the received data and compares the result.
- **However, a attacker can create a valid checksum or CRC from the altered data.**

Guaranteeing Integrity



- Several mechanisms against malicious intentional change of intercepted data exist
- Transmitted data is encoded with a MAC (Message Authentication Code)
- A MAC uses cryptographic hashing mechanisms that can not be broken or forged
- Uses a secret key known only to the sender and receiver.
- The sender uses the secret key to scramble the data and the checksum or CRC
- Tempering with the data introduces errors



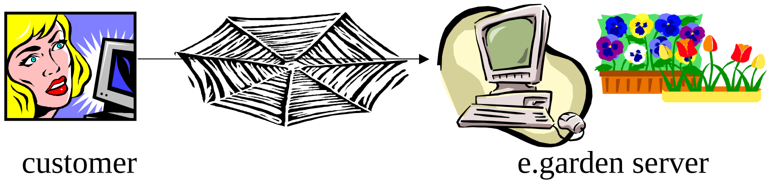
Access Control and Passwords

- On conventional computer systems, simple passwords are sufficient and efficient to protect the access to the system.
- Simple password mechanisms are vulnerable on networks because they are susceptible to eavesdropping.
- Wiretapping is easy especially that passwords on telnet, FTP or HTTP are clear text.

Outline of Lecture 16

- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

Who is Who?



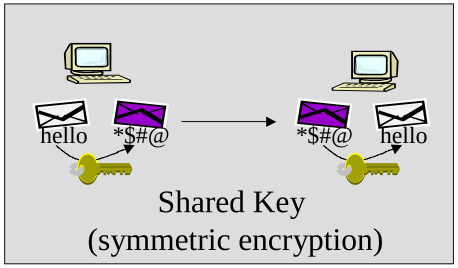
How do you know the customer is the customer he/she pretends to be?
How do you know the server is the server it purports to be?
Is it really the the web page I want to connect to?
Is it really the company I want to make a transaction with?
Is it really the customer I think I am dealing with?

Authentication

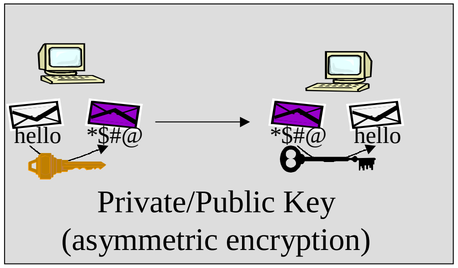
- The process of making sure the server and the client are indeed the server and client they purport to be is called *authentication*.
- User authentication is one of the most difficult aspect of computer security.
- Authentication is based on digital signatures
- To sign a message, the sender encrypts the message using a key known only to the sender

Encryption

• The encryption of a message ensures that the message remains confidential despite wiretapping.
• Sender Scrambles the bits of the message in a way that only the intended receiver can unscramble the message. Based on keys.
• Intercepting a messages is useless since no information extraction.



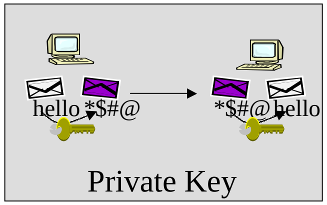
Shared Key
(symmetric encryption)



Private/Public Key
(asymmetric encryption)

Encryption with Shared Key

• The receiver and the sender share the same secret key
• The sender encrypts the message with a key K and the receiver decodes the encrypted message with the same key K.
• Example: DES



Private Key

E= *encrypt* (Key,M)
M=*decrypt* (Key,E)

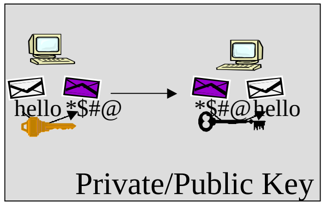
Mathematically *decrypt* is inverse of *encrypt*
decrypt = *encrypt*$^{-1}$

Encryption with Private/Public Key

• Encryption and decryption have *one-way* property.
• The encryption function has the mathematical property that a message encrypted with the public key cannot be easily decrypted except with the private key, and a message encrypted with the private key cannot be decrypted except with the public key.
• To ensure confidentiality, the sender uses public key of receiver to encrypt the message. Decryption requires receiver's private key.
• Example: RSA

E= *encrypt* (PrivK,M)
M=*decrypt* (pubk,E)

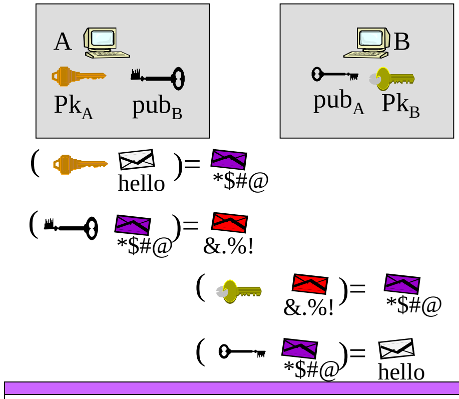
E=*encrypt*(pubk,M)
M=*decrypt*(PrivK,E)



Private/Public Key

Authentication with Digital Signature

- The encryption mechanism can be used for authentication.
- If two parties each has a private key and the public key of the other, the scenario is as follows:



•When A wants to send a message to B

•A signs the message with PK$_A$ then encrypts the message with pub$_B$

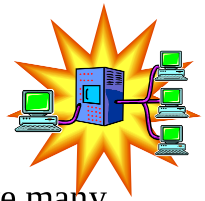
•B receives the message and is the only one to decode it with PK$_B$ then uses pub$_A$ to decrypt it

•The message is authentic since only A has PK$_A$ and confidential since only B has PK$_B$

Outline of Lecture 16

- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

Internet Firewall



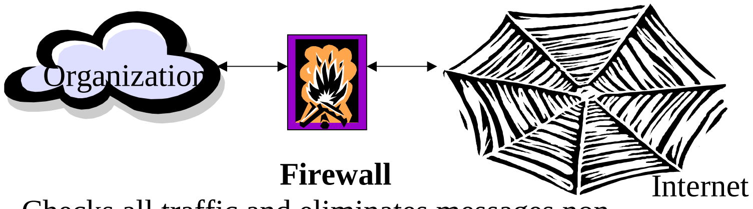
- Although encryption technology helps solve many security problems another technology is also needed.
- Securing every computer in an organization is too expensive. Better create a protective wall
- Firewall technology helps protect an organization’s computers and networks from unwanted Internet traffic.
- The firewall is placed between the organization and the rest of the Internet to keep problems spreading from the Internet to the organization.

Firewalls

- All traffic entering the organization passes through the firewall
- All traffic leaving the organization passes through the firewall
- The firewall rejects any traffic that does not adhere to security policy of the organization
- The firewall itself is immune to security attacks
- If an organization has multiple Internet connections, a firewall should be placed on each

Firewall Tasks

- The firewall prevent outsiders from probing all computers in an organization
- Prevents flooding the organization’s network with unwanted traffic
- Prevent attacking a computer by sending a sequence of IP datagrams that is known to cause the computer system to misbehave.



Checks all traffic and eliminates messages non conform to the security policy of the organization

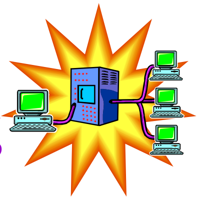
Packet Filtering

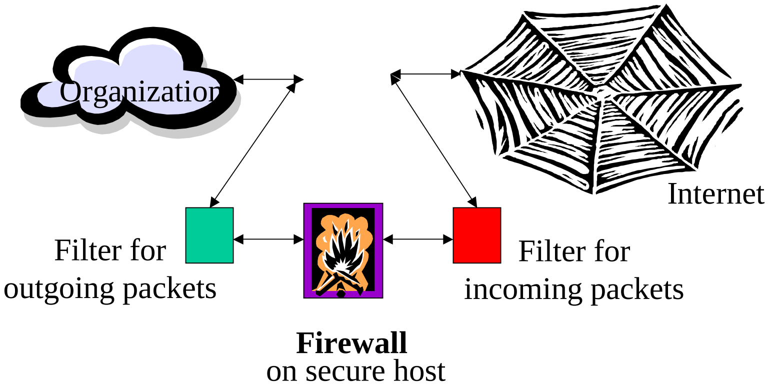
- Packet filtering is the primary mechanism that firewalls use.
- To control which computer in the organization that can communicate with the outside world, the firewall stops all packets with given IP address in the header.
- The same is used to control which computer from the outside can communicate with which computer in the organization.
- Discard specific packets based on the source and destination IP address in the packet header

Filtering Services

- In addition to low-level IP address packet filtering, we can also examine the protocol in the packet or the high-level service to which the packet correspond.
- Can prevent traffic on one service while allowing traffic to other service
- Example allow HTTP and SMTP and FTP only
- Can use a boolean combination of destination, source and services.

Firewall with Packet Filtering

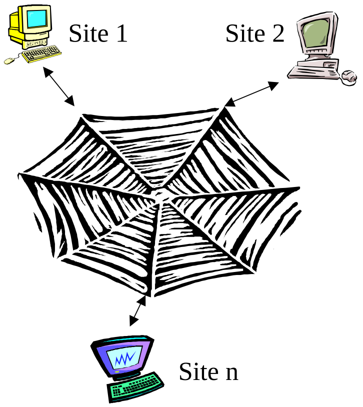




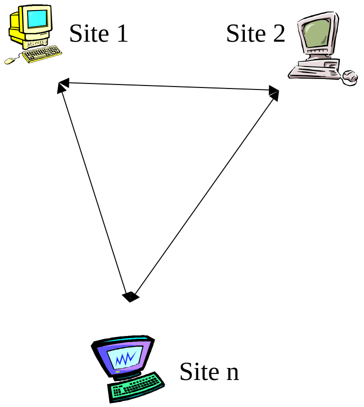
Outline of Lecture 16

- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

Private Networks



Typical Internet connection between routers at 3 sites



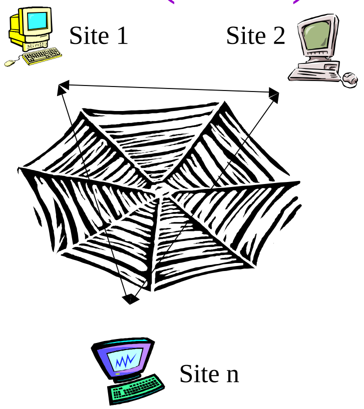
Dedicated connections between routers at 3 sites

Plus & Minus of Private Networks

- Using leased lines to interconnect sites makes the network completely secure (completely private)
- Nobody else has access or can read passing data
- Leasing dedicated lines ➔Very high costs
- Internet can not guarantee confidentiality but the costs are low: just get ISP on both ends.
- Can we have the advantages of both worlds?

Virtual Private Network (VPN)

- VPN is implemented in software
- Each router runs a VPN software
- VPN software acts as a packet filter
- VPN software encrypts packets, all communication remains confidential

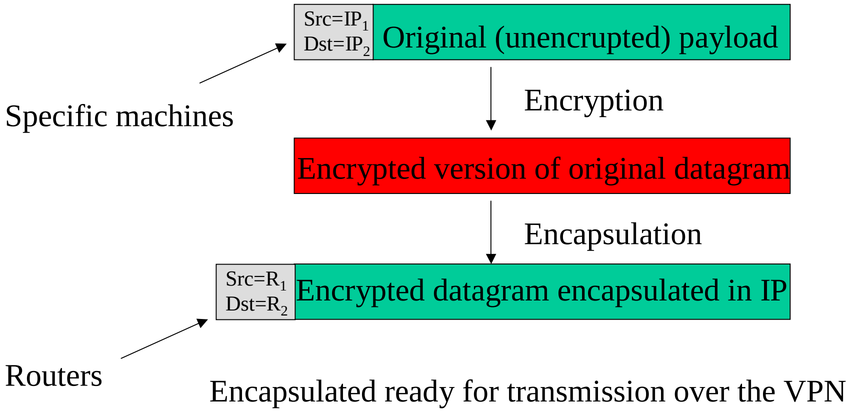


Logical connections between 3 sites with VPN software on routers

Tunneling

- Should the entire datagram be encrypted for transmission?
- If datagram header is encrypted, routers wouldn’t know who is the receiver
- If the packet header is not encrypted, some information could be deduced (who is sending and who is receiving may be observed)
- The keep information completely hidden VPN uses IP-in-IP tunneling

IP-in-IP Tunneling



Src=IP$_1$ Dst=IP$_2$ Original (unencrupted) payload

Specific machines

Encryption

Encrypted version of original datagram

Encapsulation

Src=R$_1$ Dst=R$_2$ Encrypted datagram encapsulated in IP

Routers

Encapsulated ready for transmission over the VPN

Outline of Lecture 16

- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

Secure HTTP

- S-HTTP request header
  - Secure * secure-HTTP/1.1
  - Content-Privacy-Domain *PEM or PKS-7*
  - Content-Type: application/http
  - Security-Scheme, Certificate-Info, Key-Assign
- S-HTTP response header
  - Secure-HTTP/1.1 200 OK

Negotiation

- S-HTTP allows both parties to negotiate their needs and preferences regarding security parameters (algorithm, key length,etc.)

Vulnerability

- S-HTTP is vulnerable since it is susceptible to low level attacks at the TCP or IP level. It is secure at the application level only.

Secure Socket Layer (SSL)

See assignment 6

- Unlike secure HTTP, SSL is implemented at a lower layer in the OSI model. Therefore, it can be used to enhance security in not only HTTP, but in other protocols such as FTP, telnet, NNTP, etc.
- SSL opens and maintains a secure channel through which communication takes place.
- Unlike HTTP, SSL is stateful.

Secure Channel Properties

- **Channel is authenticated**: The server always authenticates the clients and the clients can authenticate the server. Use of asymmetric cryptography with public/private key
- **Channel is private**: Encryption is used for all messages after a handshake is used to define a secret key. Use of symmetric cryptography for data encryption.
- **Channel is reliable**: Each message includes a message integrity check using a MAC

SSL Handshake

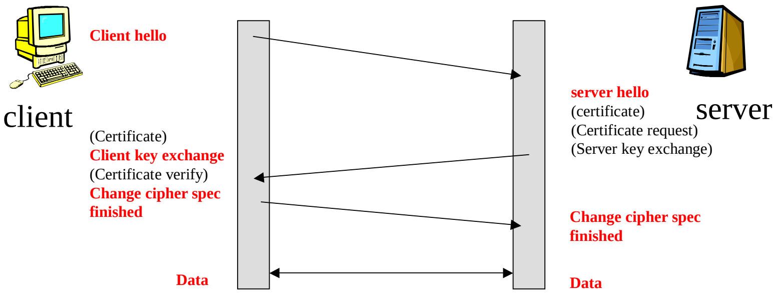
- During an SSL session, some variables need to be defined. The server needs to determine:
  - Version of SSL supported
  - Encryption algorithm to be used
  - Session ID (each SSL session has a unique ID)
  - Compression algorithm to be used (if needed)
  - 2 random numbers
- These are determined at the negotiation phase known as handshake (SSL handshake protocol)
- Authentication also occurs at the handshake

Handshake Protocol

1. Browser transmits a *client hello* message
2. The server sends back a *server hello* message
3. The server sends its certificate if the client must authenticate the server. A *server key exchange* message may be sent for the agreed upon encryption algorithm
4. The server requests a certificate from the client
5. The server transmits a *server hello done* message
6. If requested the client send a certificate or *no certificate alert* message.A *client key exchange* message is sent.

Handshake Protocol

7. If everything is fine, the client sends a *change cipher spec* message with the parameters agreed upon.
8. Client sends a *finished* message
9. The server sends its own *change cipher spec* message
10. The server sends a *finished* message



Certificates

- A certificate is an electronic method of verifying the authenticity of a server
- A client verifies if the server it has connected to is the right server by checking the certificate
- The certificate is checked against a list of certificates stored in a database or a certificate authority, a third party that issues certificates
- Certificates have expiration dates.
- You can issue your own certificates and distribute them to users you authorize to access your site.

Outline of Lecture 16

- Aspects of Security
- Authentication and Encryption
- Internet Firewalls and Packet Filtering
- Virtual Private Networks
- Secure HTTP (SHTTP) and Secure Socket Layer (SSL)
- Securing your Site

Basic Steps

- Make sure CGI scripts execute under ownership of fake user (nobody or www) which has very little privileges
- All documents and programs should be writable only by owner
- Logs should not be writable or readable by the world
- Support usernames and passwords whenever needed.
- Always create *index.html* in all directories

Consider Problems with CGI

- Be careful what sort of scripts can be uploaded on the server
- Validate input of Forms and be strict
- Ex: “/usr/lib/sendmail *user*”

  and *user* is

  “john.smith@somewhere.ca; rm index.html”

  In Perl or other languages, this could be executed by the system after sending the e-mail