

**Security & Privacy
on the WWW**

Briefing for CS4173

Topic Outline

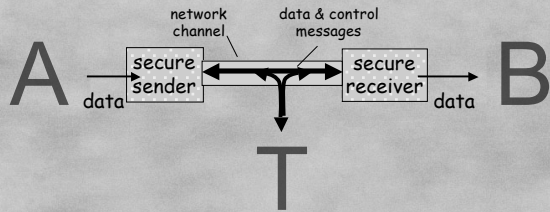
1. Information Security
 - Relationship to safety
 - Definition of important terms
 - Where breaches can occur
 - Web techniques
 - Components of security
 - Firewalls, and Encryption
 - Secure Socket Layer (SSL) & HTTPS
2. Privacy
 - Definition
 - Reasons for concern
 - Rôles
 - Web Techniques: P3P

Information Security

‘[The] protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.’

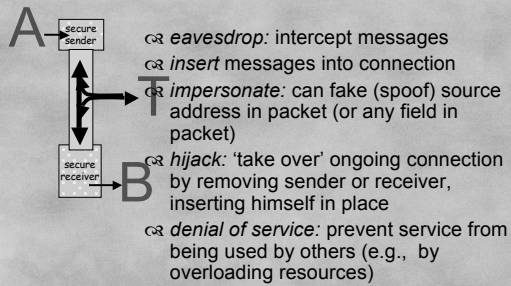
— Alliance for Telecommunications Industry Solutions (ATIS)
Network Performance, Reliability, and Quality of Service Subcommittee
<http://www.atis.org/tg2k/_information_systems_security.html>

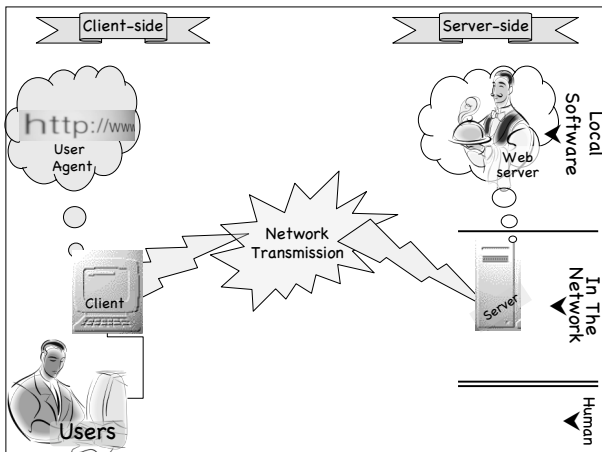
Security Issues in a Nutshell



Based on a diagram by Kurose & Ross

What can 'the intruder' do?★





Components of Security

Protection				Assurance	
Authorization	Accountability	Availability			
Access Control	Data Protection	Auditing	Non-repudiation	Service Continuity	Disaster Recovery
Authentication				Design Assurance	
Cryptography				Development Assurance	
				Operational Assurance	

Diagram by
Konstantin Beznosov

Important Concepts (1 of 2)★

Confidentiality: only sender, intended receiver should “understand” message contents
 ☞ sender encrypts message
 ☞ receiver decrypts message

Authentication: sender and receiver want to confirm identity of each other

Trust: sender and receiver must have confidence in system and its maintainers

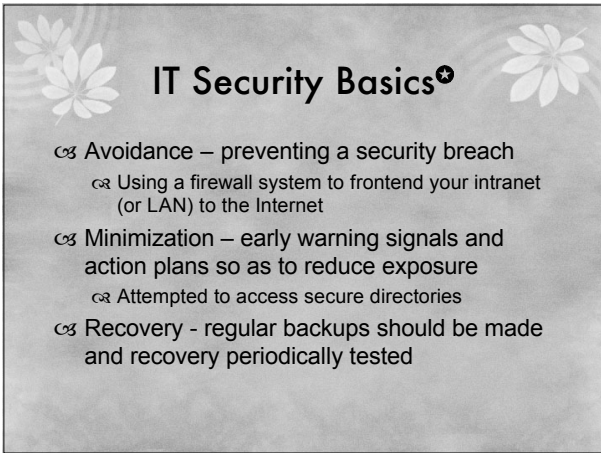
Important Concepts (2 of 2)★

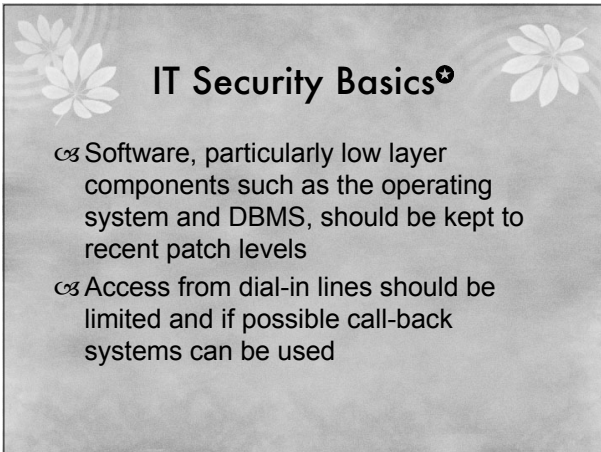
Message Integrity / Data Protection: sender and receiver want to ensure message not altered (in transit, or afterwards) at least **without detection**

Access and Availability: services must be available to users (through the system) and users must be able to use the system

Access Control / Authorization: only specific people (or agents) can use the system







IT Security Basics*

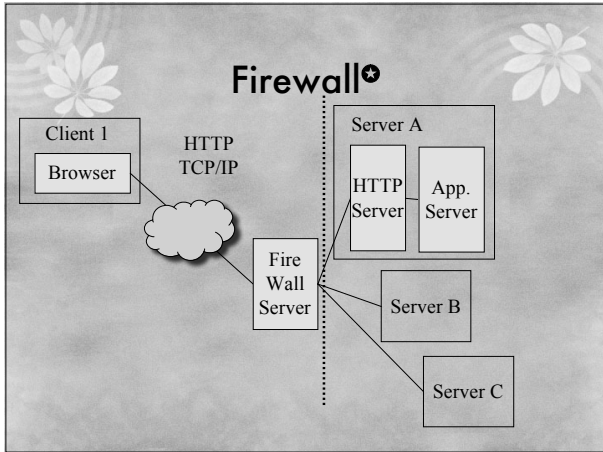
- ☞ Passwords (and potentially User Ids) should be forced to change periodically
- ☞ Passwords should be difficult to guess
 - ☞ Try to create passwords such as:
To Be or Not To Be ➔ 2b0n2b
- ☞ Databases should be secured in terms of access rights to data (usually by individual or group)

Physical Security*

- ☞ Large mainframe systems have always had adequate physical security
- ☞ The transition from LAN to WAN to Internet has caused new interest in these methods
- ☞ Physical security means locked doors and security personnel
- ☞ Options are to host on a secure ISP/ASP (InternetHosting.com)

Using a Firewall*

- ☞ A firewall server or router acts as an electronic security cop
- ☞ No machine other than firewall is directly accessible from Internet
- ☞ May also function as a "proxy" server allowing intranet systems to access only portions of the Internet
- ☞ Internet security methods are focused at the firewall reducing cost and admin overhead



Cryptography*

- ☞ Cryptography or ciphering is an ancient method of encoding a message — only a receiver with a key can decipher the content
- ☞ A single (symmetric) secret key is used to encrypt and decrypt
- ☞ Requires the communication of the key between sender and receiver!
- ☞ Basis of nuclear war-head command and control security

Public Key Cryptography*

- ☞ In 1976 Diffie & Hellman at Stanford U. developed *public-key cryptography*
- ☞ Asymmetric:
 - ☞ Private key – kept secret by owner
 - ☞ Public key – distributed freely to all who wish to send
 - ☞ Generated by computer algorithm, so a mathematical relation exists between them ... however ...
 - ☞ It is computationally difficult to determine the private key from the public key, even with knowledge of the encryption algorithm

Public Key Cryptography*

- ☞ The keys come in the form of tightly coupled pairs which anyone can generate using methods such as RSA, SHA-1, DSA (RSA is most common)
 - ☞ Javascript demo: <http://shop-is.sourceforge.net/crypto2.htm>
- ☞ There is only one public key corresponding to any one private key and vice versa
- ☞ Sender encodes data using public key of receiver
- ☞ Receiver decodes data using unique private key, no one else can do the same
- ☞ This ensures integrity of the data

Authentication*

- ☞ How can you be sure that the person sending the encrypted data is who they say they are
- ☞ This requires some method of authenticating the identity of the sender
- ☞ The solution is for the sender to “sign” the data using his/her private key – the data is encrypted using the sender’s private key
- ☞ The receiver validates (decrypts the data) the “signature” using the sender’s public key
- ☞ This will work as long as receiver can be sure the sender’s public key belongs to the sender and not an imposter ... enter PKI

Integrity and Authentication*

- ☞ Example: Consider a merchant wants to send a secure message to a customer:
 - ☞ Merchant encrypts message using customer’s public key
 - ☞ Merchant then signs message by encrypting with their private key
 - ☞ Customer decrypts using the merchants public key to prove authenticity of sender
 - ☞ Customer decrypts using their private key to ensure integrity of message

PKI – Public Key Infrastructure*

- œ Integrates PK cryptography with digital certificates and certificate authorities (CA)
- œ Digital certificate = issued by a CA, includes user name, public key, serial number, expiration date, signature of trusted CA (message encrypted by CA's private key)
- œ Receipt of a valid certificate is proof of identity – can be checked at CAs sight
- œ www.verisign.com is major player

Security and HTTPS*

- œ Certificate is an entity's public key plus other identification (name, CA signature)
- œ SSL – Secure Socket Layer
 - œ Lies between TCP/IP and HTTP and performs encryption
- œ HTTPS is the HTTP protocol that employs SSL – it uses a separate server port (default = 443)

Secure sockets layer (SSL)*

- œ transport layer security to any TCP-based app using SSL services.
- œ used between Web browsers, servers for e-commerce (shttp).
- œ security services:
 - œ server authentication
 - œ data encryption
 - œ client authentication (optional)
- œ server authentication:
 - œ SSL-enabled browser includes public keys for trusted CAs.
 - œ Browser requests server certificate, issued by trusted CA.
 - œ Browser uses CA's public key to extract server's public key from certificate.
- œ check your browser's security menu to see its trusted CAs.

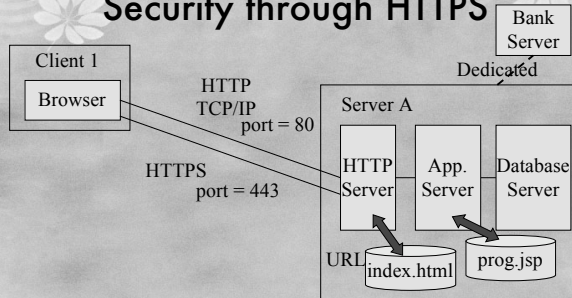
SSL (continued)★

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
 - All data sent into TCP socket (by client or server) encrypted with session key.

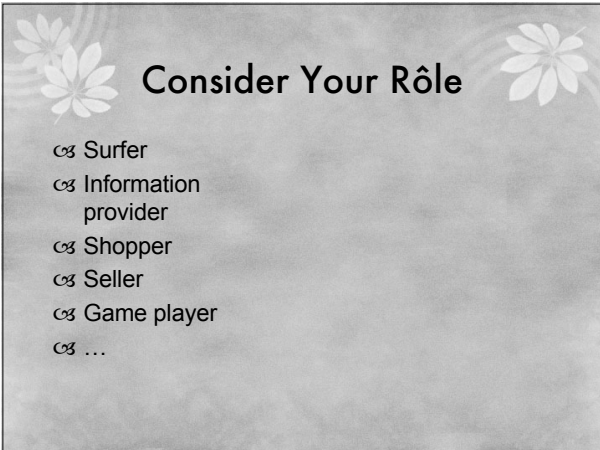
- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

Security through HTTPS



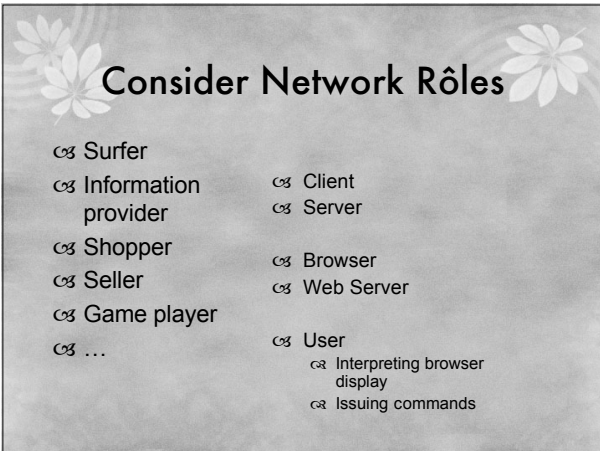
SSL – Secure Socket Layer

- Client makes HTTPS connection to server
- Server sends back SSL version and certificate
- Client checks if certificate from CA
- Client creates session "premaster secret", encrypts it and sends it to server and creates "master secret"
- Server uses its private key to decrypt "premaster secret" and create the same "master secret"
- The master secret is used by both to create session keys for encryption and decryption



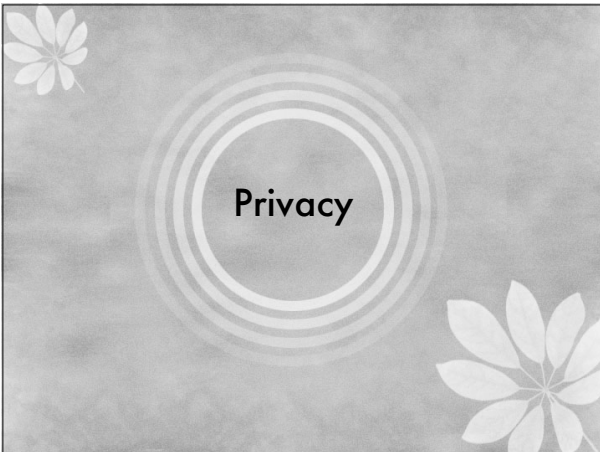
Consider Your Rôle

- ☞ Surfer
- ☞ Information provider
- ☞ Shopper
- ☞ Seller
- ☞ Game player
- ☞ ...



Consider Network Rôles

☞ Surfer	☞ Client
☞ Information provider	☞ Server
☞ Shopper	☞ Browser
☞ Seller	☞ Web Server
☞ Game player	☞ User
☞ ...	☞ Interpreting browser display
	☞ Issuing commands



Privacy

Some Definitions of Privacy

- ☞ Robert Ellis Smith, editor of the Privacy Journal, defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves." [6]
- ☞ According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity. [7]
- ☞ According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person. [8]

Source: Privacy International's PHR2004-Overview of Privacy (13/11/2004 version)

The Right To Privacy

Universal Declaration
of Human Rights (Article 12)

No one shall be subjected
to arbitrary interference
with his privacy,
Everyone has the right to
the protection of the law
against such interference
....

(10 Dec. 1948,
UN GA Res. 217 A (III))

Scott McNealy
(Sun's CEO)

'You have zero
privacy anyway.
Get over it.'

(25 Jan. 1999
at a press conference)

P3P*

- ☞ The Platform for Privacy Preferences Project
- ☞ W3C standard <<http://w3.org/P3P/>>

☞ Expected to enable simple, automated ways
for WWW users to gain more control over the
use of personal information

- ☞ A high-level data interchange language (like
PICS codes for filtering and Common Content
leases)
- ☞ Not a whole solution, only an infrastructure

* Source: W3C P3P Project webpage <<http://w3.org/P3P/>>, 10 March 2006

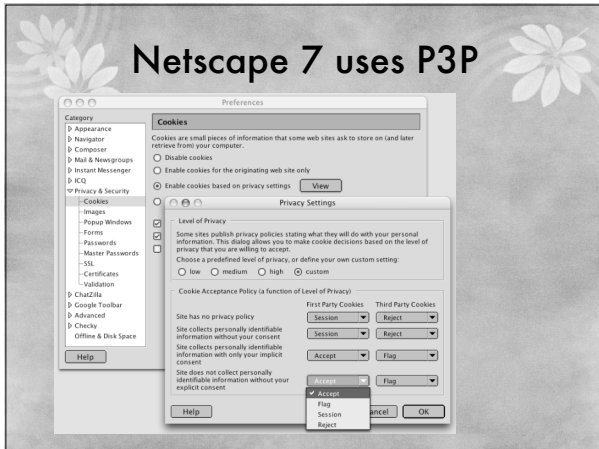
P3P: How*

☞ 'P3P-enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences.'

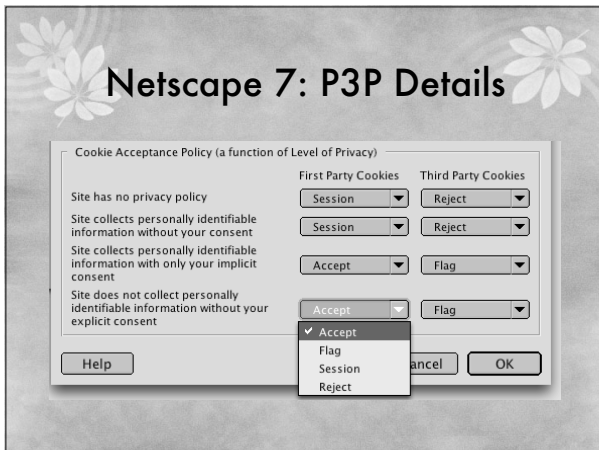
☞ 'P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.'

* Source: W3C P3P Project webpage <<http://w3.org/P3P/>>, 10 March 2006

Netscape 7 uses P3P



Netscape 7: P3P Details



Example P3P Policies

- ☞ <http://www.entraspan.com/p3p/display.html>
- ☞ <http://www.cs.dal.ca/~jamie/w3c/policy.html>

P3P Resources

- ☞ www.w3.org/P3P/
- ☞ See especially
 - ☞ How to create a policy
 - ☞ Entities
 - ☞ Expiry
 - ☞ Verification
 - ☞ How to implement a policy
 - ☞ Requires server administration
 - ☞ Use of keywords

Credits

◉ Some of these slides and diagrams are from Dr. Danny Silver of Acadia U.'s Jodrey School of Computer Science, and Dalhousie U.'s Faculty of Computer Science

* Some of these notes are based on slides provided with the textbook Computer Networking: A Top Down Approach Featuring the Internet (2nd edition).
 By Jim Kurose and Keith Ross (copyright held by the authors)
 Published by Addison-Wesley in July 2002.

From Privacy International's PHR2004-Overview of Privacy
 [6] Robert Ellis Smith, Ben Franklin's Web Site 6 (Sheridan Books 2000).

[7] Privacy as an Aspect of Human Dignity, 39 New York University Law Review 971 (1964).

[8] Privacy and the Limits of Law, 89 Yale Law Journal 421, 428 (1980).

<URL[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x34782589&als\[theme\]=Privacy%20and%20Human%20Rights&headline=PHR2004*_toc879395](http://www.privacyinternational.org/article.shtml?cmd[347]=x34782589&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004*_toc879395)>
