Security
The Tension

- Security vs. ease of use: the more security measures added, the more difficult a site is to use, and the slower it becomes

- Security vs. desire of individuals to act anonymously
IS INTERNET FRAUD REALLY A PROBLEM?

Credit Card Fraud Rate

Internet: 3%
Traditional: 0.1%

Internet fraud rate is 30 times higher
According to the 2008 Internet Crime Complaint Center (IC3)
Up 33% over 07
275,284 complaints

• Loss from 72,940 cases of fraud referred to federal, state and local law enforcement was $246.6 million
• Median dollar loss of $931 per complaint -- up from $239.1 million in total reported losses in 2007.
• The highest median dollar losses came from check fraud ($3,000), confidence fraud ($2,000), and Nigerian (West African 419) "advance fee" scams ($1,650).
2008 Top 10 IC3 Complaint Categories (Percent of Total Complaints Received)

- Non-delivery: 32.9%
- Auction Fraud: 25.5%
- Credit/Debit Card Fraud: 9.0%
- Confidence Fraud: 7.9%
- Computer Fraud: 6.2%
- Check Fraud: 5.4%
- Nigerian Letter Fraud: 2.8%
- Identity Theft: 2.5%
- Financial Institutions Fraud: 2.2%
- Threat: 1.9%
world relies on physical security -
Ecommerce world - reliance on electronic means to protect data, communications & transactions.

THREE TYPES OF SECURITY DIMENSIONS

1. Infrastructure security (hard/software)
2. Transactions security (web/moving)
3. Data/information security (message itself)
Do you see a Role for Laws and Public Policy

- New laws have granted local and national authorities new tools and mechanisms for identifying, tracing and prosecuting cybercriminals
  - National Infrastructure Protection Center – unit within National Cyber Security Division of Department of Homeland Security whose mission is to identify and combat threats against U.S. technology and telecommunications infrastructure
  - USA Patriot Act
  - Homeland Security Act

- Government policies and controls on encryption software
Name Some of the Most Common Security Threats in the E-commerce Environment

- Malicious code (viruses, worms, Trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- **Hacking** and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- **Sniffing**
- Insider attacks
- Poorly designed server and client software
- DoS and dDoS attacks
Malicious Code

- **Viruses**: Have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- **Worms**: Designed to spread from computer to computer
- **Trojan horse**: Appears to be benign, but then does something other than expected
- **Bots**: Can be covertly installed on computer; responds to external commands sent by the attacker
Unwanted Programs

- Installed without the user’s informed consent
  - **Browser parasites**: Can monitor and change settings of a user’s browser
  - **Adware**: Calls for unwanted pop-up ads
  - **Spyware**: Can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.
Phishing and Identity Theft

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter
  - One of fastest growing forms of e-commerce crime

- Many of you have gotten the “we are upgrading our server or the “I am the wife of Amad who ..”
Hacking and Cybervandalism

**Hacker:** Individual who intends to gain unauthorized access to computer systems

**Cracker:** Hacker with criminal intent (two terms often used interchangeably)

**Cybervandalism:** Intentionally disrupting, defacing or destroying a Web site

Types of hackers include:
- White hats
- Black hats
- Grey hats
Spoofing (Pharming) & Spam (Junk) Web Sites

- Spoofing (Pharming)
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Threatens integrity of site; authenticity

- Spam (Junk) Web sites
  - Use domain names similar to legitimate one, redirect traffic to spammer-redirection domains
Other Security Threats

- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network.
- Insider jobs: Single largest financial threat.
- Poorly designed server and client software: Increase in complexity of software programs has contributed to increase in vulnerabilities that hackers can exploit.
DoS and DDoS Attacks

- **Denial of service (DoS) attack**
  - Hackers flood Web site with useless traffic to inundate and overwhelm network

- **Distributed denial of service (DDoS) attack**
  - Hackers use numerous computers to attack target network from numerous launch points
Why did it prove to be so effective against Estonia?

What are botnets? Why are they used in DDoS attacks?

**ATTACK ON ESTONIA A MAY 9, 10 2007**

- **Denial of service (DoS) attack**
  - Hackers flood Web site with useless traffic to inundate and overwhelm network

- **Distributed denial of service (DDoS) attack**
  - Hackers use numerous computers to attack target network from numerous launch points
DESIGN A SYSTEM TO SEND A SECURE MESSAGE

- WHAT ARE YOUR INFRASTRUCTURE NEEDS?
- WHAT DOES THE SOFTWARE DO?
- WHAT TYPES OF SECURITY ARE THERE IN YOUR SYSTEM?
- HOW ARE COMPUTERS LINKED?
- HOW DO YOU KNOW WHO YOU ARE “TALKING” TO?
SECURITY NEEDS:

_authentication:

- A way to verify user’s identity before payments are made

_integrity:

- Ensuring that information will not be accidentally or maliciously altered or destroyed, usually during transmission
SECURITY NEEDS:

Encryption:
- making messages indecipherable except by those who have an authorized decryption key

Non-repudiation:
- Merchants protection - customer’s unjustifiable denial of placed orders
- Customers protection - against merchants’ unjustifiable denial of payments
Securing Channels of Communication

- **Secure Sockets Layer (SSL):** Most common form used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted) Part on customers’ PC – so no special software needed

- **Secure Electronic Transaction (SET):** More complicated comprehensive security protocol - provides privacy, authenticity, integrity, repudiation – must install “Digital Wallet”

- **S-HTTP:** Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP

- **Virtual Private Networks (VPNs):** Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocols
SECURE SOCKET LAYER - SSL

AUTOMATICALLY ENCRYPTS TCP/IP

WEB, EMAIL ETC - SERVER SECURITY HIGHEST LEVEL
URL IS HTTPS COMMUNICATIONS ARE ENCRYPTED

Variety of encryption algorithms and authentication methods. While SSL can encrypt credit cards from consumer to merchant more needed for security
Cyber criminals (full length)

Bank hacking

Hacker caught
WHAT ARE THE 2 TYPES

1. PRIVATE/SECRET KEY
   Some believe penetrable. Maybe secure “enough”

2. PUBLIC KEY
   Most popular algorithm is RSA (Rivest, Shamir and Adelman) Various key sizes (e.g. 1,024 bits)
   Most secure - Never known to be broken (to date)
**Symmetric Key Encryption**

Private / Secret Key

- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- **Advanced Encryption Standard (AES):** Most widely used symmetric key encryption today; offers 128-, 192-, and 256-bit encryption keys; other standards use keys with up to 2,048 bits
Private Key
Private/Secret Key Cryptography (symmetric)

64 bit key Data Encryption Standard DES Most widely accepted algorithm

SET uses DES

Key_{sender} = Key_{receiver}

Public key sent

Original Message

Sender

Scrambled Message

Encryption

Internet

Scrambled Message

Receiver

Message received

Decryption

public key

Key_{receiver}
Public Key Encryption

- Solves symmetric key encryption problem of having to exchange secret key
- Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
- Both keys used to encrypt and decrypt message
- Once key used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient’s public key to encrypt message; recipient uses his/her private key to decrypt it
1. Public Key Cryptography

two stages of decryption

Public Key_{receiver} delivered in advance

Code has info about private key to “open”

Message

Original Message

Scrambled Message

Sender

Internet

Public key

Private Key_{receiver}

Original Message

Receiver

Public Key Message decrypted with R’s private key

Decryption

1^{st} private key

2^{nd} public key

Public key used to transmit secret key of DES algorithm because faster/efficient in handling encryption/decryption
Public Key Encryption using Digital Signatures and Hash Digests

- Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data
- Double encryption with sender’s private key (digital signature) helps ensure authenticity and nonrepudiation
Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)

- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
1. DIGITAL SIGNATURE

two stages of decryption

1. Public Key_{\text{sender}} - delivered in advance to receiver

2. ENCRYPTED S private KEY - public key to “open”

Digital “SIGNATURE” ATTACHED >

Decryption

1\text{st} private key

2\text{nd} public key
Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
Certificate Security Schemes

- Identifying the holder of a public key (Key-Exchange)
- Issued by a trusted certificate authority (CA)

Name: "Dr. Kip"
key-Exchange Key:
Signature Key:
Serial #: 29483756
Other Data: 10236283025273
Class of certificate
Dates valid
Issuing authority digital signature
Expires: 6/18/03
Signed: KB’s Signature
“CHECK IT OUT”

**VERISIGN**
- Only CA open to public
- 3 levels of certificates

**COMMERCIAL CAs**
- Cylink
- GTE
- BBN
- NETSCAPE

* In the case of credit cards authorities CCAs
GCA Geopolitical Certificate Authority (verisign) certify Card CAs

**W3 FOR**
**FAQs ON INTERNET SECURITY**

http://www.w3.org/Security/Faq/www-security-faq.html
Digital Certificates & Certifying Authorities

Digital Certificates
- 3RD Party-Verify holder of a public & private key is who they claim to be

Certifying Authorities (CAs)
- Maintain responsibility for checking user's identity
- Verifying validity of digital certificates
- Issue digital certificates
- Verify the information creates a certificate that contains the applicant's public key along with identifying information
- Uses their private key to encrypt certificate and sends the signed certificate to applicant
Certificate Information

This certificate is intended to:

• Guarantee the identity of a remote computer

Issued to: www.subway.com

Issued by: Secure Server Certification Authority

Valid from 12/20/98 to 1/8/00
How an Online Credit Transaction Works

Figure 5.18, Page 308

1. Consumer makes purchase
2. SSL provides secure connection through Internet to merchant server
3. Merchant software contacts clearinghouse
4. Clearinghouse verifies account and balance with issuing bank
5. Issuing bank credits merchant account
6. Monthly statement issued with debit for purchase
BREAK !!!
Public key