Security

Encryption encodes information to hide it from everyone else … maintaining your privacy

Security Basics

Security Worries --
- Reading info as it's being transmitted
- Mischief on computer: erasing files, etc.
- Gather key info to impersonate you
- Others have your info, they can misuse it or "provide it" to unqualified persons

Security is a serious problem, and only you can prevent the loss of your info

What Can Happen?

Viruses & worms are common ways for malicious software to enter computer
- Virus--malicious SW riding in on other SW
- Worm--SW purposely transmitting itself

Worms usually travel by attachments to email: .exe, .zip, .dmg, …
- Open attachments only if you know the sender and trust him/her

Phishing

Stealing your information is easiest if people give it up voluntarily
- Goal: SSN, Bank Acct. #, Security Info for purposes of identity theft
- Technique: Send SPAM that looks like legit mail from bank, credit union, govt. … claiming it must verify your information
- The whole thing is a spoof trying to get you to give up private information

Spyware

Spyware is software designed to set up shop on your computer to steal information or computer services
- Spyware most often rides along with downloads; be wary of
  - Music and video downloads
  - Software downloads

Major Protection

You must run virus protection software to keep your computer safe
- It's easy to install and worth the $$
- Keep it current
- Don't open attachments
- Other concerns
  - Disable 3rd party cookies
  - Don't answer phishing scams
  - Get music & SW from reputable source
Maintaining Privacy

To keep information private it must be hidden from “prying” computers. As children, most of us used “secret” codes. Most often the code was a Caesar Cipher – an alphabetic shift by a constant amount.

<table>
<thead>
<tr>
<th>Clear Text</th>
<th>Encode</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
<td>IJKLMNOPQRSTUVWXYZ</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
</tr>
</tbody>
</table>

Coded Text: LW VWB AXG WV CAI

Breaking Caesar Cipher

Fixed substitutions don’t work, ’cause letters have a known distribution.

- In a large text, count the frequency of each letter, match the results to distribution.
- The twelve most frequent letters account for 80% of English text.
- ETAOINSHRDLU

Encryption Issue

Traditionally, encryption technology has been "breakable" with effort.

- Breakable codes let law enforcement and governments watch criminals and spies.
- Codes are good enough for the honest.

New computer encryption is unbreakable:

- It’s called “strong encryption” ... should it be legal to be able to keep secrets absolutely?

Strong encryption: serious issue of public interest

Encryption Issue

Traditionally, encryption technology has been "breakable" with effort.

- Breakable codes let law enforcement and governments watch criminals and spies.
- Codes are good enough for the honest.

⇒ New computer encryption is unbreakable.

Encryption Setup: Key Exchange

To communicate securely, users must meet before sending/receiving.

**General Encryption Setup**

Encryption is most important for when sending information.

\[ K_w \text{ } \rightarrow \text{ } \text{Sender} \rightarrow E_{K_w}(T) \rightarrow \text{Receiver} \leftarrow D_{K_w}(E_{K_w}(T)) = T \]

**Problem: Key Exchange**

To communicate securely, users must meet before sending/receiving.

\[ K_w \text{ } \rightarrow \text{ } \text{Sender} \rightarrow E_{K_w}(T) \rightarrow \text{Receiver} \leftarrow D_{K_w}(E_{K_w}(T)) = T \]

This doesn’t work for eCommerce.
Revise Encryption Setup

Public Key Encryption is based on publishing the key

\[ \text{Sender uses public key to encrypt } K_{sr} \]

\[ \begin{array}{c|c|c}
\text{Sender} & \text{Cipher Text } E_{r}(T) & \text{Receiver} \\
\text{Encrypt w/ } K_{r} & & \text{Decrypt w/ } K_{r} \\
\text{Clear Text } T & & \text{Clear Text } T = D_{r}(E_{r}(T))
\end{array} \]

RSA Encryption

Rivest, Adelman and Shamir invented a PKC scheme called RSA

- The secret is to pick the key, \( K_{sr} \), right
- Pick two prime numbers — numbers divisible only by themselves and 1 — that are 2 greater than a multiple of 3… weird!
- Examples are 5, 11, 17, 23, 29, ...
- \( K_{r} = p \cdot q \) so that it is 129 digits

What Makes RSA Work?

Though the numbers get huge, computer can handle them quickly

- These codes are strong because breaking them needs \( s \), which needs \( p \cdot q \), which means factoring \( K_{r} \)
- Factoring is computationally tough — best methods are only somewhat better than grammar school, “try all small primes”
- Picking 129 digit key, means no computer can factor it … so the code is unbreakable

RSA Challenge

After inventing their scheme (1977), RSA challenged people to break it

- Their first key was broken in 1994 using 1000 computers over 8 months
- Their secret message: THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Doomed? No. There are many other 129 digit keys, or if people get nervous make 200 digit keys or more … breaking gets harder very fast; encrypt/decrypt doesn’t

Is Strong Encryption Smart

Should we allow people to use strong encryption? Or should only breakable codes be legal?

- It hampers law enforcement and security
- Most criminals reveal plans in other ways
- PKC exists and is known, so build in escape — Trap door — Key Escrow
- But are these schemes really secure?