Networking security: where are the vulnerabilities?

Recall our prior discussion… asusme you have a router and thus a private IP address.

Network connections with encryption

Turn on router’s encryption feature to encrypt the wireless signal.

Eaves-dropping difficult on this wireless link after enabling encryption (e.g., WPA)

Better: encryption now activated in your friend’s router

Even though both you and your BFF are using encryption at your “ends,” this is not “end-to-end” encryption. End to end encryption refers to keeping the data encrypted while it travels over the internet. The standard Internet TCP/IP network protocols do not encrypt packet data. But, some applications send data in encrypted form, and there are options (e.g., VPN) for creating end-to-end encryption.
“End-to-end Encryption” via VPN

VPN client software

The University of Oregon VPN gateway.

VPN benefit: your PC gets a second IP address, this one assigned by the VPN server; makes it appear to UofO servers that your PC is on the UofO network.

What is “encryption”?

- Simply put, encryption is a scheme for scrambling data to make it difficult to decipher

Two encryption approaches

- **The shared key** approach
  - Already discussed, the most “obvious” case
  - Like having a shared key to a padlock

- **The public key** approach
  - Not obvious! Give everyone the key to your lock?
  - We will see how this work in a few minutes.

Shared Key example: the “Caesar” cipher

*Key value: 3*

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Cyphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>TREATY</td>
<td>IMPOSSIBLE</td>
</tr>
<tr>
<td>UHNDDB</td>
<td>LUPYPVHSD</td>
</tr>
</tbody>
</table>

Prior scenario was “shared key” (password)

- Wireless hub encryption standards (such as WPA or WPA2) use the shared-key approach
  - You define a password (the key) within the wireless hub.
  - The same password (key) must be configured in your computer’s networking software

Shared key encryption also use when communicating with web servers

Jane Smith’s CCN is 4408 3380 7002 2652

How is the shared key established?

By your computer initially sending password information using the server’s “public key”

Public/private key encryption

- Two mathematically-related, yet separate keys
  - The formula linking public and private key is sufficiently complicated that knowing one # doesn’t let you figure out the other
  - In other words, the formula connecting the two is more complex than: public value + private value = 100
  - The couple guys who came up with the formula have earned 100’s of million of $ using it to secure data for customers
  - They also published the formula for everyone to see

- Your Private Key: you keep this # secret!
- Your Public Key: you publicly disclose this #
- Information encrypted by public key can only be decrypted by its own private key, and vice versa.
Public/private Key Encryption

Anyone can encrypt using the public key, but only the holder of the private key can decrypt. Security depends on the secrecy of the private key.

Using a private key as a “digital signature”

Alice scrambles her message with her private key. If you can unscramble the message with Alice’s public key, then you know the message wasn’t tampered with since being scrambled by the holder of Alice’s public key.

But, how do you know that person is really Alice?

Digital sig. proves message has not been tampered with, but to deal with the impersonation issue industry created “Certificate Authorities” (next slide)

Obtaining a public/private key pair for your company?

- You pay a “Certificate Authority” (CA) to generate and issue a key pair
- Verisign (a big CA) or its competitors
- Generally you enter into a 2 year service agreement
- For the next 2 years, Verisign’s server sends all your site visitors a “Verisign digital certificate” that provides your firm’s name and public key for encrypted dialog with your webserver
- Browser (e.g., Firefox, IE) can show user that certificate information which show
- User can feel safe to the extent they trust in Verisign and public/private key encryption

Summary: 3 diff. security purposes

- Eavesdropping (Confidentiality)
- Tampering (Integrity)
- Impersonation (Authentication)

Agenda

- Security
- Encrypted networking
- Types of encryption
- Shared key
- Public key
- Information privacy discussion

Some Modern Threats to Info. Privacy

- Electronic Surveillance
- Hacker attacks (later)
  - Phishing email
  - Look at these two sites:
    - http://www.sonicwall.com/file/phishing
  - Viruses
  - SpyWare (“alien ware”)
    - e.g., keyloggers
- Public records
  - Fundrace example
A Carnegie Mellon study showed that it doesn’t take much to find someone with a minimum of data. Simply by knowing gender, birth date, and postal zip code, 87 percent of people in the United States could be pinpointed by name.

Companies have four standard approaches for tracking data about us:
1. Accepting what we knowingly provide
2. Logging our “clickstream” data
3. Using cookies to store our session data on their site
   - Site can thus “remembers us” when we return later (as per our online advertising discussion)
4. Buying data from data aggregators.

Data Aggregators: big business
- Acxiom, a $1.3 billion a year business
  - The firm holds data profiling some two hundred million Americans.
  - Combines public source data on real estate, criminal records, and census reports, with private information from credit card applications, warranty card surveys, and magazine subscriptions.
- ChoicePoint
  - Accidentally in 2005 sold financial records on 145,000 people to a cybercrime identity theft ring.
  - Fined $15M ($0.015B) dollars from the Federal Trade Commission
  - In February, 2008, Reed Elsevier acquired ChoicePoint for $4.1 billion.
Be careful about how your company handles privacy

- For companies and government organizations, policies are evolving and becoming stricter.
- HIPAA (the U.S. Health Insurance Portability and Accountability Act) governs data use and privacy among healthcare providers, insurers, and employers.
- The European Privacy Directive governs data use for firms’ operating in the EU.

Corporate “Code of Ethics”

- Example: how your firm will treat customer information (“privacy code”)
  - Opt-out Model
  - Opt-In Model (friendlier)

- Code of Ethics
  - Should be documented/enforced

Security is a management issue

- In a fairly recent Computer Crime and Security Survey...
  - 90% of large companies and government agencies reported computer security breach
  - 80% reported sizeable financial loss
- Many companies, in addition to the Chief Information Officer (CIO), now have a Chief Information Security Officer (CISO).

Conclusions

- Networking and encryption technologies exist (e.g. encryption) to help protect you
- Suspicion can protect you from many common threats
  - Both high tech (e.g., phishing) and low
- Continue to learn about security threats over time

Conclusions

- Managers need to identify new business opportunities
- Example: car insurance
  - SafeCo’s “teensurance”
  - Progressive’s Snap Shot
- How far should businesses take these trends?
  - Pizza delivery scenario
  - “Picture mining”… Microsoft Sea Dragon