CS155b: E-Commerce

Lecture 8: February 1, 2001

TPSs and Content-Distribution Businesses
Security Technologies

- Encryption
  - Symmetric Key
  - Public Key
- Signature
- PKI
- Rights Management
- Time stamping
- Secure Containers
Product- or Service-Developer’s Goal

- Choose the right ingredients and weave them together into an effective end-to-end technical protection system (TPS).
- Ingredients must be “right” w.r.t. business model and legal and social content as well as technical context.

Notoriously Difficult! (Shapiro and Varian may be too optimistic.)
General Points about TPSs

• TPS is a means, not an end. Cannot answer legal, social, or economic questions about ownership of or rights over digital documents.
• No TPS is perfect.
• Continued improvement in TPS requires ongoing R&D, including “circumvention.”
• TPS easier to design for special purpose devices and systems (e.g., cable television) than for the Internet.
• TPS should serve customers’ needs, e.g., assured provenance, as well as rightsholders’ needs.
Common Elements of Many TPSs

- Mass-Market broadcast content
  - Anyone can get ciphertext, which is broadcast on low-cost channel (e.g., web page, broadcast TV).
  - Encrypted once.
- Decryption key \( k \) sent only to paying customers on lower-bandwidth, higher-cost channel.
Possible Realization for Web Pages

- Customer U and content-server use basic security protocol, e.g., SSL, to create “session key” $K_U$ and transfer payment from U to server.
- Server sends $k' = E(k, K_U)$ to U.
- U’s browser computes $k = D(k', K_U)$, downloads encrypted content, decrypts it using k, and displays it.
Possible Shortcomings

• Why can’t U print, save, or otherwise redirect displayed content?

• Why can’t a hacker steal k while it’s in use?

• Interaction of browser with other local-network software, e.g., back-up system?
Crypto. Theory Myth: Private Environments

KDC

Key Generation

Alice

Bob

Alice

Y ← E(X, K_{AB})

Bob

X ← D(Y, K_{AB})
Modern Computing Reality

Alice

Admin

$A_i$

$A_i$

Bob

Admin

$B_1$

$B_k$

Eve

Alice
Real Sources of Compromise

- Unwatched Terminals
- Administrative Staff Changes
- Misconfigurations
- OS Bugs
- Bad Random-Number Generators

Not sophisticated break-ins!
Secure Socket Layer (SSL)

- SSL was first developed by Netscape Corp. in 1994 and became an Internet Standard in 1997 (version 3.x).
- SSL is a cryptographic protocol to secure two applications communicating across a “socket” (cf. TCP).
- Data transmitted through an SSL connection is encrypted.
- It is mostly used by WWW applications (web servers and browsers). The string https:// in an URL specifies the browser to open a secured socket connection to the server (port 443).
- SSL uses digital certificates for authentication. There is no “trust hierarchy” in SSL, so browsers are preloaded with certificates of trusted CAs.
- Due to U.S. export regulations, products using SSL sold in foreign markets use weakened cryptography (40-bit key vs. 128-bit key).
SSL In Online Retailing

- Most Internet retail sites use SSL to secure online payments.
- Online merchants purchase digital certificates from CAs (e.g., Verisign) to authenticate itself to the browser software.
- SSL is NOT an electronic payment protocol. It is used to safely transmit sensitive financial information (e.g., credit card number, personal address, etc.)
- It means online merchants using SSL (e.g., Amazon.com) do not process the credit cards in real-time. A traditional mail order/telephone order (MOTO) protocol is used after for payment processing later,
- SSL provides security in authentication and communication. It does not address other security issues: it is up to the individual to trust a name linked to a certificate, and in its ability to protect and not misuse its database.
The SSL Handshake

Client hello

Server hello
  Present Server Certificate
  *Request Client Certificate
  Server Key Exchange

Client Finish
  *Present Client Certificate
  Client Key Exchange
  *Certificate Verify
  Change Cipher Spec

Server Finish
  Change Cipher Spec

Application Data

* Optional messages
Possible Realization for Pay-TV

- \( K_{ui} \) is entered in \( i^{th} \) “set-top box” when box is installed.

- \( E(k, K_{u1}), \ldots, E(k, K_{uN}) \) are broadcast with encrypted program.

Shortcoming: *One* broken box can be used to steal *all* future programs.
Watermarking

Note similarity with and difference from digital signature scheme.

Open Problem: Public-key watermarking.
Uses of Watermarking in TPS

- Broadcast of marked object, controlled distribution of keys. (Same architecture as in broadcast of encrypted content . . . and same shortcomings.)
- Web crawlers can search for unauthorized copies of marked objects.
- Unauthorized modification of marked objects can be detected by “fragile watermarking schemes.”
- Special-purpose devices can refuse to copy marked objects.
Superdistribution

Content is packaged with “terms and conditions” that are checked by a “rights-management system” and can be augmented by value-adding middlemen.
TPS Design Principles

- Know the $$ value of content
- Following rules: Convenient
- Breaking rules: Inconvenient
- Breaking rules: Conscious
- Renewable/Improvable Security
- Don’t let Pirates use your distribution channel
- Provide value that pirates don’t
Known Risks
→
TPS
→
Copyright Law
→
Residual Risks

Unknown Risks
INTERTRUST

- Full Name: Intertrust Technologies Corporation
- Employees: 190 (end of 1999)
- Stock Price: $4.56 (Jan 29, 2001)
- Revenues in 1999: $1,541,000
- Business Area: Digital Right Management (DRM)
MAIN PRODUCTS

• Commerce DRM Platform: Can be used to create applications to securely manage, sell, and fulfill digital information.

• Commerce Applications: Partners of the applications built on top of the commerce platform

• Integrated System for DRM: Chips
BRIEF HISTORY

- 1990  Founded
- 1997  Annual Revenue More than $1M
- Q4, 1999  Listed as a Publicly Traded Company
- Feb, 2000  Historic Peak of Stock Price ($97)
- Jan, 2001  Virgin Records, Zomba Music, Daft Life and, Intertrust Announce Strategic Alliance
NET INCOME CHART

Net Income

Quarter

Q1 99, Q2 00, Q3 00, Q4 00, Q1 01, Q2 01, Q3 01