CS155b: E-Commerce

Lecture 6: Jan. 25, 2001

Security and Privacy, Continued
FIREWALL

- A barrier between an internal network & “the Internet”
- Protects the internal network from outside attacks
- Executes administrator-defined security policy
- Decides whether a datastream is allowed to pass through or not
- Main Components:
  - packet filter
  - proxy
Interconnection of Networks

- Recursively build larger networks
PACKET FILTER

- Works at IP layer
- Rule-table-driven
- Forwards, refuses, or drops a packet according to the rules
- An example rule table

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>…</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128.<em>.</em>.*</td>
<td>130.<em>.</em>.*</td>
<td>Any</td>
<td></td>
<td>Fwd</td>
</tr>
<tr>
<td>2</td>
<td>61.<em>.</em>.*</td>
<td>130.<em>.</em>.*</td>
<td>23</td>
<td></td>
<td>Refuse</td>
</tr>
<tr>
<td>3</td>
<td>61.<em>.</em>.*</td>
<td>Any</td>
<td>21</td>
<td></td>
<td>Drop</td>
</tr>
</tbody>
</table>
PROXY

- Works at application layer
- One proxy per (application layer) protocol
  - HTTP proxy, FTP proxy, …
- User authentication required
- Different users can have different privileges
- Can be made transparent to users
SEVERAL CONFIGURATIONS POSSIBLE

• A Sample Configuration: Dual-home Host

• Trade-offs: Security vs. Accessability, Security vs. Cost
CHECKPOINT

- Full Name: Check Point™ Software Technologies Limited
- Employees: 1000 +
- Stock Price: $146.5 (Jan 22, 2001)
- Revenues in 2000: $425.3 million
- Business Area: Internet Security
MAIN PRODUCTS

- **FireWall-1®**: a popular firewall product
- **Open Platform For Security (OPSEC)**: an enterprise-wide framework for security policies extending FireWall-1®
- **VPN-1**: a family of virtual private networking solutions
- **Provider-1™**: a security management solution
BRIEF HISTORY

- 1993  Founded
- June 1996  Initial Public Offering
- 1998  Annual Revenues More than $100M
- June 2000  Stock Price More than $100
- Q3, 2000  Quarterly Revenues More than $100M
Discussion Point

- Firewalls aren’t perfect
  E.g., “Address spoofing” is a problem

- Why is CheckPoint so successful? Importance of “feeling secure”? “Knee-high protection?”
Symmetric Key Crypto

\[ D(E(x, k), k) = x \]

(decryption, encryption, plaintext, key)

- Alice and Bob choose \( k_{AB} \)
- Alice: \( y < -- E(x, k_{AB}) \) (ciphertext)
- Alice --> Bob: \( y \)
- Bob: \( x < -- D(y, k_{AB}) \) (Eve does not know \( k_{AB} \))
Well Studied and Commercially Available

- DES
- IDEA
- FEAL-n
- RC5
- AES

• Users must deal with
  - Government (especially export)
  - Key management
Public Key Crypto

\[ D(\text{E}(x, PK_u), SK_u) = x \]

(user’s Secret Key, user’s public key)

Bob generates \( SK_{bob}, PK_{bob} \)

Bob publishes \( PK_{bob} \)

Alice: Lookup \( PK_{bob} \)

\[ y \leftarrow \text{E}(x, PK_{bob}) \]

Alice --> Bob: \( y \)

Bob: \( x \leftarrow \text{D}(y, SK_{bob}) \)

(Eve does not know \( SK_{bob} \))
Digital Signatures

Doc1
-JF

... Doc2
-JF

-Docn
-JF

Trickier than the paper “analogue”
3-part Scheme

Key Generation Procedure

\[ \text{directory} \]

\[ \text{JF’s machine} \]

PK_{jf} \quad SK_{jf}
Verification Procedure

- Doc
- $PK_{jf}$
- SIG

Accept / Reject
Examples

- RSA
- El Gamal
- DSA
- McEliece
$\text{http://www.bob-soft.com}$

$$P(\ ) \{ \ldots \}$$

$$\text{SP} = \text{signature}(P, SK_{bob})$$
Bob-soft: $PK_{bob}$
Sue-soft: $PK_{sue}$

Alice: Verify $(P, PK_{bob}, SP)$
New Potential Problem

- Is $\text{PK}_{\text{bob}}$ the “Right Key”?

- What does “Right” mean?
Traditional Meaning

Bob-soft $\leftrightarrow$ PK$_{bob}$

Accurate?

Traditional Solution

Alice's Computer $\rightarrow$ PK$_{CA}$
Bootstrapping Trust

\[(\text{Bob-soft, } \text{PK}_{\text{bob}})\]

\[\text{Signature Algorithm}\]

\[\text{CERT}_{\text{bob}}\]

\[\text{Name}_1, \text{PK}_1, \text{CERT}_1\]
\[\text{Name}_2, \text{PK}_2, \text{CERT}_2\]
\[\vdots\]
\[\vdots\]
\[\vdots\]
• **Technical Question**: Is this the right PK?

• **Business Question**: Can you make money selling public-key certificates?

• **Political Question**: Crypto export

• **Legal Question**: Do we have a right to use encryption? To some form of “electronic privacy”?
VeriSign:
Enable everyone, everywhere to use the Internet with confidence

- Through its acquisition of Network Solutions, VeriSign serves as the gateway to establishing an online identity and Web presence, with more than 24 million domain name registrations in .com, .net and .org.
- As the leader in the Web site security market, VeriSign provides Internet authentication, validation and payment services.
- Through VeriSign Global Registry Services, VeriSign maintains the definitive directory of over 24 million Web addresses and is responsible for the infrastructure that propagates this information throughout the Internet. VeriSign Global Registry Services responds to over 1.5 billion DNS look-ups daily.
History

- VeriSign opened HQ in Mountain View: April 1995
- IPO: January 1998
- Acquired Network Solutions: June 9, 2000
- Currently: 2000+ employees
Product Line

- **Web Site Trust Services**
  Authenticate your site to customers and protect Internet transactions with SSL encryption.

- **Payment Processing**
  Securely accept, process, and manage credit card and other payment types for B2B, B2C, and person-to-person purchases on your site.

- **Code Signing**
  Digitally sign software and macros for safe online downloading to your customers.

- **Secure E-Mail**
  Digitally sign and encrypt your e-mail to safeguard it from intrusion and alteration online.

- **Web Identity**
  Register for and manage Web addresses (domain names).
• **Web Authoring**
  Build a professional-looking Web site and then enhance and promote it with business features

• **Enterprise Trust Services**
  Protect your intranet, extranet, e-mail systems, and Virtual Private Networks as well as B2B transactions with PKI and Internet infrastructure solutions.

• **Network Security**
  Protect information with firewalls, VPNs, network appliances, consulting resources, and security management.

• **Global Registry Services**
  Domain name registrars: take advantage of registry services and Domain Name System (DNS) support.

• **Wireless Trust Services**
  Carriers, service providers, manufacturers, and developers: enable a secure wireless commerce environment through an array of standards, devices, and applications.
“Internet Identity” ↔ “Real-World Identity”

- Expertise? Liability?

- Suppose you are “Purely” Internet Business? (Recall bob-soft.com)

- Authorization vs. Authentication

- Importance of “Feeling secure”