ECE 297:11 - Lecture 1

Security Services

Basic Concepts of Cryptology

Need for information security

• widespread use of data processing equipment: 
  computer security

• widespread use of computer networks and distributed computing systems:
  network security

Security Threats and Security Services
Security Threats in Banking Systems

Bank A
- interception
- modification
- unauthorized access

Bank B
- fabrication
- Timing attacks
- Radiation analysis

Network Security Threats (1)

Interruption
- Interruption
- Modification
- Fabrication

Network Security Threats (2)

Passive
- Interception
  - Release of message contents
  - Traffic analysis

Active
- Interruption (availability)
- Fabrication (authenticity)
- Modification (integrity)
Security services
Protecting data

in transit
• confidentiality
• integrity
• authentication
• non-repudiation

at rest
• access control
  - identification
  - authorization
  - auditing
• availability

Identification
(User Authentication)

On the basis of
• what you know (passwords, PINs)
• what you have (magnetic card, smart card)
• what you are (fingerprints, handprints, voiceprints, keystroke timing, signatures, retinal scanners)

Basic Security Services (1)

1. Confidentiality
   Bob Alice
   Charlie

2. Message integrity
   Bob Alice
   Charlie

3. Message authentication
   Bob Alice
   Charlie
Basic Security Services (2)

4. Non-repudiation
   - of sender  - of receiver   - mutual

Technique: *digital signature*

```
<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGITAL</td>
</tr>
<tr>
<td>A6E3891F2939E38C745B</td>
</tr>
<tr>
<td>25288960CA2458EF5349</td>
</tr>
<tr>
<td>245CBA653448E349EA47</td>
</tr>
</tbody>
</table>

Main Goals:
• unique identification
• proof of agreement to the contents of the document
```

Handwritten and digital signatures

*Common Features*

<table>
<thead>
<tr>
<th>Handwritten signature</th>
<th>Digital signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unique</td>
<td></td>
</tr>
<tr>
<td>2. Impossible to be forged</td>
<td></td>
</tr>
<tr>
<td>3. Impossible to be denied by the author</td>
<td></td>
</tr>
<tr>
<td>4. Easy to verify by an independent judge</td>
<td></td>
</tr>
<tr>
<td>5. Easy to generate</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Handwritten signature</th>
<th>Digital signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Associated physically with the document</td>
<td>6. Can be stored and transmitted independently of the document</td>
</tr>
<tr>
<td>7. Almost identical for all documents</td>
<td>7. Function of the document</td>
</tr>
<tr>
<td>8. Usually at the last page</td>
<td>8. Covers the entire document</td>
</tr>
</tbody>
</table>
Relations among security services

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Basic Concepts of Cryptology

Cryptology

- Cryptography
- Cryptanalysis

from Greek:
- cryptos - hidden, secret
- logos - word
- graphos - writing
Basic Vocabulary

encryption (encipherment)
message (plaintext, clear message)
\[ M \rightarrow C \]

decryption (decipherment)
message (plaintext, clear message)
\[ M \rightarrow C \]

cryptographic key
\[ K \]

M bits

N bits

cryptographic key

Message

Cryptosystem (Cipher)

message

N bits

cryptographic key

K bits

M bits

ciphertext

Definition of a cryptosystem (cipher)

\[ \forall K \in K \; \forall M \in M \; D_K(E_K(M)) = M \]
**Substitution Cipher**

Key = \[
\begin{array}{cccccccccccccc}
abcdefghijklmnopqrstuvwxyz
f q i s h n c v j t y a u w d r x l b m z o g k p
\end{array}
\]

**enciphering**

TO BE OR NOT TO BE

```
\| \| \| \| \| \|
BD QH DX WDB BD QH
```

**deciphering**

```
\| \| \| \| \| \|
TO BE OR NOT TO BE
```

Number of keys = 26! ≈ 4 ⋅ 10^{26}

---

**Kerckhoff’s principle**

The security of a cipher MUST NOT depend on anything that cannot be easily changed

A. Kerckhoff, 1883

---

**Unpublished vs. published algorithm?**

<table>
<thead>
<tr>
<th>Unpublished algorithm</th>
<th>Published algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Cryptanalysis must include recovering the algorithm</td>
<td>1. The only reliable way of assessing cipher security</td>
</tr>
<tr>
<td>2. Smaller number of users, smaller motivation to break</td>
<td>2. Prevents backdoors hidden by designers</td>
</tr>
<tr>
<td>3. Unavailable for other countries</td>
<td>3. Large number of implementations = low cost + high performance</td>
</tr>
<tr>
<td></td>
<td>4. No need for anti-reverse-engineering protection</td>
</tr>
<tr>
<td></td>
<td>5. Software implementations</td>
</tr>
<tr>
<td></td>
<td>6. Domestic and international standardization</td>
</tr>
</tbody>
</table>
**Fundamental Tenet of Cryptography**

If lots of smart people have failed to solve a problem, then it probably will not be solved anytime soon.

---

**Security of unpublished ciphers**

Commercial packages cracking unpublished encryption schemes built-in:

- MS Word, MS Excel, MS Money
- Word-Perfect, ProWrite, Data Perfect
- Lotus 1-2-3, Symphony, Quattro-Pro
- Paradox, Semantec’s Q&A
- PKZip

Time: 1-2 minutes  
Price: ~ $200  
Companies: Access Data  
Crak Software

*Passwords recovered even for empty files!*

---

**Access Data – DNA: Distributed Network Attack**

- client-server application  
- DNA client runs in the background, only taking unused processor time  
- performs an exhaustive key search on Office ‘97 and Office 2000 encrypted documents

*Expected recovery times (200 MHz, Intel machines):*

<table>
<thead>
<tr>
<th>Product</th>
<th>Maximum Time</th>
<th>Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 Client Network</td>
<td>16 Days</td>
<td>8 Days</td>
</tr>
<tr>
<td>50 Client Network</td>
<td>8 Days</td>
<td>4 Days</td>
</tr>
<tr>
<td>100 Client Network</td>
<td>4 Days</td>
<td>2 Days</td>
</tr>
<tr>
<td>500 Client Network</td>
<td>20 Hours</td>
<td>10 Hours</td>
</tr>
<tr>
<td>1,000 Client Network</td>
<td>10 Hours</td>
<td>5 Hours</td>
</tr>
</tbody>
</table>
Breaking ciphers used in GSM (1)

GSM - world's most widely used mobile telephony system
- 51% market share of all cellular phones, both analog and digital
- over 215 million subscribers in America, Europe, Asia, Africa, and Australia
- In the US, GSM employed in the "Digital PCS" networks of Pacific Bell, Bell South, Omnipooint, etc.

Two voice encryption algorithms:
- A5/1 and A5/2
  encrypt voice between the cellphone and the base station

Breaking ciphers used in GSM (2)

Both voice encryption algorithms
- never published
- designed and analyzed by the secretive "SAGE" group (part of ETSI – European Telecommunications Standard Institute)
- A5/1 believed to be based on the modified French naval cipher

Both algorithms reverse-engineered by "Marc Briceno" with the Smartcard Developer Association published by the Berkeley group
- A5/1 in May 1999,
- A5/2 in August 1999

Breaking ciphers used in GSM (3)

Published attacks

A5/2
- August 1999, Ian Goldberg and David Wagner, U.C. Berkeley
  Number of operations in the attack $\sim 2^{46}$

A5/1
- May 1999, Jovan Golic
  Number of operations in the attack $\sim 2^{68}$
- December 1999, Alex Biryukov and Adi Shamir
  Less than 1 second on a single PC with 128 MB RAM and two 73 GB hard disks.
  Based on the analysis of the A5/1 output during the first two minutes of the conversation.
Features required from today’s ciphers

- **STRENGTH**
- **PERFORMANCE**
- **FUNCTIONALITY**
  - easy key distribution
  - digital signatures

Software or hardware?

**SOFTWARE**
- low cost
- flexibility (new cryptoalgorithms, protection against new attacks)
- security of data during transmission

**HARDWARE**
- speed
- random key generation
- access control to keys
- tamper resistance (viruses, internal attacks)

Basic hardware implementations of cryptography

- VLSI chip
- smart card
- PCMCIA card
- cryptographic card
- stand-alone cryptographic device
Applications most suitable for hardware implementations

- hardware accelerators for security gateways and routers
- wireless communications
- universal smart cards for electronic commerce
- electronic wallet
- Certificate Authority - center for registration of public keys
- key-escrow cryptography
- military devices
- high-grade security devices

Evolution of cryptography and cryptanalysis

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mathematics</td>
<td>DES</td>
<td>RSA</td>
<td>ECC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptanalyzer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NSA

National Security Agency
(also known as “No Such Agency” or “Never Say Anything”)

Created in 1952 by president Truman

Goals:
- designing strong ciphers (to protect U.S. communications)
- breaking ciphers (to listen to non-U.S. communications)

Budget and number of employees kept secret
Largest employer of mathematicians in the world
Larger purchaser of computer hardware
RSA Security Inc.

- patents for RSA, RC5, RC6 and other cryptographic algorithms
- over 500 mln users of the basic cryptographic library BSAFE
- RSA Laboratory
- RSA Conference
- spin-off companies
  - VeriSign - Public Key Infrastructure

Companies introducing security into their products/services

- software
  - Lotus
  - Microsoft
  - Netscape
  - Novell
  - Oracle
  - Intuit

- hardware
  - IBM
  - Motorola
  - Intel
  - Compaq
  - Sun
  - Hewlett-Packard

- telecom
  - AT&T
  - Worldcom
  - Nothern Telecom

- finances
  - Visa
  - Mastercard
  - Verifone

Worldwide Survey of Cryptographic Products

NAI Labs, June 2001

<table>
<thead>
<tr>
<th>Companies</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>413</td>
<td>763</td>
</tr>
<tr>
<td>532</td>
<td>758</td>
</tr>
</tbody>
</table>

Foreign products developed in 43 countries distributed in at least 76 countries
Foreign Cryptographic Products

Increase in the number of foreign cryptographic products and companies

American and international standards regarding public key cryptography