Lecture 1
Class introduction

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.

To view a copy of this license, visit:
http://creativecommons.org/licenses/by-sa/4.0/

Lecture 1—Contents

Why Information Theory + Security?

Security terminology
Goals
Attacks and threats
Services
Mechanisms

Class summary
Security goals

Desirable features of communication and networks

**Confidentiality** information is available to the intended receiver only

**Integrity** information is received exactly as sent

**Availability** service is always available even if someone intends to disrupt the network (see difference vs. reliability and safety)

**Accountability** it is always possible to identify who is responsible for any information event

**Privacy** information is (used but) not disclosed to anyone (see conflict with accountability)

...
Security terminology

Security services

Security services should protect communications and network protocols from attacks

- **Secrecy** makes message unintelligible for eavesdroppers
- **Integrity protection** makes it possible to detect whether a message was intercepted and modified
- **Access control** can protect from denial of service
- **Message authentication** allows to detect forged messages
- **Entity authentication** protects from masquerades
- **Notarization** prevents repudiation by source and/or destination
- **Anonymization** prevents consistent association between message and user

Security mechanisms

A security mechanism is a way to implement some security service

- **Encryption** message is transformed and only the intended receiver can reverse the transform
- **Digital signature** a string is appended to the message that can only be created by the legitimate transmitter but can be publicly verified
- **Intrusion detection** identify characteristics of malicious behaviour (signature) or non-typical legitimate behaviour (anomaly)
- **Message authentication codes** a string is appended to the message that can only be created by the legitimate transmitter or receiver
- **Distribution of cryptographic keys**
- **Randomization** events of the same category are randomly permuted to break dependences

Security goals, threats, services and mechanisms

<table>
<thead>
<tr>
<th>Goals</th>
<th>Threats</th>
<th>Services</th>
<th>Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Eavesdropping</td>
<td>Secrecy</td>
<td>Encryption</td>
</tr>
<tr>
<td>Integrity</td>
<td>Forgery</td>
<td>Integrity protection</td>
<td>Key agreement</td>
</tr>
<tr>
<td>Availability</td>
<td>Repudiation</td>
<td>Authentication</td>
<td>Digital signature</td>
</tr>
<tr>
<td>Accountability</td>
<td>Masquerade</td>
<td>Notarization</td>
<td>Authentication codes</td>
</tr>
<tr>
<td>Privacy</td>
<td>Denial of service</td>
<td>Access control</td>
<td>Intrusion detection</td>
</tr>
<tr>
<td></td>
<td>Jamming</td>
<td>Jamming rejection</td>
<td>Spreading</td>
</tr>
</tbody>
</table>

Unconditional vs computational security

**Computational security** systems can be broken by an attacker with enough computational power

- **Post-quantum security** systems have not been shown breakable by quantum computers in short time

In **unconditional security**, the attacker is not better off at guessing by observing the protocol communications. However, in designing the system, (statistical) knowledge of the attacker channel is often required
Lecture 1—Contents

Why Information Theory + Security?

Security terminology
- Goals
- Attacks and threats
- Services
- Mechanisms

Class summary

Class summary: core lectures


Secrecy without cryptography. The wiretap channel model. Rate-equivocation pairs. Secrecy rates. Secrecy capacity for binary, Gaussian and fading channel models. Extension to OFDM and MIMO channels

Security from uncertainty. Secret key agreement from common randomness on noisy channels. Information theoretic models and performance limits of quantum cryptography.


Class summary: elective lectures (I)

The gossip game. Broadcast and secrecy models in multiple access channels. The role of trusted and untrusted relays.


A cipher for free? Information theoretic security of random network coding.

The jamming game. Optimal strategies for transmitters, receivers and jammers in Gaussian, fading and MIMO channels.

Alea iacta est. Secure and true random number generation. Randomness extractors and smooth guessing entropy.

Class summary: elective lectures (II)

Writing in sympathetic ink. Information theoretic models of steganography, watermarking and other information hiding techniques.

Leaky buckets and pipes. Information leaking and covert channels. Timing channels.

The dining cryptographers. Privacy and anonymity. Secure multiparty computation.

Piecing it together. Universally composable security in the computational, information theoretic and quantum information frameworks

Information theoretic democracy. Privacy, reliability and verifiability in electronic voting systems.

The Big Brother. An information theoretic formulation of database security: the privacy vs utility tradeoff.