Course

- Title: Network Security (ICE615)
- Credit/Hour: 3/3
- Prof: Kwangjo Kim (x6118)
- TA: Wooseok Ham (x6236)
- Hour: Tue. / Thu., AM 10:30 - 12:00
- Web page: http://caislab.icu.ac.kr/course/2002/autumn/ice615

Syllabus

1. Course Description
   This course offers how to evaluate a variety of vulnerabilities over the existing network and how to construct security protocols and their applications by using cryptoalgorithms, digital signature and hash function to guarantee integrity of information and authentication of network entities. Moreover, every student can get the knowledge on a typical network authentication protocol like Kerberos, secure e-mailing system like PEM, X.400, S/MIME and PGP, emerging network security protocol like IPSEC and SET protocol and firewall.

2. Textbook
   - Auxiliary:
     3. Internet RFCs / Handout

3. Test and Evaluation
   - Midterm Exam: 15%  - Quiz:5%  - Final Exam:25%  - Homework: 15%  - Term Project: 15%
   - Term Paper: 20%, Attendance: 5% (Total: 100%)
### Weekly Lecture

<table>
<thead>
<tr>
<th>Week</th>
<th>Contents</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Digital Signature &amp; Hash ft TP Pro</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Basic Protocol</td>
<td>HW#1</td>
</tr>
<tr>
<td>4</td>
<td>Applied Protocol</td>
<td>9/26</td>
</tr>
<tr>
<td>5</td>
<td>Authentication System</td>
<td>HW#2</td>
</tr>
<tr>
<td>6</td>
<td>TP Contest #1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Midterm Exam Written</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Authentication Protocol TP Rep#2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week</th>
<th>Contents</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Kerberos</td>
<td>HW#3</td>
</tr>
<tr>
<td>10</td>
<td>E-mail Security I</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>E-mail Security II</td>
<td>HW#4</td>
</tr>
<tr>
<td>12</td>
<td>IPSEC</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Web Security/Firewall</td>
<td>HW#5</td>
</tr>
<tr>
<td>14</td>
<td>TP contest</td>
<td>TP Paper</td>
</tr>
<tr>
<td>15</td>
<td>Final Exam</td>
<td>Written</td>
</tr>
</tbody>
</table>

### Term Projects(l)

2001

- Anonymous Authentication in Dynamic Groups
- The implementation of security manager in Open Bluetooth Axis stack
- Cryptanalysis of the Rijndael
- Multiple Selective Mutual Authentication Protocol For Peer-to-Peer System
- Round Saving Bulletin-based Tripartite Electronic Lottery Protocol
- Secure Massager Protocol using Rijndael
- Trust analysis of web of trust
- Denial of Service Attacks and Countermeasures Analysis
- Study on X.509 certificates and CA’s Certificate path validation
- Compare Firewall Products
- Traitor tracing
- Implementing Secure IRC application with ElGamal
- Secure Distributed Document Sharing System

(c)ICU Kwangjo Kim 3

(c)ICU Kwangjo Kim 4
Term projects(II)

2000
- Anonymous Channel
- A Proposal of Efficient Wireless PKI
- DPA and Countermeasure
- Why IPSec is required for Multicast Networks
- Integrated Security Manager for scanning system’s vulnerability

1999
- A Study on Key Management Protocol
- GMN Authentication Protocol
- Video copyright protection using digital watermarking
- A Study on the existing Network security Mechanism
- Authentication Method in Wireless Personal Area Network

Why are you taking this course?

- Need credits
- Thought a real professor was teaching
- Want to be rich and famous
- Security is a hot issue.
- Want to be a information warrior
- Want to be a hacker
- Want to know DES, MD5, and AES
- Etc.
Security

- Protecting asset
- Security goals
- Security policy
- Identify threats
- Develop controls / countermeasure
- Disaster plan

Computer Security

- Asset
  - Hardware
  - Software
  - Information
- Goal
  - Privacy (Confidentiality)
  - Integrity (Accuracy)
  - Availability
Threats

- Natural and Physical
- Unintentional
- Intentional
  - Interruption
  - Interception
  - Modification
  - Fabrication

Threat Jargon

- Active (Program)
  - Worm (independent) : program that replicates itself through network
  - Logic bomb : malicious instructions that trigger on some event in the future, such as a particular time occurring
  - Trojan horse : program that does something unexpected (and often secretly)
  - Trapdoor : an undocumented entry point intentionally written into a program, often for debugging purposes, which can be exploited as a security flaw
  - Virus : program fragment that, when executed, attached itself to other programs
- Passive
  - Sniffer
  - Wiretap
  - TEMPEST
  - Social Engineering (dumpster diving)
Countermeasures

- Education
- Physical protection
- Authentication
- Authorization
- Auditing

* Threat/countermeasures: never ending cycle

---

Risks and Countermeasures

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mea sure</th>
<th>DB Storage</th>
<th>Host computer</th>
<th>Wireless Network</th>
<th>Router</th>
<th>Telephone FAX Terminal</th>
<th>Smart Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data/file deletion, copy modification</td>
<td>Access Control Secure DBMS</td>
<td>OS/Application vulnerabilities, Denial-of-service, Virus, Replay attack, EMI/EMC</td>
<td>Encryption, Certification, Access Control</td>
<td>Router traffic, Wiretapping</td>
<td>Protocol Vulnerability, Traffic overload</td>
<td>Impersonation EMI/EMC, Impersonation Duplication</td>
<td></td>
</tr>
</tbody>
</table>

Network Security

Layer 1: Confidentiality, Encryption, Traffic Control
Layer 2: Authentication, Authentication Exchange
Layer 3: Integrity, Data Integrity
Layer 4: Non-repudiation, Digital Signature
Layer 5: Access Control
Layer 6: Notorization
Layer 7: Security Label, Detection, Audit, Recovery

Are we at risk?

- **Assets**
  - air defense
  - command and control
  - banking
  - power grid
  - phone system
  - traffic signal
  - corporate e-mail
  - refinery
  - DMV(Dep’t of Motor Vehicles)
  - medical records
  - personnel records
  - nuclear weapon system
  - Taco Bell
  - electronic funds transfer
  - air traffic control
  - elevator
  - trains
  - grades
  - stock exchange
  - TV/radio
  - police record
  - payroll

- **Information Warfare / Electronic Warfare**
The Attackers

- Amature
- Insider (greed, disguntled)
- Kids
- Hackers
- Criminals
- Spies
- Sociopath(terrorist/vandal)

Why?

- Money
- retribution
- sport
- pathological
- political/military

; easy to do, hard to catch, harder to prosecute
Detect & Correct

When an incident is detected:
- Don’t panic
- Identify the problem
- Stop the damage
- Assess the damage
- Save evidence, document
- Restore system
- Determine/eliminate cause
- Notify mgt, CERT (CERT-KR)

Handling the Intruder

- Monitoring the intruder
- Tracing the connection
- Contacting the intruder
- Terminating the intruder :-(
Legal/Political Issues

- estimate losses
- classified or military information
- some computer laws
- rules of evidence (hardcopy)
  - US law classifies cryptography as a munitions!
  - many encryption algorithm are patented/licensed.
- key escrow.
- Should the citizens of a country have the right to create and store documents their government can’t read? -- Ron Rivest

Risk Assessment

- Identify assets and value
- Determine vulnerabilities
- Estimate probabilities
- Estimate losses
- Identify controls and their cost
- Estimate savings