

Course

- ✍ **Title : Network Security (ICE615)**
- ✍ **Credit/Hour : 3/3**
- ✍ **Prof : Kwangjo Kim**
- ✍ **TA : Byongcheon Lee**
- ✍ **Hour : Tue. / Thu., PM 1:30 - 3:00**
- ✍ **Web page :**
<http://caislab.icu.ac.kr/course/2001/autumn/ice615>

(c)ICU Kwangjo Kim

1

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

- Main : Network Security : Private Communication in a Public World, C. Kaufmann, R. Perlman, M. Speciner, Prentice Hall, 1995, ISBN 0-13-061466-1
- Auxiliary :
 - (1) Cryptography – Theory and Practice, Dougals R. Stinson, CRC Press, ISBN 0-8493-8521-0,1995.
 - (2) Cryptography and Network Security, William Stallings, Prentice Hall, ISBN 0-13-869017-0,1998.
 - (3) Internet RFCs/ Handout

3. Test and Evaluation

- Midterm Exam: 17% - Quiz:3% - Final Exam:20% - Homework: 20% - Term Project : 20%
-Term Paper : 15%, Attendance : 5%

(c)ICU Kwangjo Kim

2

Weekly Lecture

| Week | Contents | Comment | Week | Contents | Comment |
|------|-----------------------------------|----------|------|--------------------------|----------|
| 1 | Introduction | TP | 9 | E-mail Security (PGP) | HW#3 |
| 2 | Digital Signature & Hash ft HW #1 | | 10 | E-mail Security (S/MIME) | |
| 3 | Basic Protocol | | 11 | IPSEC | HW#4 |
| 4 | Applied Protocol | TP Rep#1 | 12 | Web security | TP rep#3 |
| 5 | Authentication System | | 13 | Firewall | |
| 6 | Authentication Protocol | HW#2 | 14 | TP contest | (AC'00) |
| 7 | Kerberos | TP Rep#2 | 15 | Final Exam | Written |
| 8 | Midterm Exam | Written | | | |

(c)ICU Kwangjo Kim

3

Term Projects(I)

- ✍ Security application to your majors
- ✍ Trust analysis: PGP web of trust vs. trust hierarchy
- ✍ NSA's FORTEZZA card and key escrow issues
- ✍ Security features of various software packages: data bases, OS's
- ✍ Vulnerabilities revealed by traffic analysis
- ✍ Secure OS technologies (TMACH, CMWs)
- ✍ Computer architectures for security
- ✍ Digital watermarks and copyrights
- ✍ Vulnerabilities of Java, javascript, ActiveX
- ✍ Techniques/algorithms for hi-speed crypto (parallel)
- ✍ DNS security
- ✍ Cryptographic hashes
- ✍ Information warfare /electronic warfare
- ✍ IPv6 key mgt: photuris, SKIP, ISAKMP

(c)ICU Kwangjo Kim

4

Term projects(II)

- ✍ Key distribution for multicast sessions
- ✍ Encryption in banking, e-commerce, or digital cell phone
- ✍ Electronic payment schemes (IKP, ecash, ...)
- ✍ Chaotic functions as one-time pads
- ✍ Compare firewall products
- ✍ Authorization models (capabilities, ACLs)
- ✍ Virtual Private Networks
- ✍ Compare UNIX scanners (ISS, COPS, SPI)
- ✍ X.509 certificates and CA's
- ✍ Micropayment schemes
- ✍ Implement 64-bit block ciphers (on Alpha)
- ✍ Performance comparison of: ciphers, hashes, public key
- ✍ Adding security to an application (talk, irc, ...). First add authentication, then secret-key encryption, then Diffie-Hellman, then public-key, then multi-platform.
- ✍ Etc.

(c)ICU Kwangjo Kim

5

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 an information warrior
- ✍ Want to be a hacker
- ✍ Want to know DES, MD5, and AES
- ✍ Etc./

(c)ICU Kwangjo Kim

6

Security

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

(c)ICU Kwangjo Kim

7

Computer Security

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

(c)ICU Kwangjo Kim

8

Threats

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

(c)ICU Kwangjo Kim

9

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)**

(c)ICU Kwangjo Kim

10

Countermeasures

- ✍ Education
- ✍ Physical protection
- ✍ Authentication
- ✍ Authorization
- ✍ Auditing

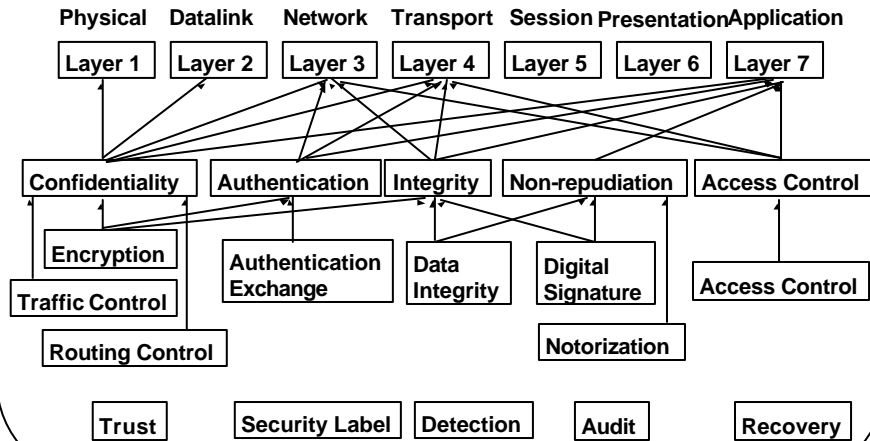
*** Threat/countermeasures : never ending cycle**

Risks and Countermeasures

| | DB Storage | Host computer | Wireless Network | Router | Telephone FAX Terminal | Smart Card |
|---------|--|---|--|--|---------------------------|--|
| Risk | Data /file deletion copy modification | OS / Application vulnerabilities Denial-of-service Virus Replay attack EM/EMC | Wiretapping Data Modification EM/EMC | Protocol Vulnerability Traffic overload | Impersonation EM/EMC | Impersonation Duplication |
| Measure | Access Control Secure DBMS | Identification Vul. diagnosis Crypto API Digital Signature TEMPEST Anti-virus Secure OS | Cipher algorithm Hash ft. | Vulnerability checking Secure Router | Identification TEMPEST | Identification Secure COS High speed LSI |

"Classification of Information Security, KIISC Review, '98.3.p.7

Network Security



(c)ICU Kwangjo Kim

13

Are we at risk ?

Assets

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

Information Warfare / Electronic Warfare

(c)ICU Kwangjo Kim

14

The Attackers

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

(c)ICU Kwangjo Kim

15

Why ?

- ✍ **Money**
 - ✍ **retribution**
 - ✍ **sport**
 - ✍ **pathological**
 - ✍ **political/military**
- ; easy to do, hard to catch, harder to prosecute**

(c)ICU Kwangjo Kim

16

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)**

(c)ICU Kwangjo Kim

17

Handling the Intruder

- ✍ **Monitoring the intruder**
- ✍ **Tracing the connection**
- ✍ **Contacting the intruder**
- ✍ **Terminating the intruder :-)**

(c)ICU Kwangjo Kim

18

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

(c)ICU Kwangjo Kim

19

Risk Assessment

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

(c)ICU Kwangjo Kim

20