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

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

- Auxilary :

(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%

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			

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

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.

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 occuring
  - 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

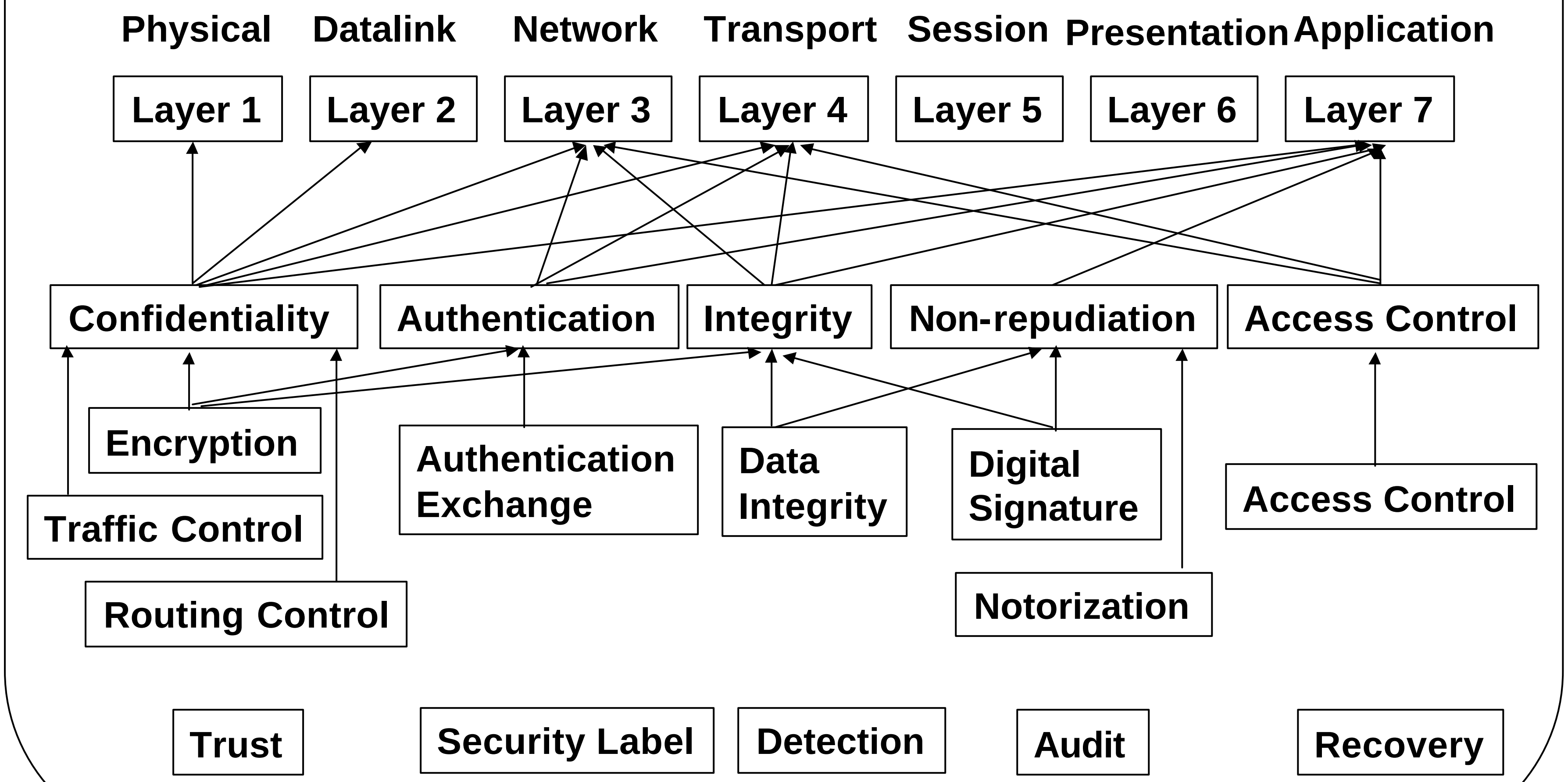
* Threat/countermeasures : never ending cycle

Risks and Countermeasures

	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 EMI/EMC	Wiretapping Data Modification EMI/EMC	Protocol Vulnerability Traffic overload	Impersonation EMI/EMC	Impersonation Duplication
Measure	Access Control Secure DBMS	Identification Vul. diagonsis 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



Physical
Datalink
Network
Transport
Session
Presentation
Application

Layer 1
Layer 2
Layer 3
Layer 4
Layer 5
Layer 6
Layer 7

Confidentiality
Authentication
Integrity
Non-repudiation
Access Control

Encryption
Traffic Control
Routing Control
Authentication Exchange
Data Integrity
Digital Signature
Notorization
Access Control

Trust
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