Course

- Title : Cyber Security (CS748)
- Credit/Hour : 3/3
- Prof : Kwangjo Kim (Room 2215@N5)
- TA : Jangseong Kim,
- Hour : Tue. / Thu., 16:00 - 17:15
- Web page :

  http://caislab.kaist.ac.kr/lecture/2010/fall/cs748/index.html

Prof. Kwangjo Kim

- Academic History
  - BS (1981) and MS (1983)from EE@Yonsei Univ.
  - Ph.D(1991) from EECS@Yokohama National University
- Career
  - '79 ~ '97 : Section Head of Coding Tech. #1 in ETRI
  - '96 ~ '97 : Adjunct Professor at Computer Science Dept. in ChungNam National Univ.
  - '99 ~ '00 : Visiting Professor at Univ. of Tokyo, Japan
  - '99 ~ '05 : Director of IACR / Institute for IT-gifted Youth
  - '98 ~ '09 : Professor / Dean of School of Engineering in ICU
  - '02 : 1000 World Leaders of Scientific Influence by ABI
  - '05 ~ '06 : Visiting Scholar at MIT/UCSD
  - '09.1~'09.12: President of KIISC
  - '09.3 ~ : Professor in CSD@ KAIST
- Academic Activities
  - More than 100 Program Committee Members of Crypto and Security Conferences
  - Chairperson of Asiacrypt Steering Committee ('05-'08)
  - More than 20 invited talks to international conferences
- Awards
  - Presidential Citation ('09.9), Minister of NIS ('09.12)

Syllabus

Objective:

This course discusses the latest issues on cyber security beginning with the introduction of basic cryptography to understand how to design authentication primitives covering multi-party cryptographic protocols and core security components for network security, *etc*. Special presentations on DDoS defenses and secure smart grid are scheduled. The enrolled student must read and present the recommended papers and practice your term project under the guidance of your professor and TA.

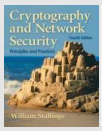
References:

W. Stallings, "Cryptography and Network Security", 4th Ed., Pearson Education Inc, ISBN 0-13-187316-4, 2006

J. Mirkovic, S. Dietrich, D. Dittrich and P. Reiher, "Internet Denial of Service, Attack and Defenses Mechanisms", 2005, Pearson Education Inc., ISBN 0-13-147573-8

Side Channel Attack: http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html

DETER : http://www.isi.edu/deter/, etc.



Grading Policy:

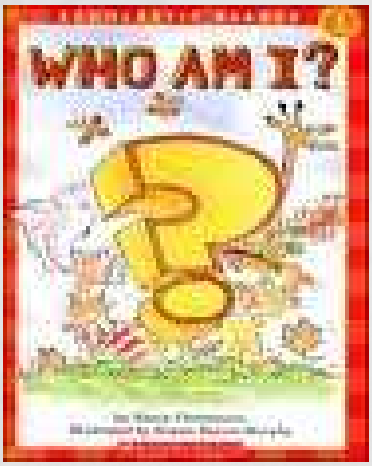
- Midterm Exam: 15% - Quiz:5% - Final Exam:15% - Homework: 10%
- Term Project : 25% -Term Paper : 25%, Attendance : 5% (Total : 100%)

What is Cyber Security?

- (Redirected from Cyber security) http://en.wikipedia.org/wiki/Cyber_security
- **Computer security** is a branch of computer technology known as information security as applied to computers and networks.
- The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
- The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events, respectively.
- The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

Your Background

- Describe your previous or current career on information security and cryptography



Weekly Lecture Plan

Week(Date)	Topic	Remark
1 (9/2,9/7)	Overview/ Basic to Cryptography I	
2(9/9,9/14)	Basic to Cryptography II	~9/14: Deadline of course change
3(9/16,9/21)	Side Channel Attack	9/16:TP Proposal 9/21: No Class
4(9/23,9/28)	Authentication Protocol/ ZKIP	9/23: No class
5(9/30,10/05)	Paper Presentation #1	
6(10/7,10/12)	Multi-party Protocol	
7(10/14,10/19)	TP Mid-Presentation	
8(10/21,10/26)	Midterm Exam	10/21
9(10/28,11/2)	SSL & TLS	
10(11/4,11/9)	IPSEC, Firewall, IDS	
11(11/11,11/16)	DDoS Defenses	
12(11/18,11/23)	Secure Smart Grid	
13(11/25,11/30)	Paper presentation #2	
14(12/2,12/07)	Car Security	
15(12/9,12/14)	TP Final presentation	
16(12/16,12/21)	Final Exam	12/16

* Schedule can be subject to change slightly depending on the number of enrolled students.

Paper Reading & Term Project

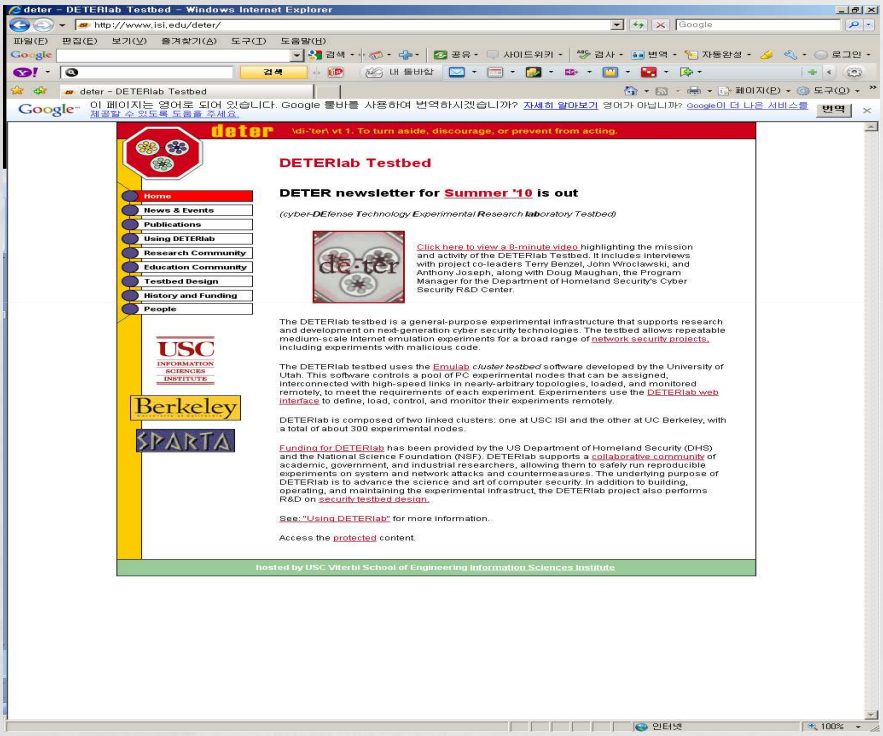
- Paper Reading
  - Recommended paper will be suggested
  - You can select among basic and advanced papers
- Term Project
  - e. g., Refer to DETER web page and select your challenging topic
  - Term Project Proposal
    - Problem Statement
    - My Approach
    - Time Schedule
    - Expected outcome
  - 2 times presentation
- Consult TA for details.

Challenging Topics for your TP

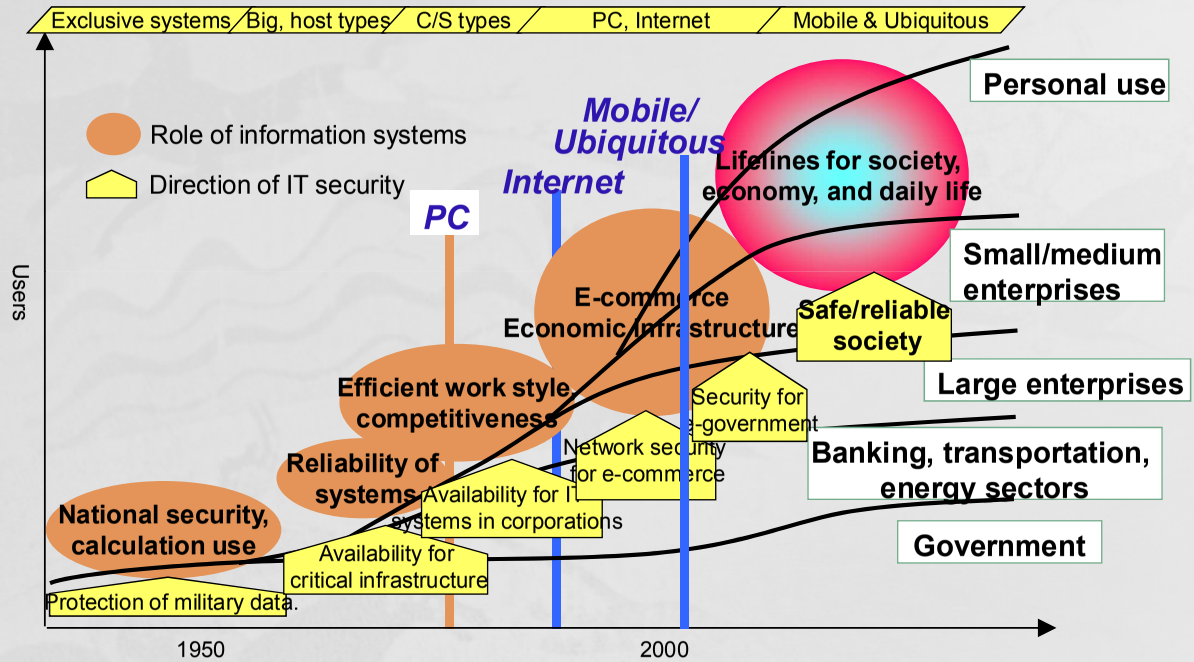
1. Scalable trustworthy systems (including system architectures and requisite development methodology)
2. Enterprise-level metrics (including measures of overall system trustworthiness)
3. System evaluation life cycle (including approaches for sufficient assurance)
4. Combatting insider threats
5. Combatting malware and botnets
6. Global-scale identity management
7. Survivability of time-critical systems
8. Situational understanding and attack attribution
9. Provenance (relating to information, systems, and hardware)
10. Privacy-aware security
11. Usable security

http://www.goingwimax.com/cybersecurity-roadmap-or-internet-roadblock-11516/

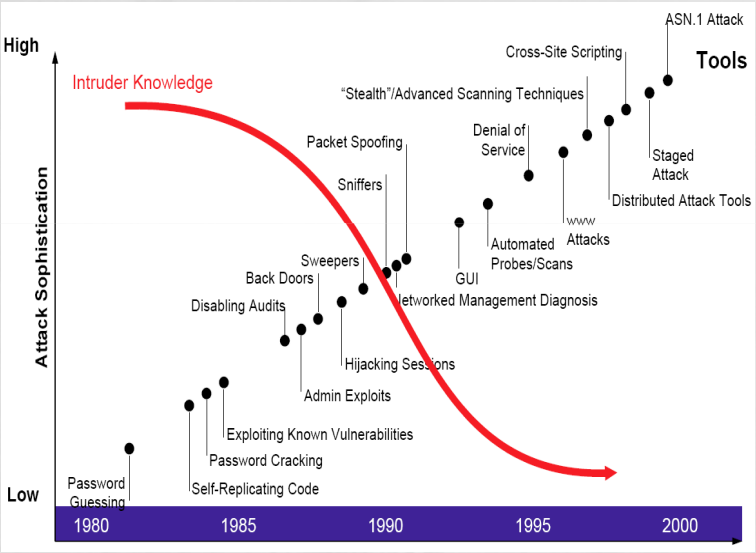
DETER Testbed



Changing IT Security



Evolution of Attack



- From an expert to anyone
- From a hobby to a profitable industry
- From annoying to destructive
- From playing to stealing
- From simplicity to complexity

Strategic Hacking Era

- Cyber Security is now in the top 5 national security priorities of most great powers and many middle powers
- Defense is not enough; all countries developing offense
- Private sector defense contractors are going on the offensive
- Everyone is attacking everyone else, even allies vs. allies
- 2 likely scenarios: chaos or severe restriction

ITU & Cybersecurity

- ITU constitutes a unique global forum to discuss related to cybersecurity
- Based on the existing mandate and country requests, the ITU Secretary-General has set cybersecurity as a top priority
- ITU Membership has been calling for a greater role to be played by ITU in matters relating to cybersecurity through a number of Resolutions, Decisions, Programmes and Recommendations
- ITU provides a global perspective and expertise and is currently promoting cybersecurity through a range of activities related to standardization, radiocommunication and technical assistance to countries, tailored to their specific needs

International Telecommunication Union

UN Resolutions on "Culture of Security" (1/2)

- **UN Resolution 57/239** (2002) on the "Creation of a global culture of cybersecurity"
- Identifies nine elements for creating a global culture of cybersecurity:

a) **Awareness**
b) **Responsibility**
c) **Response**
d) **Ethics**
e) **Democracy**
f) **Risk Assessment**
g) **Security Design and Implementation**
h) **Security Management**
i) **Reassessment**

International Telecommunication Union

UN Resolutions on "Culture of Security" (2/2)

- **UN Resolution 58/199** (2004) further emphasizes the "promotion of a global culture of cybersecurity and protection of critical information infrastructures"
  - Recognizes the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services
  - Notes the increasing links among most countries' critical infrastructures and that these are exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns
  - **Recognizes that effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders**
  - Encourages Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to **share their best practices** and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity

Cybersecurity SG Activities in ITU-T(Standardization)

- Study Group 17 has primary focus on communication security and is the Lead Study Group on security for ITU-T
- Work under way under Study Group 17 Questions:
  - Working Party 1: Network and information security
    - Q 1 Telecommunications systems security project
    - Q 2 Security architecture and framework
    - Q 3 Telecommunications information security management
    - Q 4 Cybersecurity
    - Q 5 Countering spam by technical means
  - Working Party 2: Application security
    - Q 6 Security aspects of ubiquitous telecommunication services
    - Q 7 Secure application services
    - Q 8 Telebiometrics
    - Q 9 Service oriented architecture security
  - Working party 3: Identity management and languages
    - Q 10 Identity management architecture and mechanisms
    - Q 11 Directory services, Directory systems, and public-key/attribute certificates
    - Q 12 Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration
    - Q 13 Formal languages and telecommunication software
    - Q 14 Testing languages, methodologies and frameworks
    - Q 15 Open Systems Interconnection (OSI)

CyberSecurity Issues & Challenges

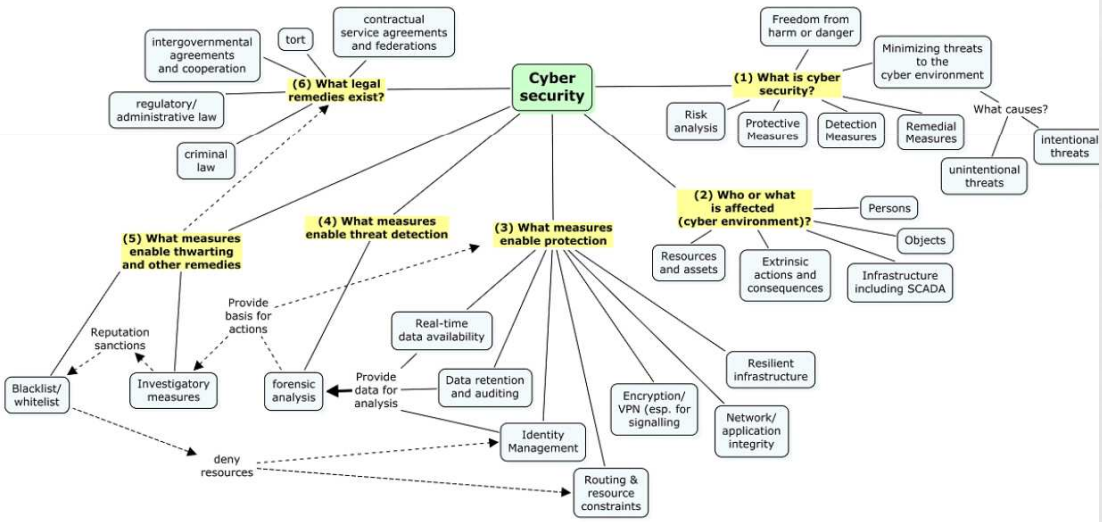
- Constant evolution of the nature of cyber threats
- Vulnerabilities in software and hardware applications and services changing and increasing
- Countries are increasingly at risk and under attack
- Low entry barriers and increasing sophistication of the type of cybercrimes committed
- Loopholes in current legal frameworks
- Absence of appropriate national organizational structures to deal with the threats
- Inadequate cooperation amongst the various stakeholders and stakeholder groups
- The lack of cybersecurity is global problem that cannot be solved by any single entity (country or organization) alone!

The world is faced with the challenging task of developing harmonized and comprehensive strategies at the global and international level and implementing these with the various relevant national, regional, and international stakeholders in the countries

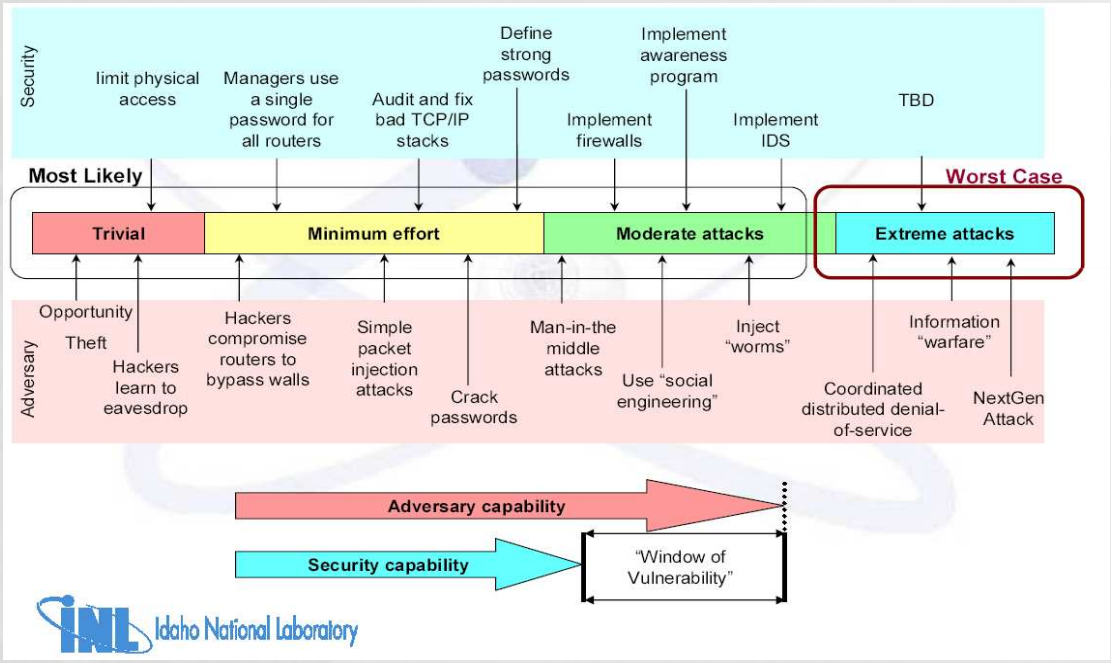
International Telecommunication Union

Cyber Security in ITU-SG17

- Question 4/17: Cybersecurity
  - Scope -



Electronic Arms Race of Cyber Security



보안 위협의 진화

과거 개별적/국소적이고 제한된 보안 위협에서 진화하여, 현재는 보안위협의 정도가 전체 IT인프라의 다운이나 광범위한 해킹으로 확대되어 위협의 영향이나 손해가 과거에 비해 훨씬 광대해짐.

❑2006 CISCO 발표자료