Introduction to Information Security
(정보보호 개론)
CS 448

Prof. Kwangjo Kim

Week 1 : Introduction I

How it begins?

Course Overview(1/2)

Objective: *This course introduces the fundamental understanding on information security to build for any secure system covering the design and breaking of classical, symmetric and asymmetric cryptosystem with mathematical background. We also deal with the cryptographic protocols and their applications to authentication and identification. After finishing this class, the students are expected to understand the broad spectrum on information security and cryptography to advance their challenging research.*

Course Webpage

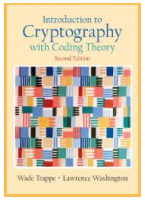
http://caislab.kaist.ac.kr/Lecture/data/2011/spring/cs448/

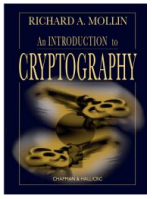
Prof. Kwangjo Kim

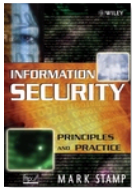
- Contact Information
  - Office : Room 2215@N5, 042-350-3550, 010-9414-1386
  - E-mail: kkj@kaist.ac.kr Home page: http://caislab.kaist.ac.kr/kkj
- Career
  - '79 ~ '97 : Section Head of Coding Tech. #1 in ETRI
  - '96 ~ '97 : Adjunct Professor at Computer Science Dept. in ChungNam National Univ.
  - '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, Honorable President of KIISC
- Academic Activities
  - More than 100 Program Committee Members of Crypto and Security Conferences
  - Editors of JMC, IJIS, etc.
  - More than 20 invited talks to international conferences
- Awards
  - Presidential Citation ('09.9), Minister of NIS ('09.12)

Course Overview(2/2)

TA: *Mr. Yi Jae Park,* ***Jiseong Gu***







Text: Handouts

References:

1. Wade Trappe, Lawrence C. Washington, "Introduction to Cryptography with Coding Theory", 2nd Ed, 2005, Prentice Hall ISBN 0-13-186239-1
2. Richard A. Mollin, "An Introduction to Cryptography", Chapman & Hall/CRC, 2001, ISBN 1-58488-127-5
3. Mark Stamp, "Information Security: Principles and Practices", ISBN:978-0-471-73848-0, 2005 Oct. Wiley International

(한국어 "정보보안 이론과 실제", 안태남 등 번역), and others.

Grading Policy:

Midterm (35%), Final (35%), Quiz (10%), HW (10%), Attendance (10%)

Who is attending this clas

- Can you survive this course?
- Why did you choose this course?
- What background do I need?
  - Programming language
  - Mathematics
- What do you want to be after this course?
- Any other question?

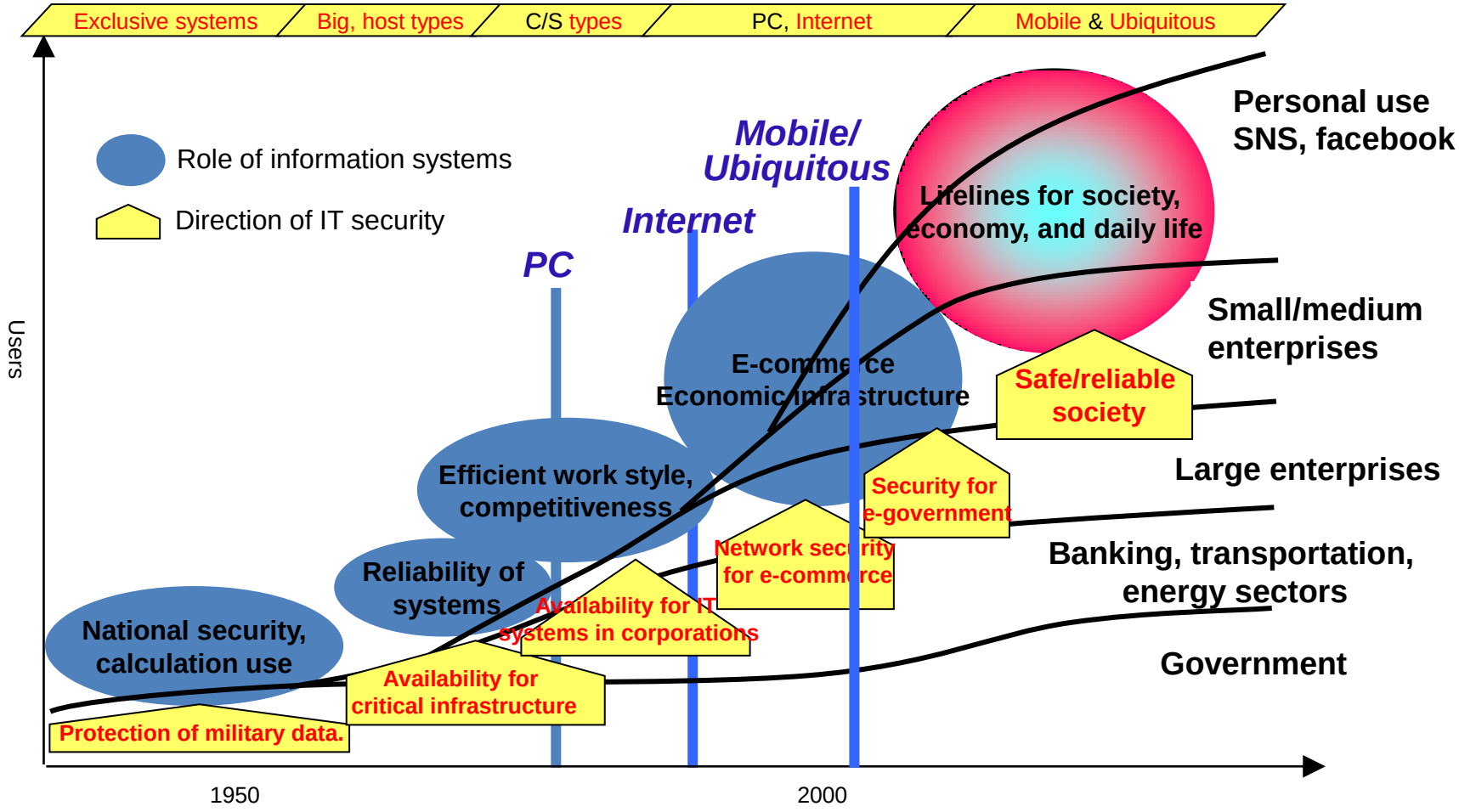
Schedule (1/2)

Week	Topic	Remark
1	Introduction I	2/8, 2/10
2	Introduction II, Basic Terms	2/15, 2/17
3	Classical Ciphers	2/22, 2/24, Quiz#1
4	Block Cipher, DES	3/1(off) , 3/3
5	AES	3/8, 3/10
6	Mode of Operation	3/15, 3/17
7	Cryptanalysis of Block Cipher, Summary I	3/22, 3/25 Programming HW #1
8	Midterm	3/29, 3/31(off)

Schedule (2/2)

Week	Topic	Remark
9	Public Key Cryptosystem Number Theory	4/5, 4/7
10	Digital Signature	4/12, 4/14, Quiz#2
11	Hash Functions	4/19, 4/21
12	Cryptographic Protocol	4/26, 4/28
13	Secret Sharing Protocol	5/3, 5/5 (off)
14	Identification Protocol	5/10(off), 5/12
15	Special Talk, Summary II	5/17, 5/19 Programming HW #2
16	Final Exam	5/24, 5/26(off)

Trends of IT Security



What is Information Security (1/2)?

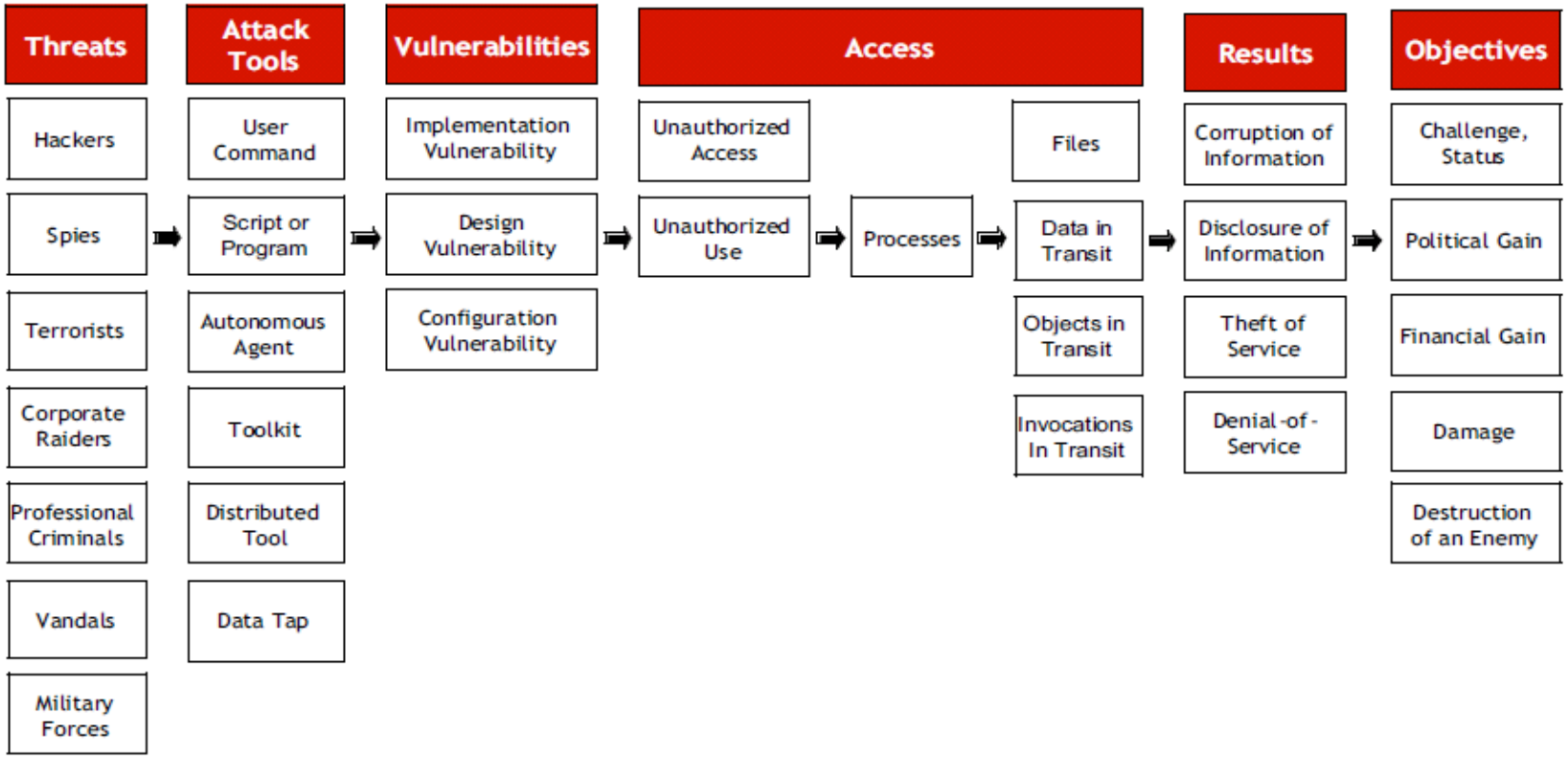
- **Data**
  - **recording of "something" measured**
  - **Raw material, just measured**
- **Information**
  - **Information is the result of processing, manipulating and organizing data in a way that adds to the knowledge of the receiver.**
  - **Processed, stored or transmitted data**
- **Knowledge**
  - **Knowledge is normally processed by means of structuring, grouping, filtering, organizing or pattern recognition.**
  - **Highly structured information**

What is Information Security (2/2)?

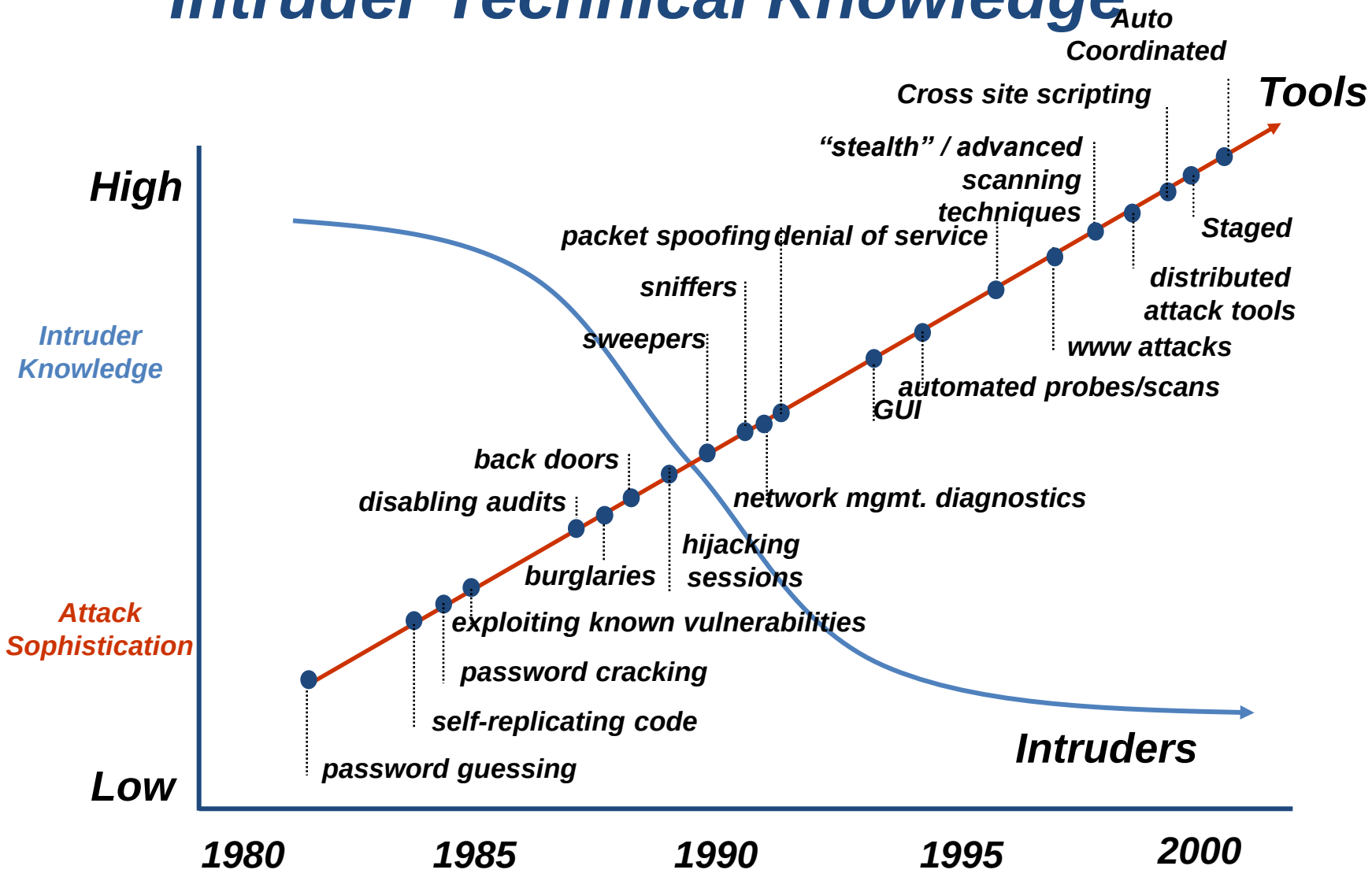
- **Information Security (정보보안, 정보보호)**
  - **Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, modification, or disruption.**
  - **The protection of computer systems and information from harm, theft, and unauthorized use.**
  - **Protecting the Confidentiality, Integrity and Availability (*aka*, CIA) of information.**
  - **Information security is an essential infrastructure technology to achieve highly trustful information-based society.**
  - **Highly information-based company without information security will lose its competitiveness .**

- **What kind of protection?**
  - **Protecting your private important document / computer**
  - **Protecting your communication networks**
  - **Protecting the Internet**
  - **Protection on Cloud computing, etc.**

Taxonomy

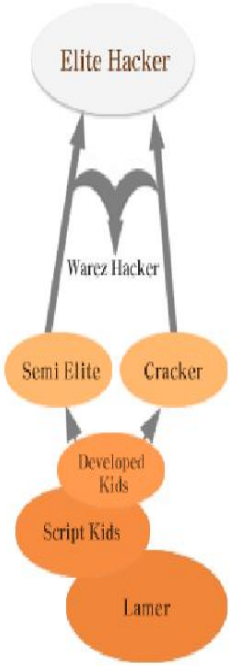

Threats
Attack Tools
Vulnerabilities
Access
Results
Objectives
Hackers
Spies
Terrorists
Corporate Raiders
Professional Criminals
Vandals
Military Forces
User Command
Script or Program
Autonomous Agent
Toolkit
Distributed Tool
Data Tap
Implementation Vulnerability
Design Vulnerability
Configuration Vulnerability
Unauthorized Access
Unauthorized Use
Processes
Files
Data in Transit
Objects in Transit
Invocations In Transit
Corruption of Information
Disclosure of Information
Theft of Service
Denial-of-Service
Challenge, Status
Political Gain
Financial Gain
Damage
Destruction of an Enemy

Attack Sophistication vs. Intruder Technical Knowledge



Hacker's Motivation

1. From a hobby to a profitable industry
2. From annoying to destructive
3. From playing to stealing
4. From simplicity to complexity



Source: http://www.discovery.com/area/technology/hackers/hackers.html

DDoS

- Distributed Denial of Service (DDoS) attacks
- form a significant security threat making networked systems unavailable by flooding with useless traffic using large numbers of "zombies"
- growing sophistication of attacks defense technologies struggling to cope
- Infected PC MS report 2010
  - 14.6/1000 PC in Korea
  - 2.2 Mil. PC in USA

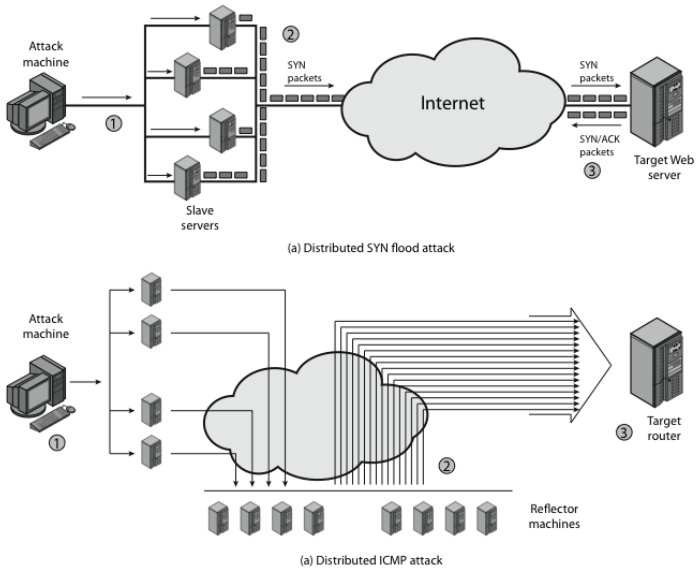
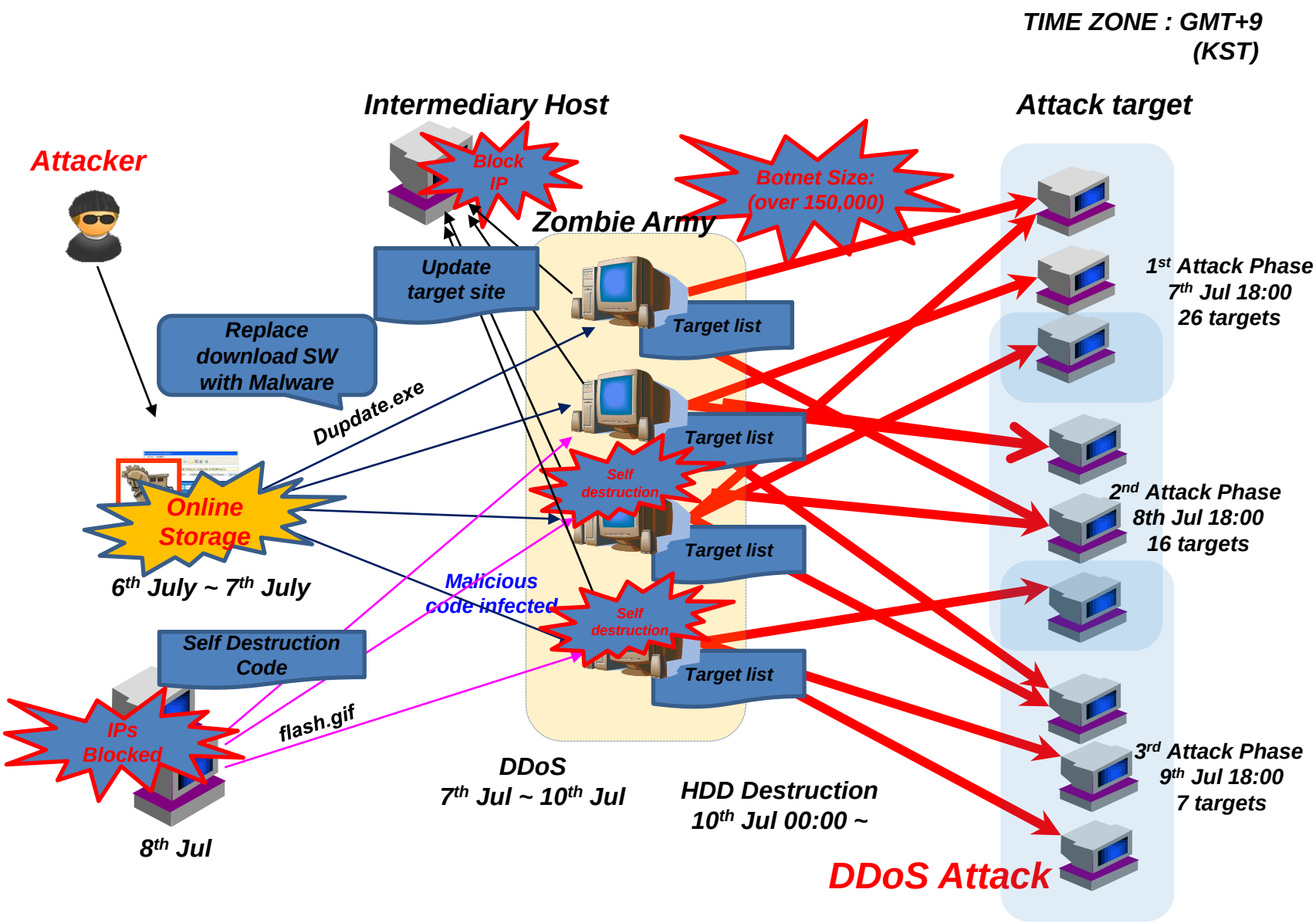


Figure 19.5 Examples of Simple DDoS Attacks

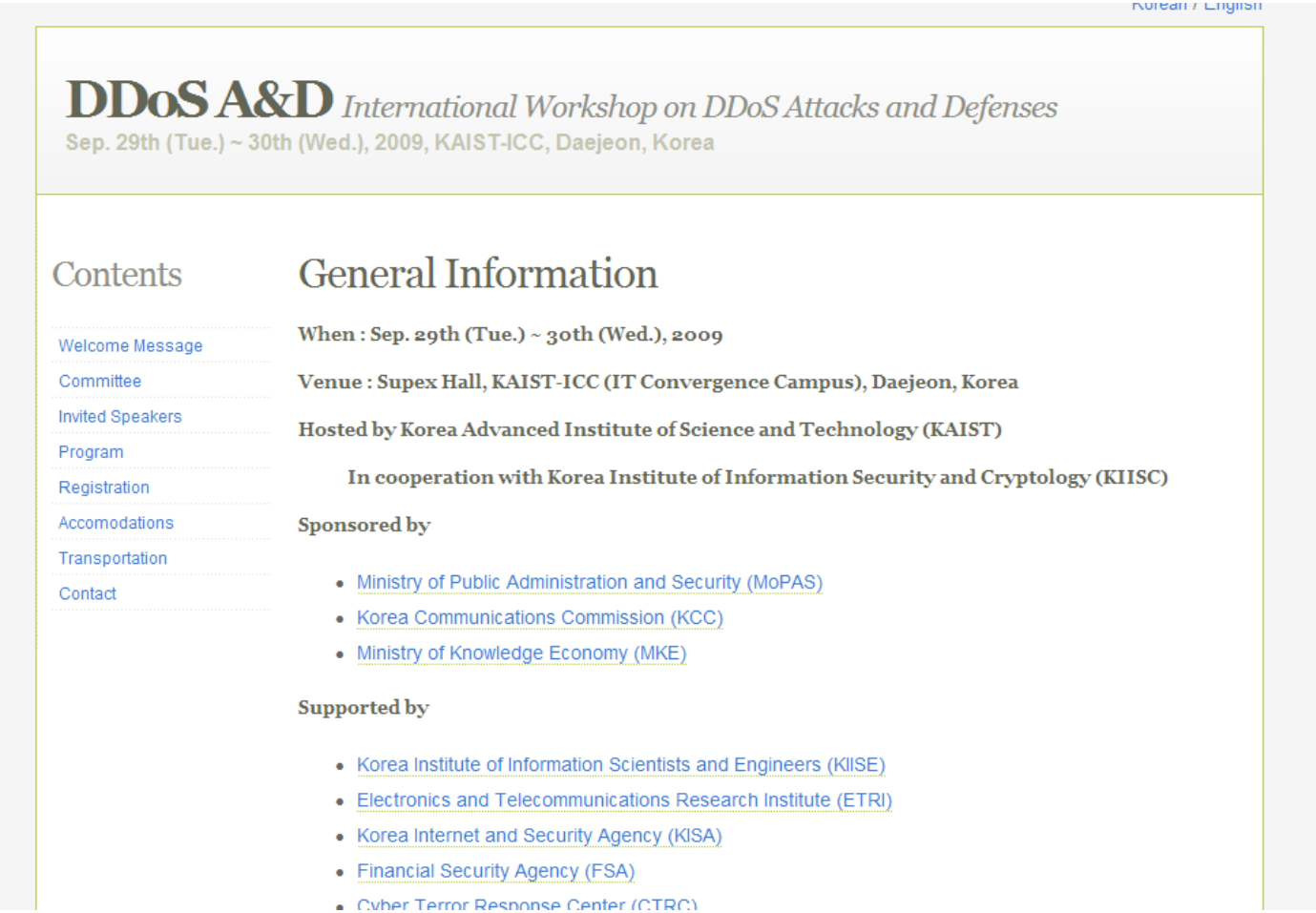
July 7th DDoS attack in Korea (2/1) (2009)



77 DDoS Attack in Korea (2/2)

- **Difficulties to respond**
  - Small amount of attack traffic generated from zombie
    - Less than 50Kbps of network traffic per PC observed
  - Various attack methods
    - Small amount of UDP/ICMP flooding (about 4% of total attack traffic)
    - Small amount of HTTP request (only 1 ~ 25Kbps of traffic measured)
    - http get flooding varying agent information in the HTTP request header made difficult to filter at victim sites
- What did you learn from this attack?

77DDoS A&D



Korean / English

DDoS A&D *International Workshop on DDoS Attacks and Defenses*

Sep. 29th (Tue.) ~ 30th (Wed.), 2009, KAIST-ICC, Daejeon, Korea

Contents

General Information

When : Sep. 29th (Tue.) ~ 30th (Wed.), 2009

Venue : Supex Hall, KAIST-ICC (IT Convergence Campus), Daejeon, Korea

Hosted by Korea Advanced Institute of Science and Technology (KAIST)

In cooperation with Korea Institute of Information Security and Cryptology (KIISC)

Sponsored by

- Ministry of Public Administration and Security (MoPAS)
- Korea Communications Commission (KCC)
- Ministry of Knowledge Economy (MKE)

Supported by

- Korea Institute of Information Scientists and Engineers (KIISE)
- Electronics and Telecommunications Research Institute (ETRI)
- Korea Internet and Security Agency (KISA)
- Financial Security Agency (FSA)
- Cyber Terror Response Center (CTRC)