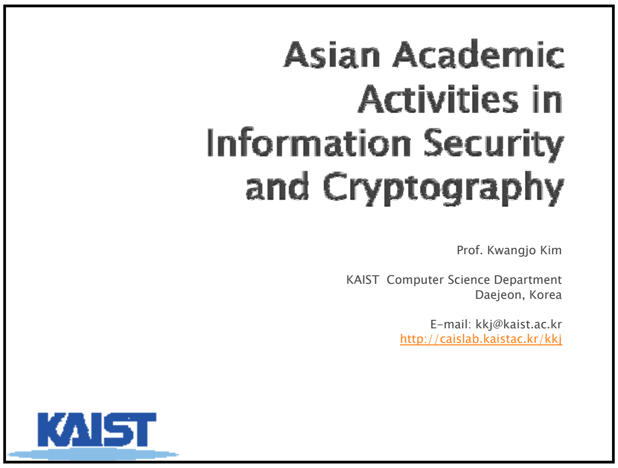
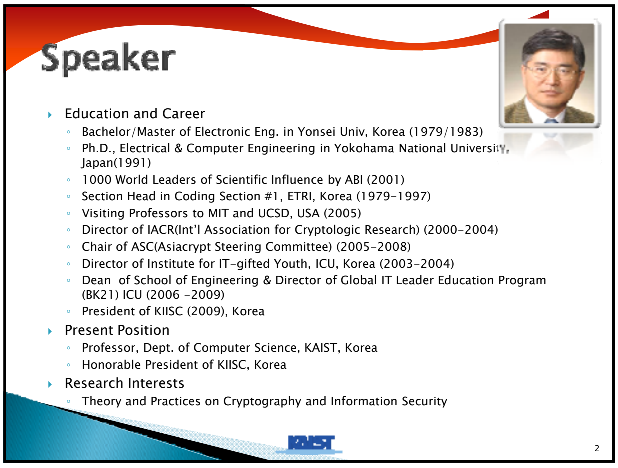


Asian Academic Activities in Information Security and Cryptography

Prof. Kwangjo Kim

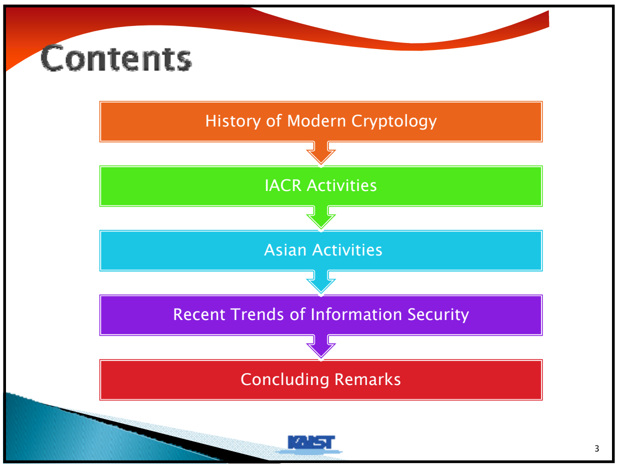
KAIST Computer Science Department
Daejeon, Korea

E-mail: kkj@kaist.ac.kr
http://caislab.kaistac.kr/kkj



Speaker

- Education and Career
  - Bachelor/Master of Electronic Eng. in Yonsei Univ, Korea (1979/1983)
  - Ph.D., Electrical & Computer Engineering in Yokohama National University, Japan(1991)
  - 1000 World Leaders of Scientific Influence by ABI (2001)
  - Section Head in Coding Section #1, ETRI, Korea (1979-1997)
  - Visiting Professors to MIT and UCSD, USA (2005)
  - Director of IACR(Int'l Association for Cryptologic Research) (2000-2004)
  - Chair of ASC(Asiacrypt Steering Committee) (2005-2008)
  - Director of Institute for IT-gifted Youth, ICU, Korea (2003-2004)
  - Dean of School of Engineering & Director of Global IT Leader Education Program (BK21) ICU (2006 -2009)
  - President of KIISC (2009), Korea
- Present Position
  - Professor, Dept. of Computer Science, KAIST, Korea
  - Honorable President of KIISC, Korea
- Research Interests
  - Theory and Practices on Cryptography and Information Security



Contents

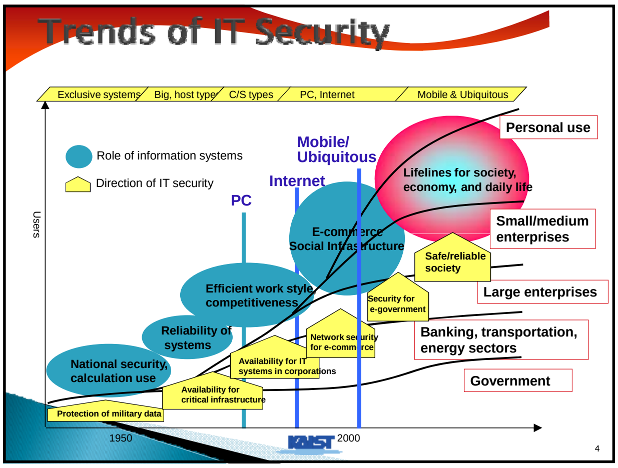
History of Modern Cryptology

IACR Activities

Asian Activities

Recent Trends of Information Security

Concluding Remarks



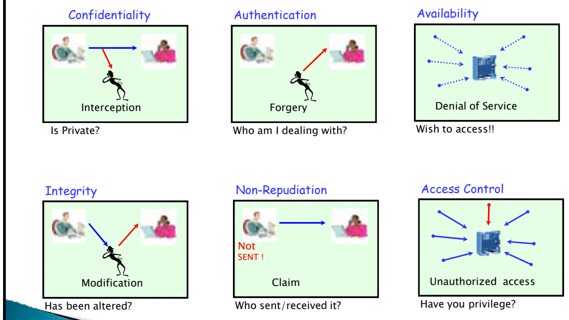
Trends of IT Security

Exclusive systems
Big, host type
C/S types
PC, Internet
Mobile & Ubiquitous
Role of information systems
Direction of IT security
Users
PC
Internet
Mobile/ Ubiquitous
Personal use
Lifelines for society, economy, and daily life
E-commerce Social Infrastructure
Small/medium enterprises
Safe/reliable society
Efficient work style, competitiveness
Security for e-government
Large enterprises
Reliability of systems
Network security for e-commerce
Banking, transportation, energy sectors
National security, calculation use
Availability for IT systems in corporations
Government
Availability for critical infrastructure
Protection of military data
1950
2000

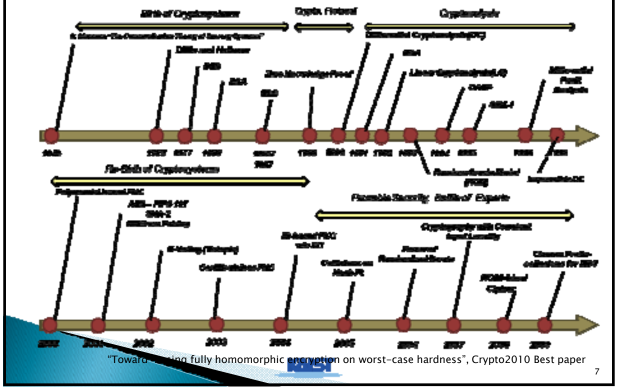
Cryptology = Cryptography + Cryptanalysis

- Cryptography : designing secure cryptosystems
  - Cryptography (from the Greek kryptós and gráphein, “to write”) was originally the study of the principles and techniques by which information could be concealed in ciphers and later revealed by legitimate users employing the secret key.
- Cryptanalysis : analyzing the security of cryptosystems
  - Cryptanalysis (from the Greek kryptós and analýein, “to loosen” or “to untie”) is the science (and art) of recovering or forging cryptographically secured information without knowledge of the key.
- Cryptology : science dealing with information security
  - Science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography and cryptanalysis.

Security Requirements



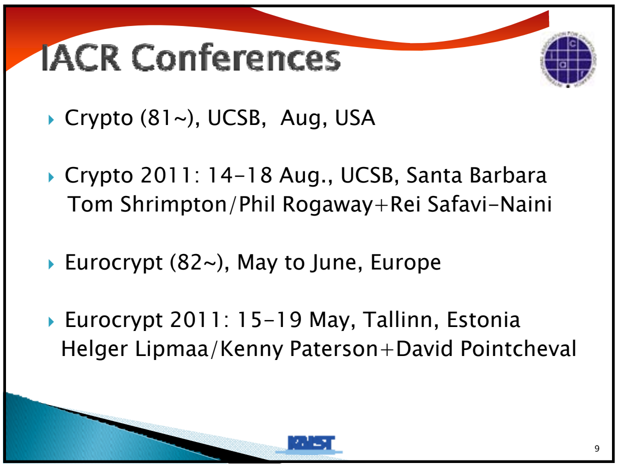
History of Modern Cryptography



“Toward basing fully homomorphic encryption on worst-case hardness”, Crypto2010 Best paper

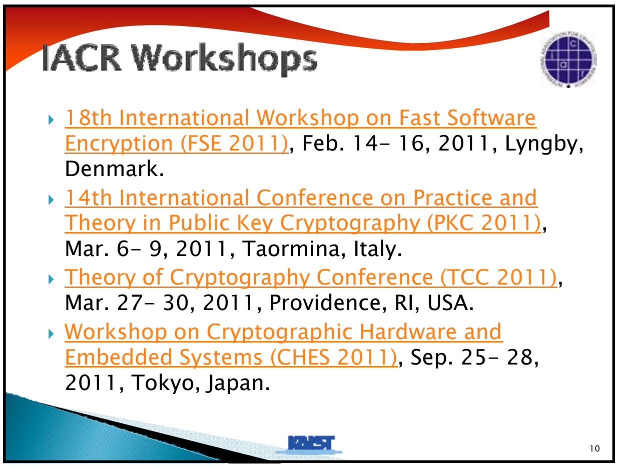
IACR

- International Associations for Cryptologic Research, http://www.iacr.org
- Non-profit organization registered in the USA, 1981
- Purposes : To advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare.
- J. of Cryptology by Springer and IACR Newsletter
- Cryptology eprint Archive: e-print.iacr.org



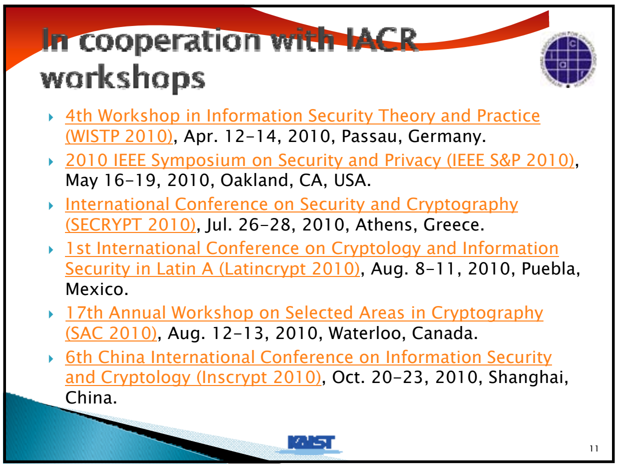
IACR Conferences

- Crypto (81~), UCSB, Aug, USA
- Crypto 2011: 14-18 Aug., UCSB, Santa Barbara
  Tom Shrimpton/Phil Rogaway+Rei Safavi-Naini
- Eurocrypt (82~), May to June, Europe
- Eurocrypt 2011: 15-19 May, Tallinn, Estonia
  Helger Lipmaa/Kenny Paterson+David Pointcheval



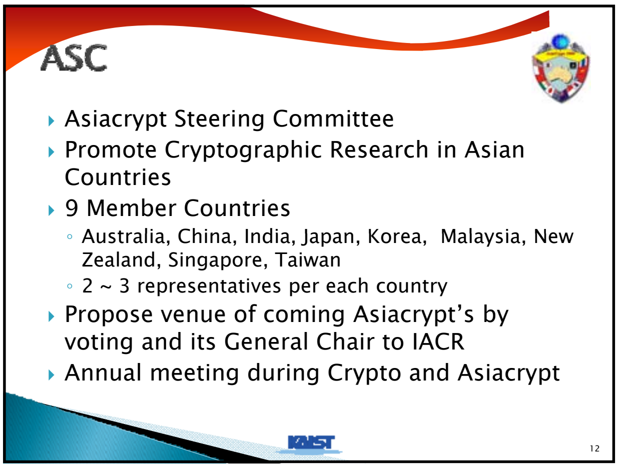
IACR Workshops

- 18th International Workshop on Fast Software Encryption (FSE 2011), Feb. 14- 16, 2011, Lyngby, Denmark.
- 14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011), Mar. 6- 9, 2011, Taormina, Italy.
- Theory of Cryptography Conference (TCC 2011), Mar. 27- 30, 2011, Providence, RI, USA.
- Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), Sep. 25- 28, 2011, Tokyo, Japan.



In cooperation with IACR workshops

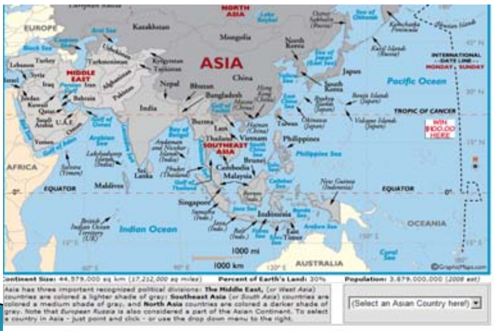
- 4th Workshop in Information Security Theory and Practice (WISTP 2010), Apr. 12-14, 2010, Passau, Germany.
- 2010 IEEE Symposium on Security and Privacy (IEEE S&P 2010), May 16-19, 2010, Oakland, CA, USA.
- International Conference on Security and Cryptography (SECRYPT 2010), Jul. 26-28, 2010, Athens, Greece.
- 1st International Conference on Cryptology and Information Security in Latin A (Latincrypt 2010), Aug. 8-11, 2010, Puebla, Mexico.
- 17th Annual Workshop on Selected Areas in Cryptography (SAC 2010), Aug. 12-13, 2010, Waterloo, Canada.
- 6th China International Conference on Information Security and Cryptology (Inscrypt 2010), Oct. 20-23, 2010, Shanghai, China.



ASC

- Asiacrypt Steering Committee
- Promote Cryptographic Research in Asian Countries
- 9 Member Countries
  - Australia, China, India, Japan, Korea, Malaysia, New Zealand, Singapore, Taiwan
  - 2 ~ 3 representatives per each country
- Propose venue of coming Asiacrypt's by voting and its General Chair to IACR
- Annual meeting during Crypto and Asiacrypt

Where is Asia?



Continent Size: 44,579,000 sq km (17,212,000 sq miles) Percent of Earth's Land: 30% Population: 3,879,000,000 (2008 est)

Asia has three important recognized political divisions: **The Middle East,** (or *West Asia*) countries are colored a lighter shade of gray; **Southeast Asia** (or *South Asia*) countries are colored a medium shade of gray, and **North Asia** countries are colored a darker shade of gray. Note that *European Russia* is also considered a part of the Asian Continent. To select a country in Asia - just point and click - or use the drop down menu to the right.

(Select an Asian Country here!) ▾

Asiacrypt (1/3)

- Before IACR Sponsorship
  - Auscrypt90: Sydney, Australia, Jennifer Seberry/Josef Pieprzyk, Rainer Rueppel, Scott Vanstone
  - Asiacrypt91: Fujiyoshida, Japan, Shigeo Tsujii/Hideki Imai, Ron Rivest
  - Auscrypt92: Queensland, Australia, William Caelli/Jennifer Seberry (Merged into Asiacrypt)
  - Asiacrypt94: Wollongong, Australia, Jennifer Seberry/Josef Pieprzyk
  - Asiacrypt96: Kyongju, Korea, Man Young Rhee/Kwangjo Kim, Tsutomu Matsomuto
  - Asiacrypt98: Beijing, China, Keqin Feng/Kazuo Ohta, Dingyi Pei
  - Asiacrypt99: Singapore, Chao Ping Xing /Kwok Yan Lam, Eiji Okamoto

Asiacrypt (2/3)

- After IACR-Sponsorship
  - Asiacrypt2000: Kyoto, Japan, Tsutomu Matsumoto/Tatsuaki Okamoto
  - Asiacrypt2001: Gold Coast, Australia, Ed Dawson/Colin Boyd
  - Asiacrypt2002: Queenstown, New Zealand, Henry Wolfe/Yuliang Zheng
  - Asiacrypt2003: Taipei, Taiwan, Chin Chen Chang/Chi Sung Laih
  - Asiacrypt2004: Jeju Island, Korea, Kwangjo Kim/Pil Joong Lee
  - Asiacrypt2005: Chennai, India, C. Pandu Rangan/Bimal Roy
  - Asiacrypt2006: Shanghai, China, Dingyi Pei/Xuejia Lai
  - Asiacrypt2007: Sarawak, Malaysia, Raphael Phan/Kaoru Kurosawa
  - Asiacrypt2008: Melbourne, Australia, Lynn Batten/Josef Pieprzyk
  - Asiacrypt2009: Tokyo, Japan, Eiji Okamoto/ Mitsuru Matsui
  - Asiacrypt2010: Singapore, Ling San/Masayuki Abe

Asiacrypt (3/3)

- Asiacrypt2011: 4-8 Dec. Seoul, Korea
  Hyong-Joong Kim/ Dong Hoon Lee+Xiaoyun Wang

- Asiacrypt2012: 2-6 Dec. Beijing, China
  Xuejia Lai/Xioyun Wang

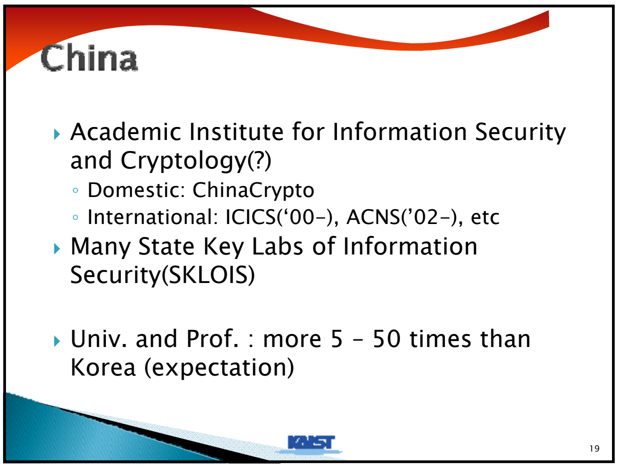
- Asiacrypt2013: Dec.1-5, Abu Dhabi, UAE

Korea

- KIISC (Korea Institute for Information Security and Cryptolgy) established in1990 http://www.kiisc.or.kr
- Domestic conference : CISC-S, CISC-W
- 3 local branches: ChungChung(M), YoungNam(LS), Honam (LW)
- International Annual Conferences: ICISC('97-), WISA('00-), IWDW('02-)
- More than 30 universities and 200 professors

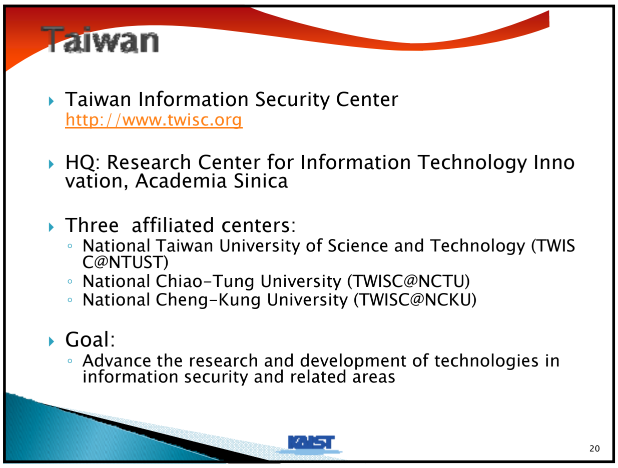
Japan

- ISEC and CSEC groups of IEICE
- Domestic Symposium: SCIS('84-), CSS('02-)
- International Annual Conferences : IWSEC('06-) , Pairing('07-)
  - PKC, Asiacrypt, FSA, CHES, *etc*.
- More than 60 universities and 400 professors including major ICT companies



China

- Academic Institute for Information Security and Cryptology(?)
  - Domestic: ChinaCrypto
  - International: ICICS('00-), ACNS('02-), etc
- Many State Key Labs of Information Security(SKLOIS)
- Univ. and Prof. : more 5 – 50 times than Korea (expectation)



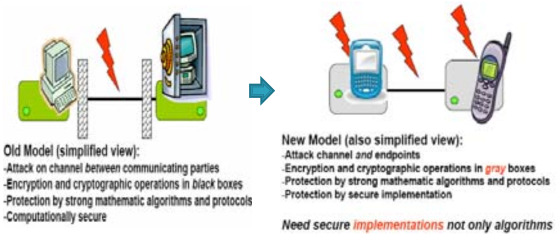
Taiwan

- Taiwan Information Security Center http://www.twisc.org
- HQ: Research Center for Information Technology Innovation, Academia Sinica
- Three affiliated centers:
  - National Taiwan University of Science and Technology (TWISC@NTUST)
  - National Chiao-Tung University (TWISC@NCTU)
  - National Cheng-Kung University (TWISC@NCKU)
- Goal:
  - Advance the research and development of technologies in information security and related areas

Australia

- No Academic Institute like KIISC or IEICE
- Annual International Conference
  - ACISP (95-)
- QUT, Wollongong, Macquarie University, Deakin Univ. , Univ. of Adelaide, *etc.*
- Other Asian Countries
  - India : Indocrypt ('99-)
  - Malaysia : Mycrypt('05-)
  - Vietnam: Vietcrypt('06-)

Model of Attack –Embedded security



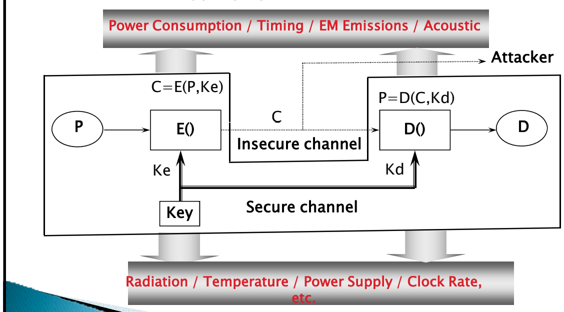
Old Model (simplified view):
-Attack on channel *between* communicating parties
-Encryption and cryptographic operations in *black* boxes
-Protection by strong mathematic algorithms and protocols
-Computationally secure

New Model (also simplified view):
-Attack channel *and* endpoints
-Encryption and cryptographic operations in *gray* boxes
-Protection by strong mathematic algorithms and protocols
-Protection by secure implementation

Need secure implementations not only algorithms

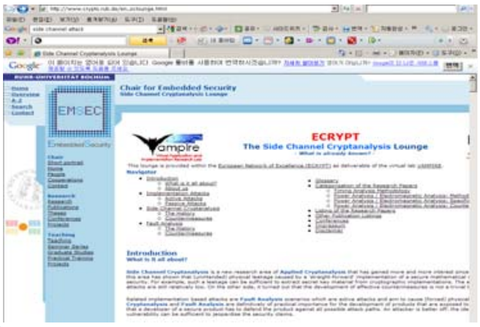
Side Channel

- Traditional Cryptographic Model vs. Side Channel


Power Consumption / Timing / EM Emissions / Acoustic
Attacker
C=E(P,Ke)
P=D(C,Kd)
P
E()
C
Insecure channel
D()
D
Ke
Kd
Key
Secure channel
Radiation / Temperature / Power Supply / Clock Rate, etc.

Let's watch video on SCA http://www.cryptography.com/technology/dpa.html

SCA Crypto Lounge



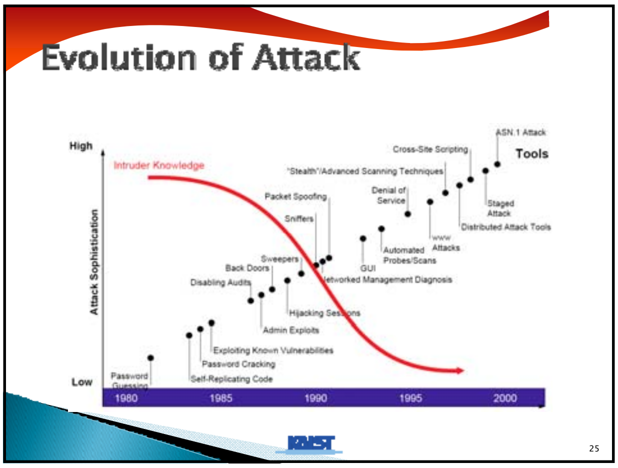
Chair for Embedded Security
Side Channel Cryptanalysis Lounge

ECRYPT
The Side Channel Cryptanalysis Lounge
- What is already known? -

Navigator

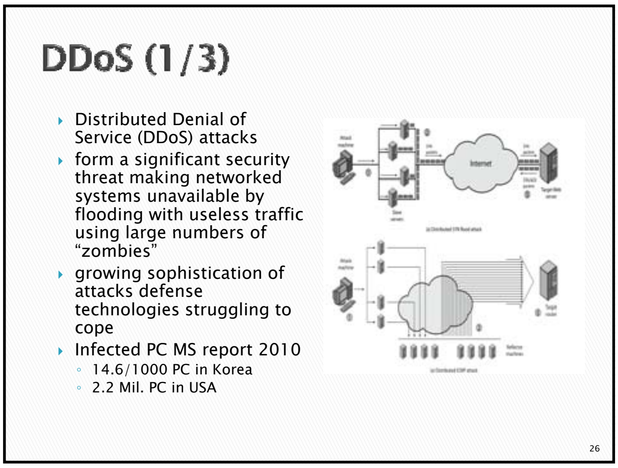
Introduction
What is it all about?

Click for details



Evolution of Attack

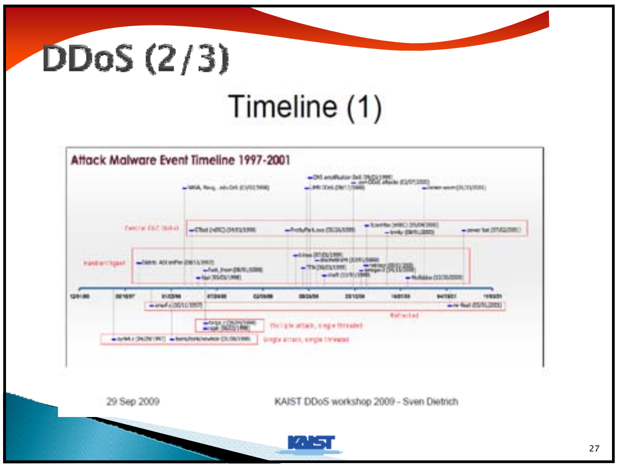
25



DDoS (1/3)

- 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

26



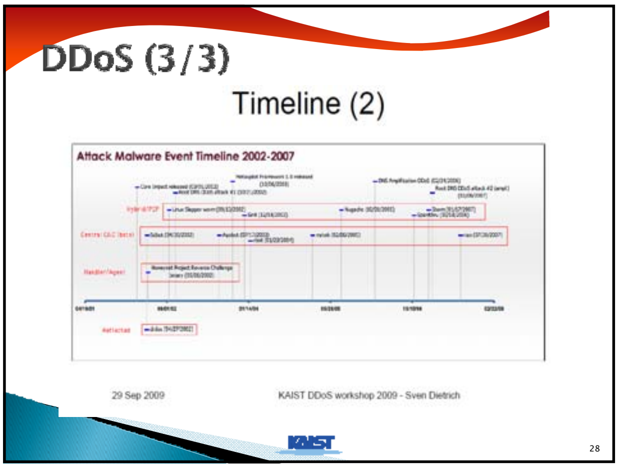
DDoS (2/3)

Timeline (1)

29 Sep 2009

KAIST DDoS workshop 2009 - Sven Dietrich

27



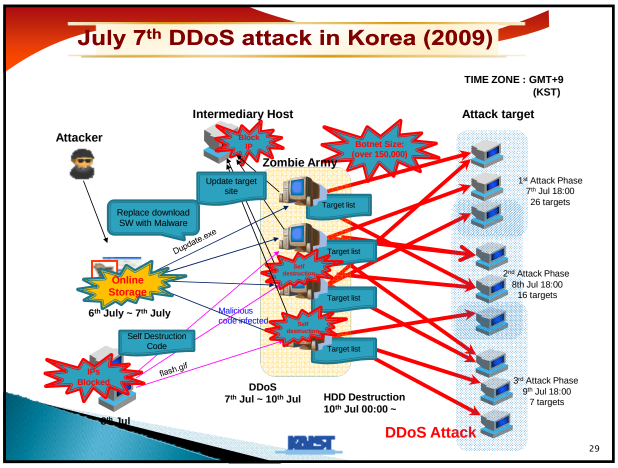
DDoS (3/3)

Timeline (2)

29 Sep 2009

KAIST DDoS workshop 2009 - Sven Dietrich

28



July 7th DDoS attack in Korea (2009)

TIME ZONE : GMT+9 (KST)

Intermediary Host

Attack target

Attacker

Block IP

Botnet Size: (over 150,000)

Zombie Army

Update target site

Replace download SW with Malware

Dupdate.exe

Target list

Target list

Target list

Target list

1st Attack Phase
7th Jul 18:00
26 targets

2nd Attack Phase
8th Jul 18:00
16 targets

3rd Attack Phase
9th Jul 18:00
7 targets

Online Storage

6th July ~ 7th July

Self destruction

Self destruction

Malicious code infected

Self Destruction Code

flash.gif

IPs Blocked

9th Jul

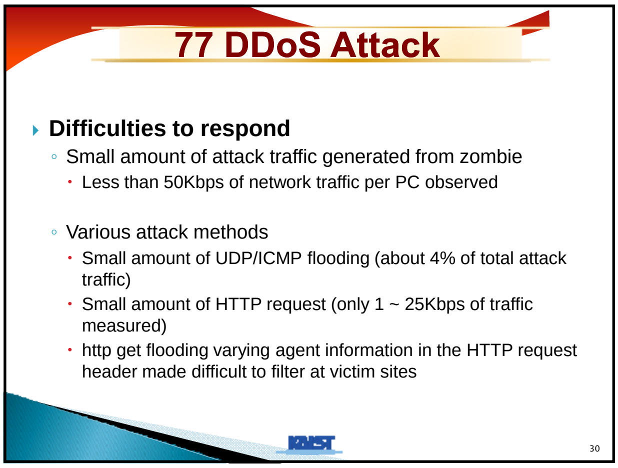
DDoS
7th Jul ~ 10th Jul

HDD Destruction
10th Jul 00:00 ~

DDoS Attack

KAIST

29

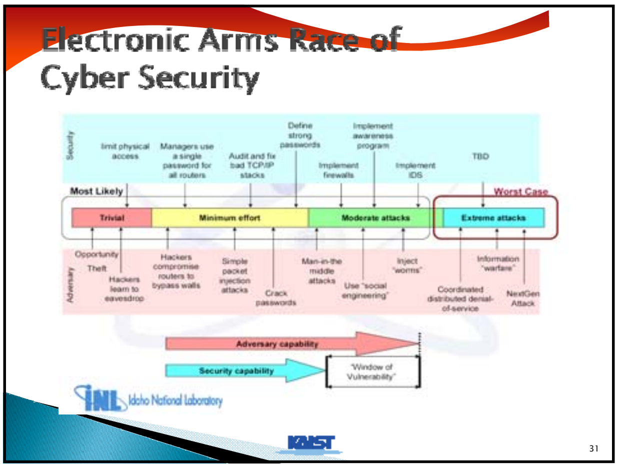


77 DDoS Attack

- **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

KAIST

30



Electronic Arms Race of Cyber Security

Security

limit physical access

Managers use a single password for all routers

Audit and fix bad TCP/IP stacks

Define strong passwords

Implement firewalls

Implement awareness program

Implement IDS

TBD

Most Likely

Worst Case

Trivial

Minimum effort

Moderate attacks

Extreme attacks

Adversary

Opportunity Theft

Hackers learn to eavesdrop

Hackers compromise routers to bypass walls

Simple packet injection attacks

Crack passwords

Man-in-the middle attacks

Use "social engineering"

Inject "worms"

Coordinated distributed denial-of-service

Information "warfare"

NextGen Attack

Adversary capability

Security capability

"Window of Vulnerability"

INL Idaho National Laboratory

KAIST

31

Concluding Remarks

- Theoretical *vs.* Practical Cryptology (or Security)
- One country *vs.* International Collaboration
- Giant Attack Step *vs.* Baby Defense Step
  - Reduce the "window of vulnerability"
- Emerging needs for security and privacy in everywhere

KAIST

32