IS511
Introduction to Information Security

Lecture 1
Introduction

Yongdae Kim

KAIST

Instructor, TA, Office Hours

- Yongdae Kim
  - yongdaek (at) kaist. ac. kr, yongdaek (at) gmail. com
  - Office: N26 201
- Insik Shin
  - insik.shin (at) cs. kaist. ac. kr
  - Office: E3-1 4425
- Seungwon Shin
  - claude (at) kaist. ac. kr, seungwon.shin (at) gmail.com
  - Office: N1 919
- Sangkil Cha
  - sangkilc (at) kaist. ac. kr
  - Office: N5 2319
- Sooel Son
  - sl.son (at) kaist. ac. kr, son.sooel (at) gmail.com
  - Office: N5 2312
- Youngjin Kwon
  - yjkwon (at) kaist. ac. kr
  - Office: E3-1 2312

KAIST

Class web page, e-mail

- http://syssec.kaist.ac.kr/~yongdaek/courses/is511
  - Read the page carefully and regularly!
  - Read the Syllabus carefully.
  - Check calendar.

- E-mail policy (done soon)
  - Profs + TA: IS511_prof@gsis.kaist.ac.kr
  - Profs + TA + Students: IS511_student@gsis.kaist.ac.kr

KAIST

Textbook

- Required
  - Security Engineering by Ross Anderson, Available at http://www.cl.cam.ac.uk/~rja14/book.html.
  - Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (Editor), CRC Press, ISBN 0849385237, (October 16, 1996) Available on-line at http://www.cacr.math.uwaterloo.ca/hac/

KAIST

Goals and Objectives

At the end of the class, you will be able to

- Use a computer system in a secure manner.
- Recognize common vulnerabilities in protocols, designs, and programs.
- Eliminate or minimize the impact of these vulnerabilities.
- Apply the principal security standards in use today to design and build secure applications.
- Apply principles, concepts, and tools from security to your own research.

KAIST

Course Content

- Overview
  - Introduction
  - Attack Model, Security Economics, Legal Issues, Ethics
- User Interface and Psychological Failures
- Cryptography
- Access Control
- Operating System Security
- Software Security
- Network Security
- Mobile Security

KAIST

Evaluation (IMPORTANT!)

- Midterm Exam: 20%
- Final Exam: 25%
- Homework: 20%
- Class Project: 30%
- Participation: 5%

KAIST

Group Projects

- Each project should have some "research" aspect.
- Group size
  - Min 2 Max 5
- Important dates
  - Pre-proposal: Mar 17, 11:59 PM.
  - Full Proposal: Mar 31, 11:59 PM.
  - Midterm report: May 5, 11:59 PM
  - Final report: Jun 9, 11:59 PM. (NO EXTENSION!!).
- Project examples
  - Attack, attack, attack!
  - Analysis
  - Measurement
  - Design

KAIST

Grading

- Absolute (i.e. not on a curve)
  - But flexible ;-)

- Grading will be as follows
  - 93.0% or above yields an A, 90.0% an A-
  - 85% = B+, 80% = B, 75% = B-
  - 70% = C+, 65% = C, 60% = C-
  - 55% = D+, 50% = D, and less than 50% yields an F.

KAIST

And…

- Incompletes (or make up exams) will in general not be given.
  - Exception: a provably serious family or personal emergency arises with proof and the student has already completed all but a small portion of the work.

- Scholastic conduct must be acceptable. Specifically, you must do your assignments, quizzes and examinations yourself, on your own.

KAIST

The Telegraph

HOME | NEWS | WORLD | SPORT | FINANCE | COMMENT | BLOGS | CULTURE | TRAVEL | LIFE
Politics | Obits | Education | Earth | Science | Defence | Health | Scotland | Royal | Celebrities

HOME » NEWS » UK NEWS » CRIME

Thieves placed bugs and hacked onboard computers of luxury cars

The leader of a gang that hacked into the onboard computers of luxury cars and bugged them with GPS tracking devices before stealing them is facing jail.

Bloomberg Our Company | Professional | Anywhere

HOME | QUICK | NEWS | OPINION | MARKET DATA | PERSONAL FINANCE | TECH | POLITICS

McAfee Hacker Says Medtronic Insulin Pumps Vulnerable To Attack

Confirmed: US and Israel created Stuxnet, lost control of it

Stuxnet was never meant to propagate in the wild.

by Nate Anderson - June 1 2012, 6:00am EDT

HACKING | NATIONAL SECURITY | 277

KrebsonSecurity
In-depth security news and investigation

FBI: Smart Meter Hacks Likely to Spread

KAIST

Iran's Flying Saucer Downed U.S. Drone, Engineer Claims

By Spencer Ackerman and Noah Shachtman | January 10, 2012 | 1:00 pm |
Categories: Tinfoil Tuesday

Most CCTV systems are easily accessible to attackers

Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.
+ Follow (512)

SPONSORED BY sas

SECURITY | 7/23/2012 @ 12:17PM | 218,082 views

Hacker Will Expose Potential Security Flaw In Four Million Hotel Room Keycard Locks

The cyberweapon that could take down the internet

› 13:30 11 February 2011 by Jacob Aron
› For similar stories, visit the Computer crime Topic Guide

27th Chaos Communication Congress

We come in peace

Wideband GSM Sniffing

The Telegraph

HOME | NEWS | WORLD | SPORT | FINANCE | COMMENT | BLOGS | CULTURE | TRAVEL | LIFE | FASHI
Politics | Obits | Education | Earth | Science | Defence | Health | Scotland | Royal | Celebrities

HOME » NEWS

Marie Colvin: Syria regime accused of murder in besieged Homs

"the security mindset involves thinking about how things can be made to fail. It involves **thinking like an attacker, an adversary or a criminal**. You don't have to exploit the vulnerabilities you find, but **if you don't see the world that way, you'll never notice most security problems**."
- Bruce Schneier

KAIST

Security Engineering

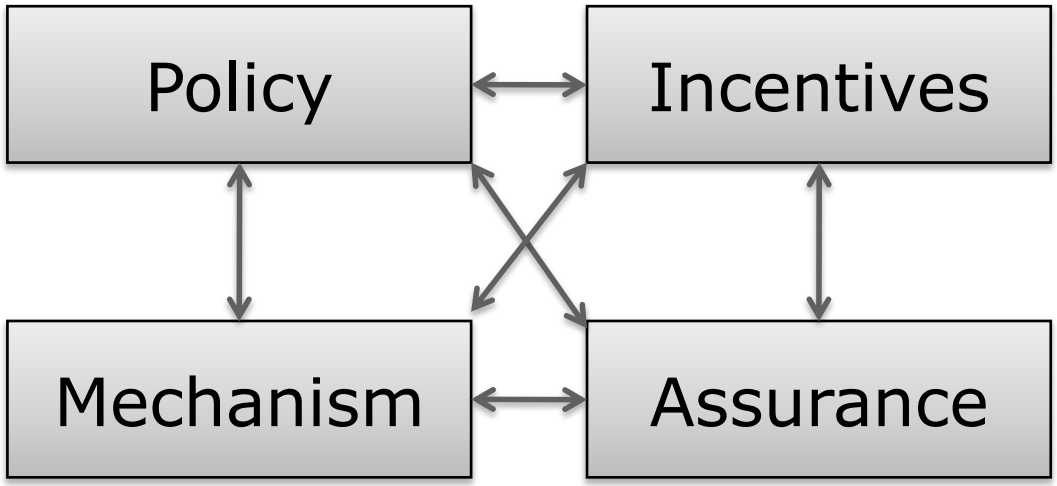
- Building a systems to remain dependable in the face of malice, error or mischance

System	Service	Attack Deny Service, Degrade QoS, Misuse	Security Prevent Attacks
Communication	Send message	Eavesdrop	Encryption
Web server	Serving web page	DoS	CDN?
Computer	;-)	Botnet	Destroy
SMS	Send SMS	Shutdown Cellular Network	Rate Control, Channel separation
Pacemaker	Heartbeat Control	Remote programming and eavesdropping	Distance bounding?
Nike+iPod	Music + Pedometer	Tracking	Don't use it?
Recommendation system	Collaborative filtering	Control rating using Ballot stuffing	?

KAIST

A Framework

- Policy: what you are supposed to achieve
- Mechanism: ciphers, access control, hardware tamper resistance



- Assurance: the amount of reliance you can put on each mechanism
- Incentive: to secure or to attack

KAIST

Example (Airport Security)

- Allowing knife => Policy or mechanism?
- Explosive don't contain nitrogen?
- Below half of the weapons taken through screening?

- Priorities: $14.7 billion for passenger screening, $100 million for securing cockpit door

- Bruce Schneier: Security theatre
  - The incentives on the decision makes favor visible controls over effective ones
  - Measures designed to produce a feeling of security rather than the reality

KAIST

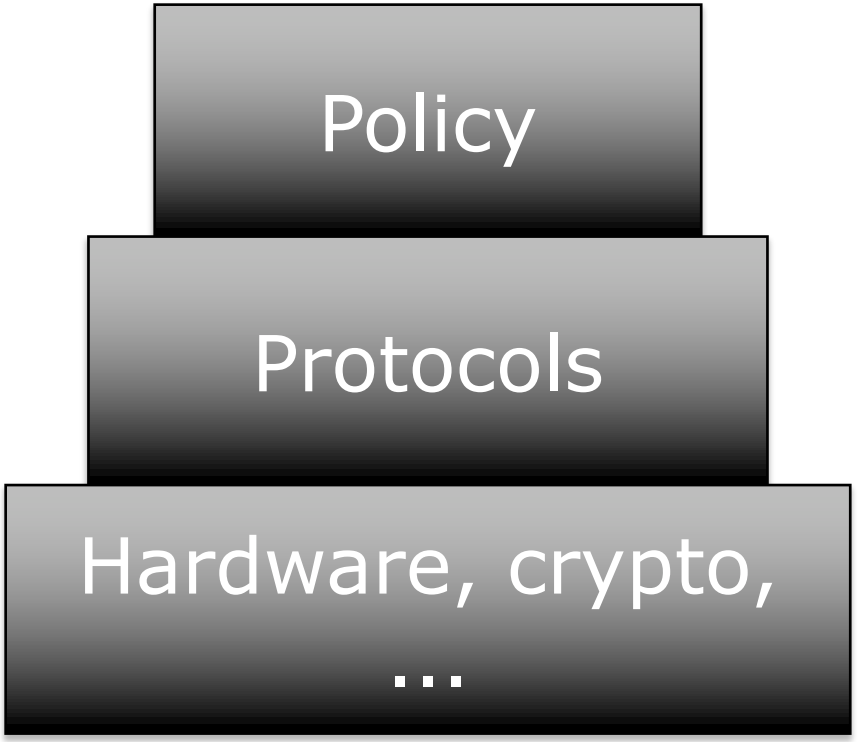
Example (Korean PKI)

- What happened?
- What was wrong?
- What should have been done?

KAIST

Design Hierarchy

- What are we trying to do?
- How?
- With what?



KAIST

Security vs Dependability

- Dependability = reliability + security
- Reliability and security are often strongly correlated in practice

- But malice is different from error!
  - Reliability: "Bob will be able to read this file"
  - Security: "The Chinese Government won't be able to read this file"

- Proving a negative can be much harder …

KAIST

Methodology 101

- Sometimes you do a top-down development. In that case you need to get the security spec right in the early stages of the project
- More often it’s iterative. Then the problem is that the security requirements get detached
- In the safety-critical systems world there are methodologies for maintaining the safety case
- In security engineering, the big problem is often maintaining the security requirements, especially as the system – and the environment – evolve

KAIST

Terminologies

- A *system* can be:
  - a product or component (PC, smartcard,…)
  - some products plus O/S, comms and infrastructure
  - the above plus applications
  - the above plus internal staff
  - the above plus customers / external users

- Common failing: policy drawn too narrowly

KAIST

Terminologies

- A *subject* is a physical person
- A *person* can also be a legal person (firm)
- A principal can be
  - a person
  - equipment (PC, smartcard)
  - a role (the officer of the watch)
  - a complex role (Alice or Bob, Bob deputising for Alice)
- The level of precision is variable – sometimes you need to distinguish ‘Bob’s smartcard representing Bob who’s standing in for Alice’ from ‘Bob using Alice’s card in her absence’. Sometimes you don’t

Terminologies

- *Secrecy* is a technical term – mechanisms limiting the number of principals who can access information
- *Privacy* means control of your own secrets
- *Confidentiality* is an obligation to protect someone else's secrets
- Thus your medical privacy is protected by your doctors' obligation of confidentiality

KAIST

Terminologies

- *Anonymity* is about restricting access to metadata. It has various flavors, from not being able to identify subjects to not being able to link their actions

- An object's *integrity* lies in its not having been altered since the last authorized modification

- *Authenticity* has two common meanings –
  - an object has integrity plus freshness
  - you're speaking to the right principal

KAIST

Terminologies

- A *security policy* is a succinct statement of protection goals – typically less than a page of normal language
- A *protection profile* is a detailed statement of protection goals – typically dozens of pages of semi-formal language
- A *security target* is a detailed statement of protection goals applied to a particular system – and may be hundreds of pages of specification for both functionality and testing

KAIST

Threat Model

- What property do we want to ensure against what adversary?

- Who is the adversary?
- What is his goal?
- What are his resources?
  - e.g. Computational, Physical, Monetary…
- What is his motive?
- What attacks are out of scope?

KAIST

Terminologies

- Attack: attempt to breach system security (DDoS)
- Threat: a scenario that can harm a system (System unavailable)
- Vulnerability: the "hole" that allows an attack to succeed (TCP)
- Security goal: "claimed" objective; failure implies insecurity

KAIST

Goals: Confidentiality

- Confidentiality of information means that it is accessible only by authorized entities
  - Contents, Existence, Availability, Origin, Destination, Ownership, Timing, etc… of:
  - Memory, processing, files, packets, devices, fields, programs, instructions, strings...

KAIST

Goals: Integrity

- Integrity means that information can only be modified by authorized entities
  - e.g. Contents, Existence, Availability, Origin, Destination, Ownership, Timing, etc… of:
  - Memory, processing, files, packets, devices, fields, programs, instructions, strings...

KAIST

Goals: Availability

- Availability means that authorized entities can access a system or service.

- A failure of availability is often called Denial of Service:
  - Packet dropping
  - Account freezing
  - Jamming
  - Queue filling

KAIST

Goals: Accountability

- Every action can be traced to "the responsible party."

- Example attacks:
  - Microsoft cert
  - Guest account
  - Stepping stones

KAIST

Goals: Dependability

- A system can be relied on to correctly deliver service
- Dependability failures:
  - Therac-25: a radiation therapy machine
    - whose patients were given massive overdoses (100 times) of radiation
    - bad software design and development practices: impossible to test it in a clean automated way
  - Ariane 5: expendable launch system
    - the rocket self-destructing 37 seconds after launch because of a malfunction in the control software
    - A data conversion from 64-bit floating point value to 16-bit signed integer value

Interacting Goals

- Failures of one kind can lead to failures of another, e.g.:
  - Integrity failure can cause Confidentiality failure
  - Availability failure can cause integrity, confidentiality failure
  - Etc…

KAIST

Security Assessment

- Confidentiality?
- Availability?
- Dependability?
- "Security by Obscurity:
  - a system that is only secure if the adversary doesn't know the details
  - is not secure!

KAIST

Rules of Thumb

- Be conservative: evaluate security under the best conditions for the adversary
- A system is as secure as the weakest link.
- It is best to plan for unknown attacks.

KAIST

Security & Risk

- We only have finite resources for security…

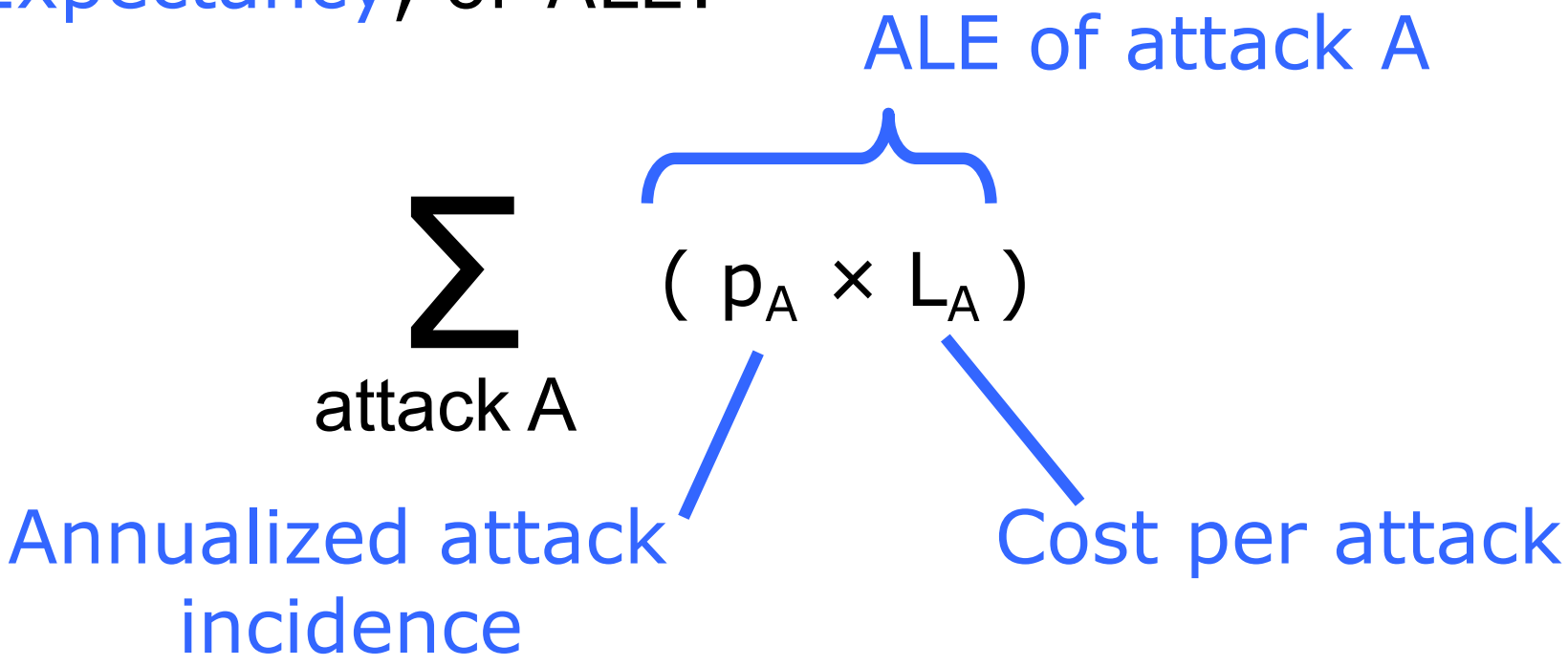
Product A	Product B
Prevents Attacks: U,W,Y,Z	Prevents Attacks: V,X
Cost $10K	Cost $20K

- If we only have $20K, which should we buy?

KAIST

Risk

- The risk due to a set of attacks is the expected (or average) cost per unit of time.
- One measure of risk is Annualized Loss Expectancy, or ALE:



KAIST

Risk Reduction

- A defense mechanism may reduce the risk of a set of attacks by reducing L_A or p_A. This is the gross risk reduction (GRR):

$$\sum_{\text{attack A}} (p_A \times L_A - p'_A \times L'_A)$$

- The mechanism also has a cost. The net risk reduction (NRR) is GRR – cost.

KAIST

Patco Construction vs. Ocean Bank

- Hacker stole ~$600K from Patco through Zeus
- The transfer alarmed the bank, but ignored

- "substantially increase the risk of fraud by asking for security answers for every $1 transaction"
- "neither monitored that transaction nor provided notice before completed"
- "commercially unreasonable"
  - Out-of-Band Authentication
  - User-Selected Picture
  - Tokens
  - Monitoring of Risk-Scoring Reports

KAIST

Auction vs. Customers

- Auction의 잘못
  - 개인정보 미암호화
  - 해킹이 2일에 걸쳐 일어났으나 몰랐던점
  - 패스워드
    - 이노믹스 서버 관리자 'auction62'
    - 데이터베이스 서버 관리자 'auctionuser'
    - 다른 데이터베이스 서버 관리자 'auction'
  - 서버에서 악성코드와 트로이목마 발견

- 무죄
  - 해커의 기술이 신기술이었다, 상당히 조직적이었다.
  - 옥션은 서버가 많아서 일일이 즉각 대응하기는 어려웠다,
  - 당시 백신 프로그램이 없었거나, 오작동 우려가 있었다.
  - 소기업이 아닌 옥션으로서는 사용하기 어려운 방법이었다.
  - 과도한 트래픽이 발생한다.

KAIST

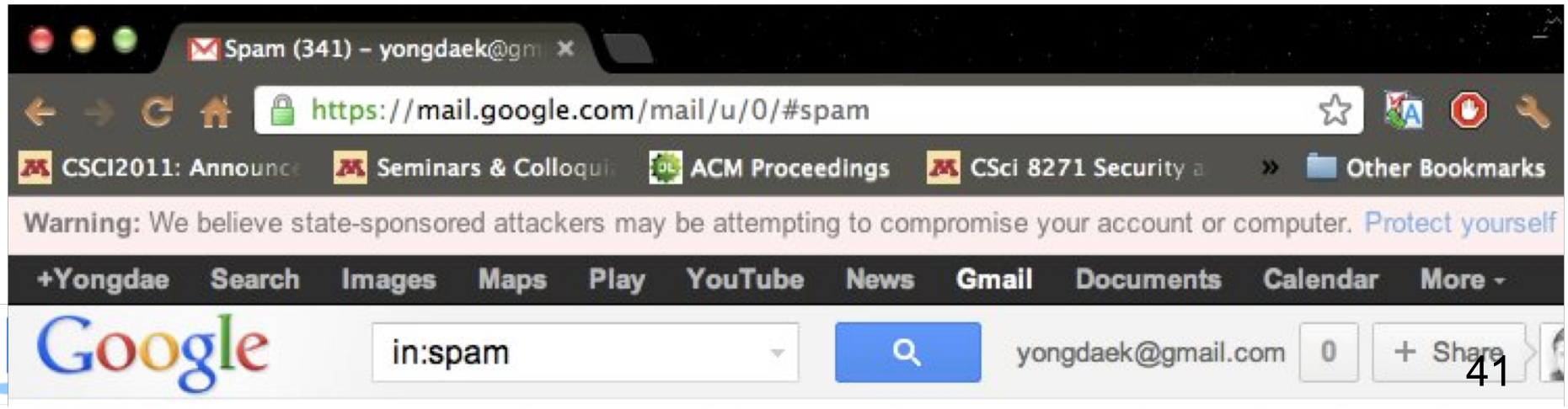
Who are the attackers?

- No more script-kiddies
- State-sponsored attackers
  - Attacker = a nation!
- Hacktivists
  - Use of computers and computer networks as a means of protest to promote political ends
- Hacker + Organized Criminal Group
  - Money!
- Researchers

KAIST

State-Sponsored Attackers

- 2012. 6: Google starts warning users who may be targets of government-sponsored hackers
- 2010 ~: Stuxnet, Duqu, Flame, Gauss, …
  - Mikko (2011. 6): A Pandora's Box We Will Regret Opening
- 2010 ~: Cyber Espionage from China
  - Exxon, Shell, BP, Marathon Oil, ConocoPhillips, Baker Hughes



Hacktivists

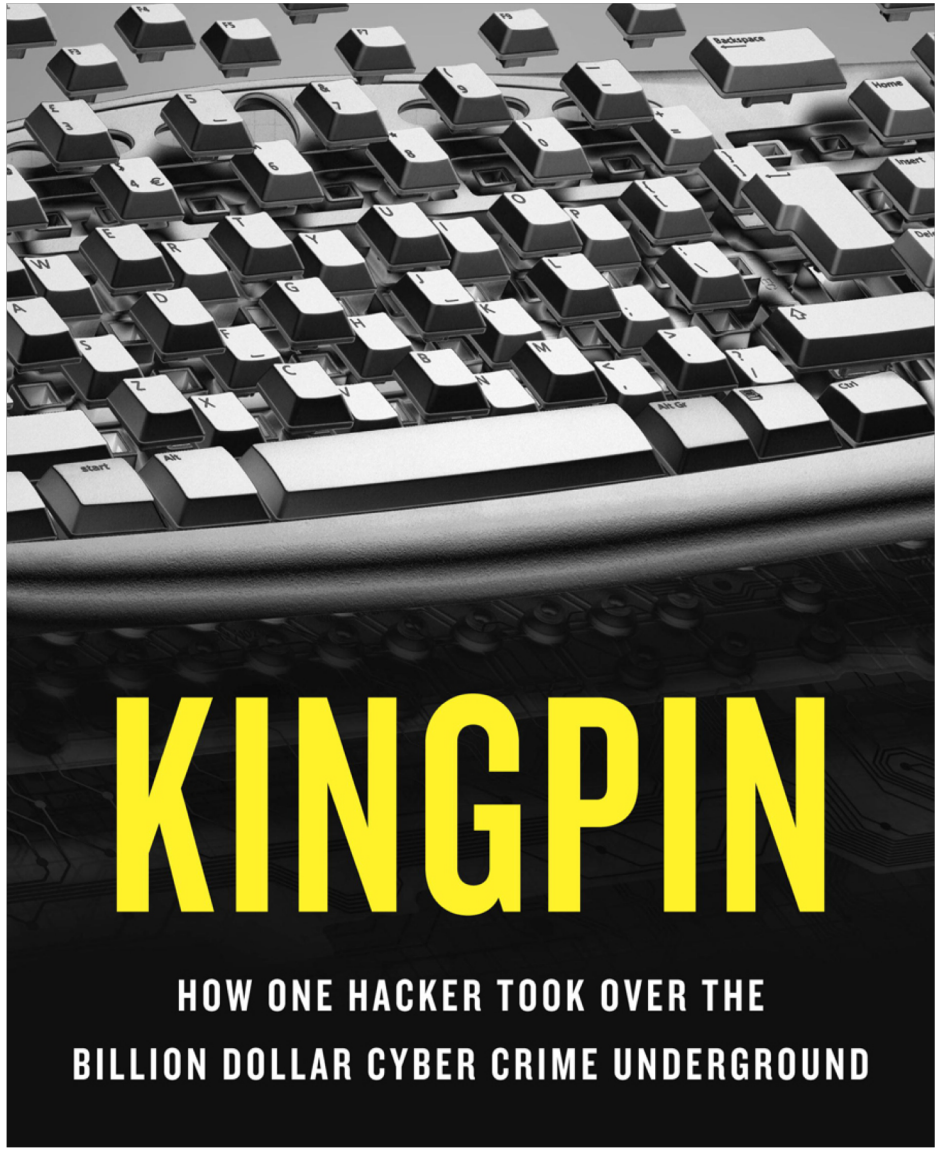
- promoting expressive politics, free speech, human rights, and information ethics
- Anonymous
  - To protest against SOPA, DDoS against MPAA, RIAA, FBI, DoJ, Universal music
  - Attack Church of Scientology
  - Support Occupy Wall Street
- LulzSec
  - Hacking Sony Pictures (PSP jailbreaking)
  - Hacking Pornography web sites
  - DDoSing CIA web site (3 hour shutdown)

KAIST

Hacker + Organized Crime Group

- No more script kiddies
- Hackers seek to earn money through hacking
- Traditional financial crime groups have difficulty with technology improvement

- Hacker + Criminals!
- HaaS = Hacking-as-a-Service



KAIST

Security Researchers

- They tried to save the world by introducing new attacks on systems

- Examples
  - Diebold AccuVote-TS Voting Machine
  - APCO Project 25 Two-Way Radio System
  - Kad Network
  - GSM network
  - Pacemakers and Implantable Cardiac Defibrillators
  - Automobiles, …

KAIST

Bug Bounty Program

- Evans (Google): "Seeing a fairly sustained drop-off for the Chromium"
- McGeehan (Facebook): The bounty program has actually outperformed the consultants they hire.
- Google: Patching serious or critical bugs within 60 days
- Google, Facebook, Microsoft, Mozilla, Samsung, …

Nations as a Bug Buyer

- ReVuln, Vupen, Netragard: Earning money by selling bugs
- "All over the world, from South Africa to South Korea, business is booming in what hackers call zero days"
- "No more free bugs."
- 'In order to best protect my country, I need to find vulnerabilities in other countries'
- Examples
  - Critical MS Windows bug: $150,000
  - Vupen charges $100,000/year for catalog and bug is sold separately
  - a zero-day in iOS system sold for $500,000
  - Brokers get 15%.

Sony vs. Hackers

2000.8 Sony Exec: do whatever to protect re

2005.10 Russinovich: Sony

2007.1 FTC: Reimburse

2011.1 Hotz: PS3 Hack

2011.4 Sony, Hotz: settled

2011.4 PSN: Hacked

2011.3 $36.27 per share

2011.5 Son: ½ day recov

2011.5 ny Exec: ologized

2011.6 $24.97 per share

2011.5 SOE: Hacked

2011.5 Sony: outage cost $171M

2011.6 Sony: Fired security staff

2012.3 Anon: Posted Unreleased Michael Jackson video