Operating Systems & Security

(478550)

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Fall, 2015

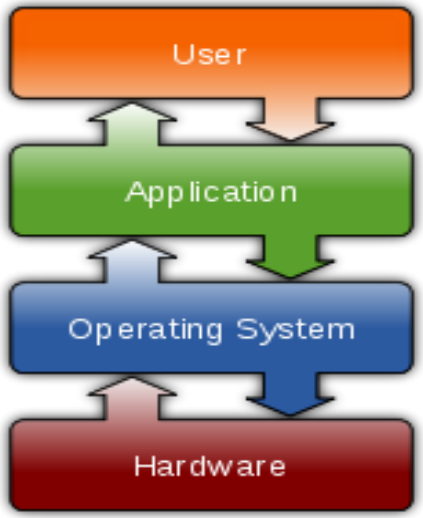
sjcho at dankook.ac.kr

Many slides taken from Textbook (Its site), The Korea Herald, and Web sites

- **Textbook site**
  - **http://williamstallings.com/ComputerSecurity/**
  - **http://www.pearsonhighered.com/educator/academic/product/1,,0132775069,00.html**

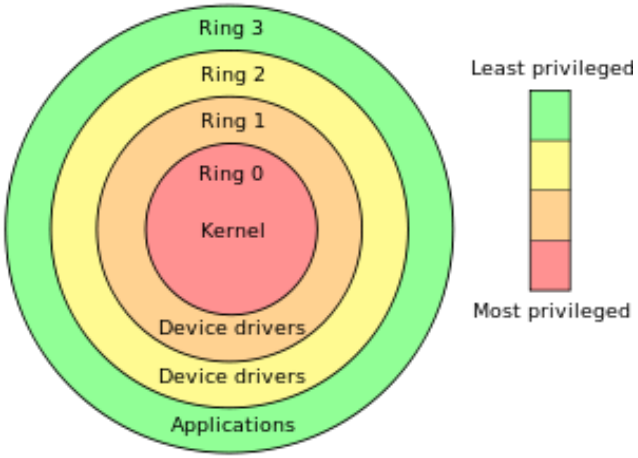
Many photos in presentation licensed from google images or wikipedia

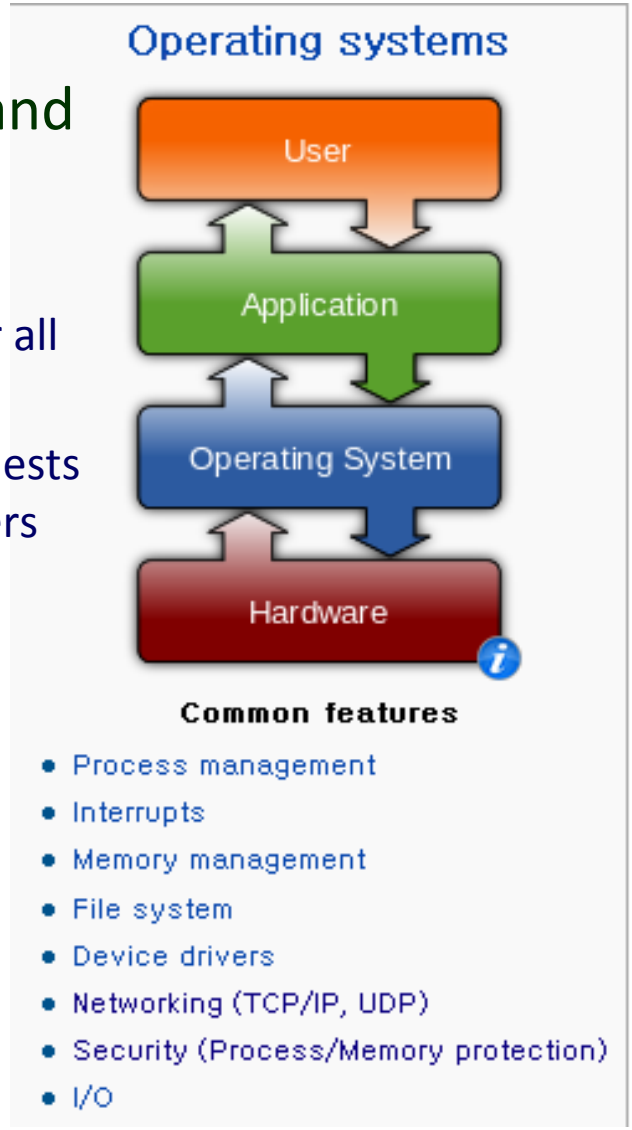
What is Operating Systems?



Operating Systems

- a collection of software that manages computer hardware **resources** and provides common services for computer programs
  - Kernel provides the most basic level of control over all of the computer's hardware devices
  - OS must be capable of distinguishing between requests which should be allowed to be processed, and others which should not be processed





What is Computer Security?

Which types of threats are there?

What Will You Learn in This Class?

- A practical introduction to a broad range of computer security topics/issues related with OS
  - Security vulnerabilities & threats, Security goals
  - Trusted Operating Systems
- How to exploit vulnerabilities & defend against attacks
  - Practical training (Practical exercise)
  - Level up practice (Hackerschool), Buffer overflow, Ret2Libc, Race condition, Simple Password cracking, DLL injection, and Hooking under Linux or Windows systems, Rootkits
  - SELinux: $sudo setenforce 1, $getenforce, chcon, restorecon, runcon, secon …
- Solving security problems in system software areas
  - Team based problem solving (Team based projects)
  - Associated with capstone design

Threat Modeling

- Risks or Threats under Internet & Mobile

- MS STRIDE Model
  - Spoofing
    - Password cracking
  - Tampering
    - Altering information
  - Repudiation
  - Information Disclosure
    - Stealing information
  - Denial-of-Services (DoS)
    - Deleting information, Crashing systems
  - Elevation of Privileges

Information Disclosure & DoS

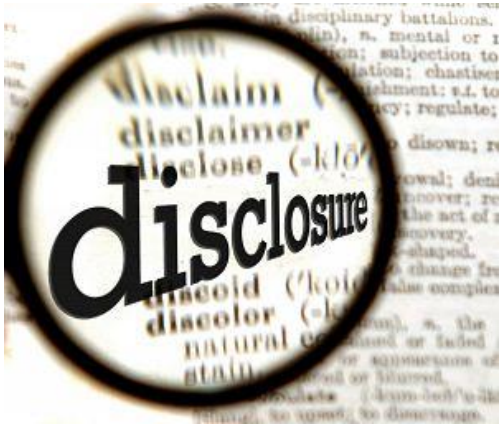
- **KB Financial chief may face punishment over data leak: regulator (Feb. 18, 2014)**
  - Last month, the Financial Services Commission revealed that some 20 million clients' personal data had been leaked from three credit card firms -- KB Kookmin, NH Nonghyup and Lotte – as well as Kookmin Bank, which shared customer data with its affiliated card firm.
  - Cyber terrorism, a global threat

Major cyber attacks in South Korea

Date	Target organization
July 2009	Cheong Wa Dae, Naver
March 2010	Shingsegae Mall
March 2011	Cheong Wa Dae, National Intelligence Service
April 2011	NongHyup
July 2011	SK Communications
Nov. 2011	Nexon
March 2012	SK Telecom, KT
July 2012	KT
March 2013	KBS, MBC, YTN, NongHyup, Shinhan Bank
June 2013	Cheong Wa Dae

Data Theft

- **Massive data thefts spark review of national ID system**
  - it is mulling over the overhaul of the 13-digit resident registration number, or RRN, which contains personal information about every single Korean, such as birthdate, birthplace, sex and other details.
  - RRNs are routinely required for a wide array of daily activities such as creating bank accounts, buying cell phones or accessing online shopping malls.
  - Government officials are considering assigning every citizen an "RRN issuance number" to replace the RRNs



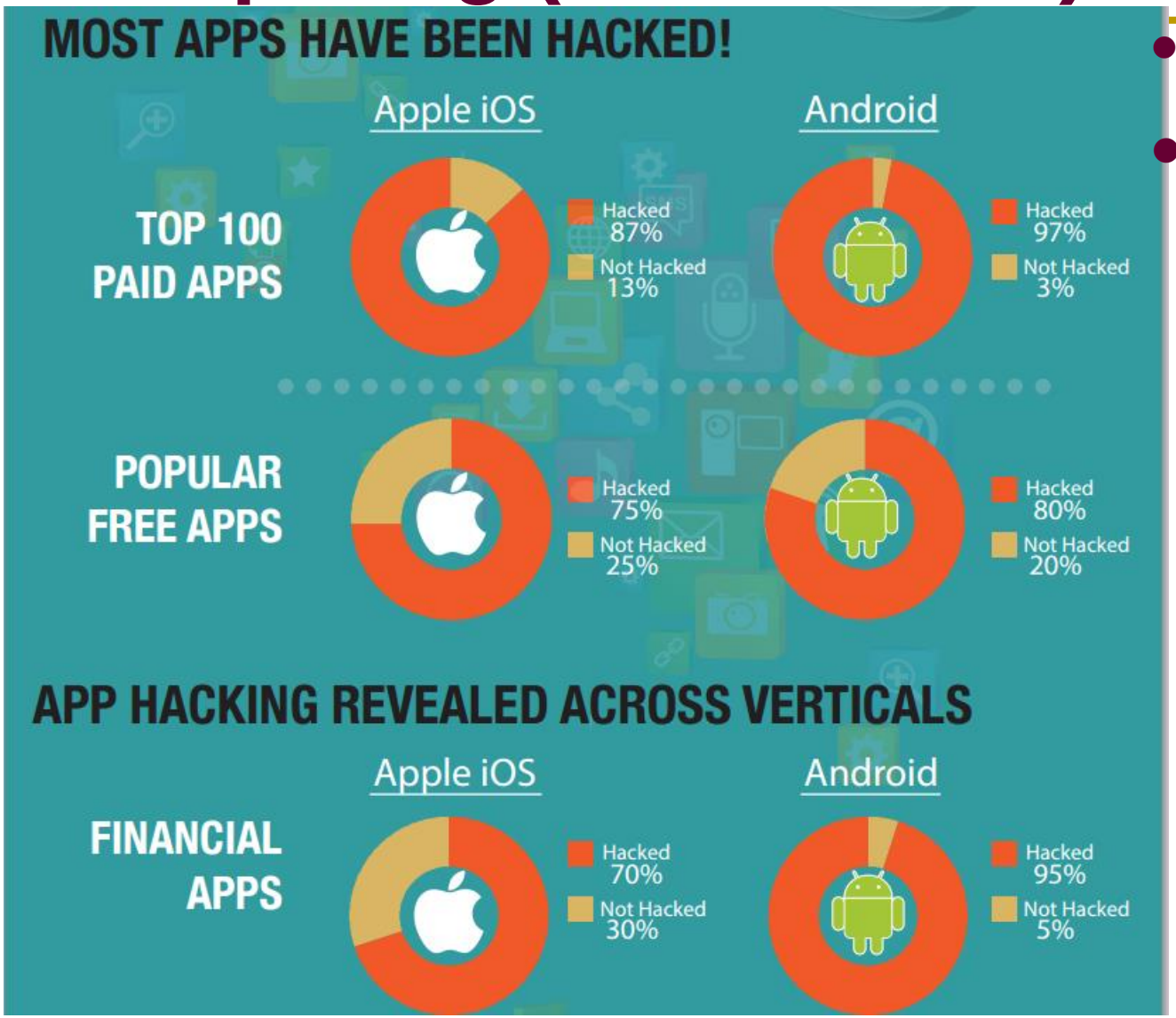
Personal Information Theft

- 15 million clients' data believed stolen (2014-01-19)
- CJ Mall user info hacked, too (2014-01-20)
- Class action suits over data leak may cost 3 card firms 170 bln won (Feb. 3, 2014)
  - The three credit card firms hit by recent massive data leaks may have to pay up to 170 billion won ($158 million) in compensation to their clients to settle class action lawsuits, data showed on Monday.
  - The credit card firms are already suffering losses as millions of their clients have canceled their plastic cards or asked for new ones, which will cost them up to 40 billion won.
  - In February 2013, SK Communications Co., the operator of local search engine Nate, was ordered by a court to pay 200,000 won each in compensation to 2,882 users for failing to protect customer data.

Information Theft

- 74,000 affected after company laptops stolen, Coca-Cola says (2014-01-26)
- Adobe says hackers stole code, data on 2.9 million customers (2013-10-04)
  - hackers broke into its networks and stole personal data on 2.9 million customers and source code for popular products including Acrobat and ColdFusion
- S. Korea request U.S. explanation on new spying claims
  - U.S. confirms S. Korean president not among eavesdropping

Tampering (= Alteration)



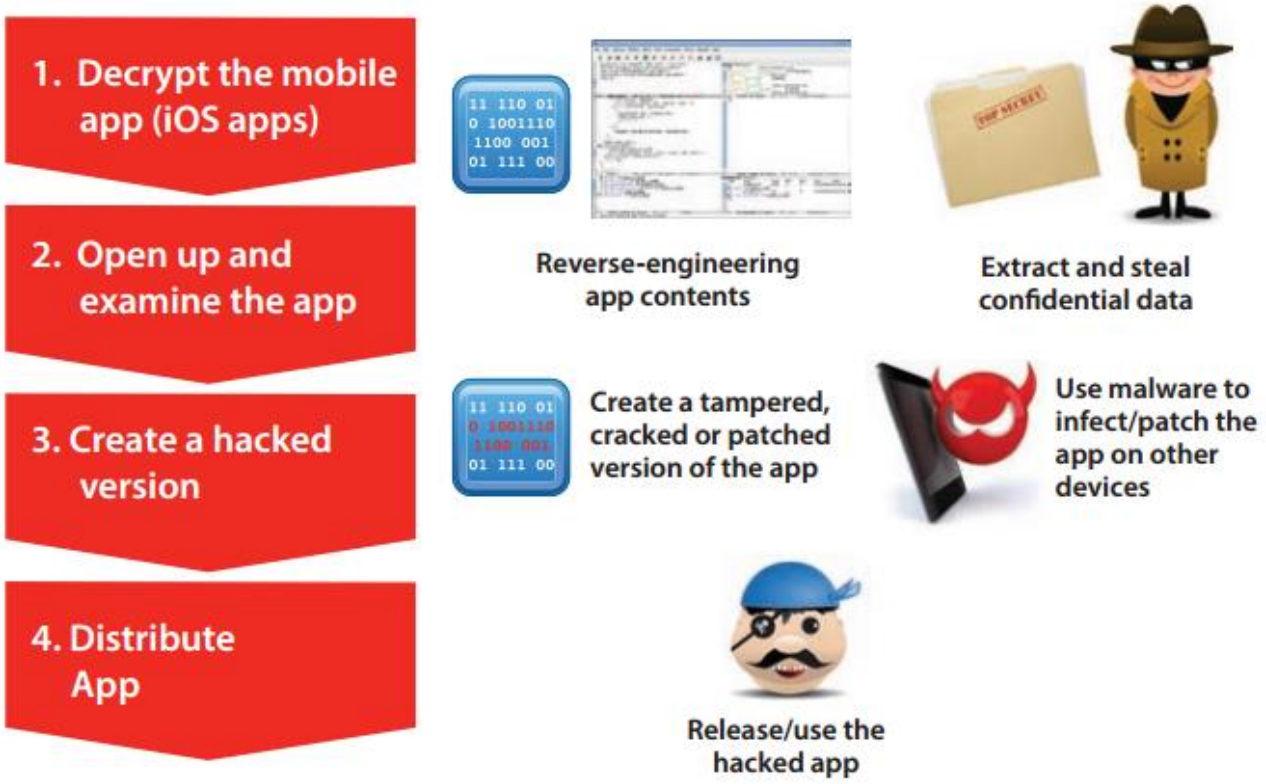
- **State of Mobile App Security – Vol. 3, 2014**
- "Anatomy of an App Hack" involves three steps:
  1. Define the exploit and attack targets
     - Compromise security
  2. Reverse-engineer the code
     - Debugging, tracing, memory analysis
     - Disassembly, de-compilation
  3. Tamper with the code;
     - Modify targeted parts of the code
- this process is made easy with widely available free or low-cost hacking tools.

https://www.arxan.com/wp-content/uploads/assets1/pdf/state_of_security_2014_11.pdf

Tampering: App Hacking

A Few Simple Steps and Readily Available Tools Make It Fairly Easy To Hack

Anatomy of an App Hack

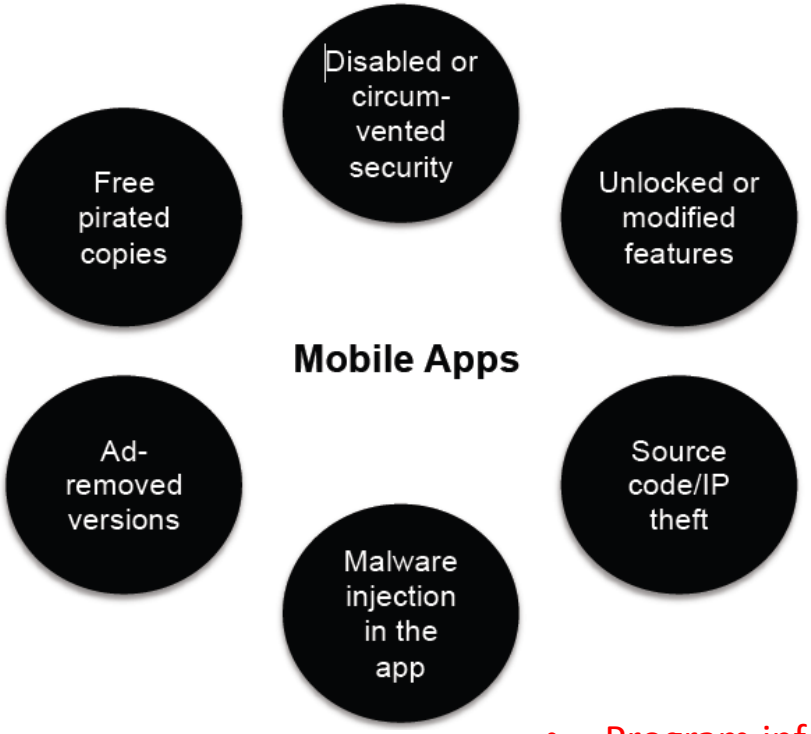


Hackers will leverage widely available tools to perform these steps. See the Appendix for a list of tools readily available for legitimate uses, but are often abused by hackers/cybercriminals to create clones and/or malicious apps.

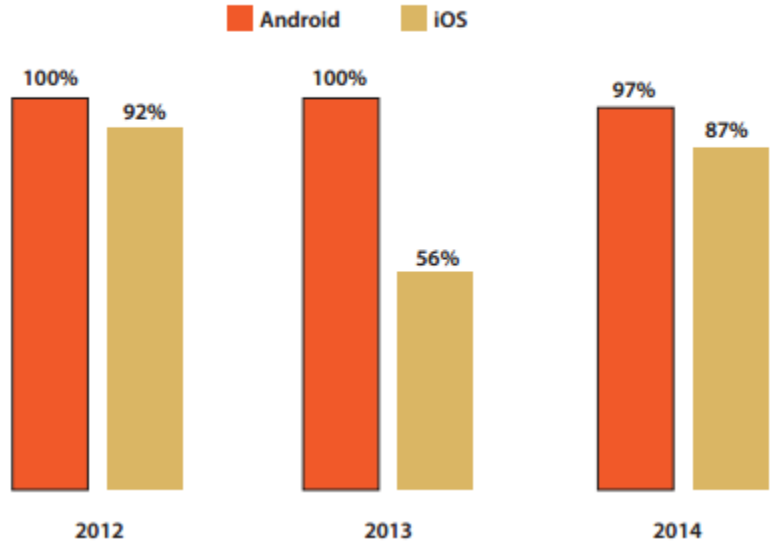
Tampering (= Alteration)

- **State of Security in the App Economy:** "Mobile Apps under Attack", 2012
- **State of Mobile App Security:** "Apps under Attack", 2014 **(Source: www.arxan.com)**

Types of Hacking Attacks faced by Mobile Apps



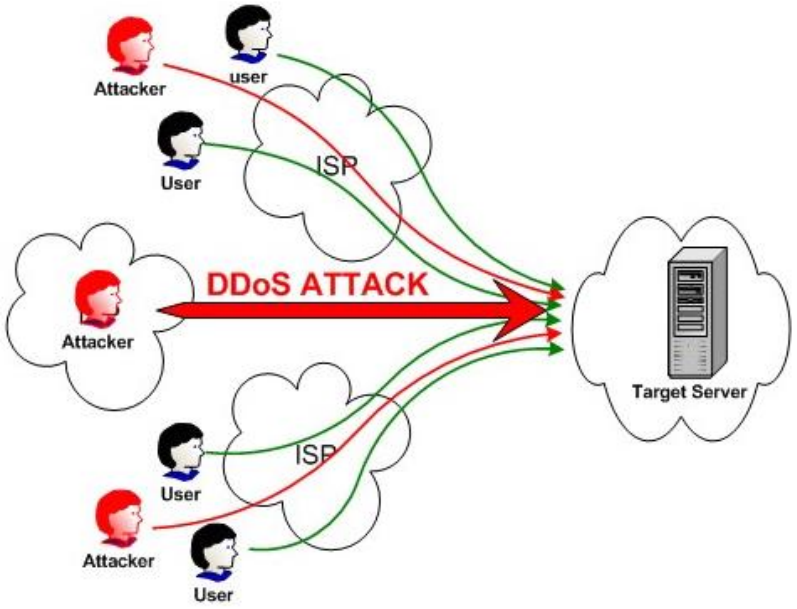
Percentage of Hacked Apps

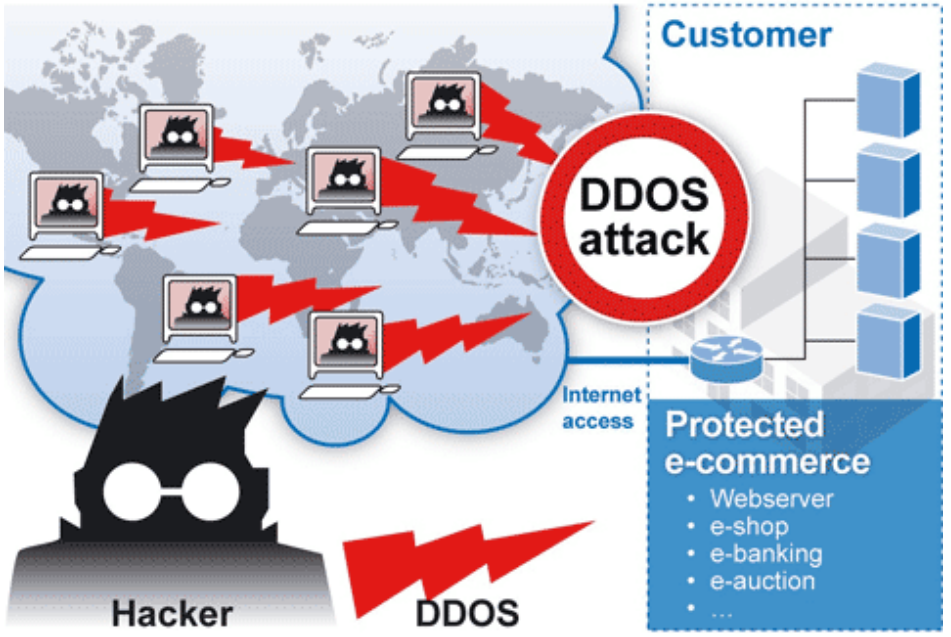


- Program infected with virus, DLL injection, Modified Ret by BoF

Denial-of-service (DoS)

- **S. Korean websites hit by DDos attack: AhnLab (2013-10-25)**
  - South Korea's largest anti-virus software firm AhnLab Inc. said Friday it detected *distributed denial-of-service* (DDoS) attacks on local companies, sounding alarm bells for their cyber security.
  - Sixteen websites operated by 13 South Korean firms, including No. 2 portal operator Daum Communications Corp. and game developer Nexon Korea Corp., experienced cyber attacks Thursday, AhnLab said.



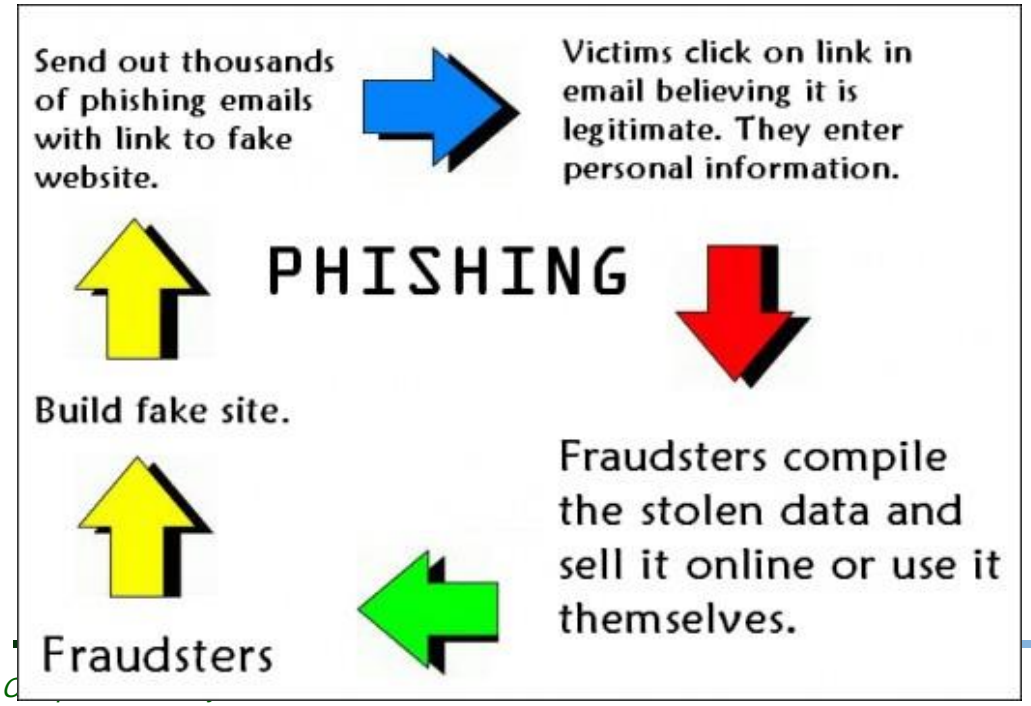


Spoofing = Masquerading

- Fake apps disguised as BBM ruin roll-out of messaging app on Android, iOS
  - BBM is BlackBerry's popular messaging platform
- New Android malware disguised as security app
  - Android Security Suite Premium -- loaded with Zeus variant ZitMo -- is a threat to companies given the bring-your-own-device (BYOD) trend
  - The latest Zeus malware masquerades as a premium security app to lure people into downloading the Trojan
  - The fake security app, called the Android Security Suite Premium, first appeared in early June with newer versions released since then
- Spreading malicious files masqueraded as Facebook image
- Intent Spoofing on Android
- When Angry Birds Attack: New Android Bug Lets Spoofed Apps Run Wild
  - Malicious programs that pose as legitimate apps for Android aren't quite a new phenomenon.

Online financial frauds (A massive smishing)

- **Alert issued on Kim Yu-na smishing**
  - **scammers send a text reading, "Thank you, Kim Yu-na. We will compensate for your robbed gold medal. Compensation of 30,000 won ($28)," along with the URL or Internet address, taking advantage of the public sentiment over the Olympic Games to cheat money out of smartphone users.**
- Four online financial scams such as SMishing, pharming, instant messenger phishing and memory hacking reached 32,060 cases in the January-October period of last year. (2014-01-31)

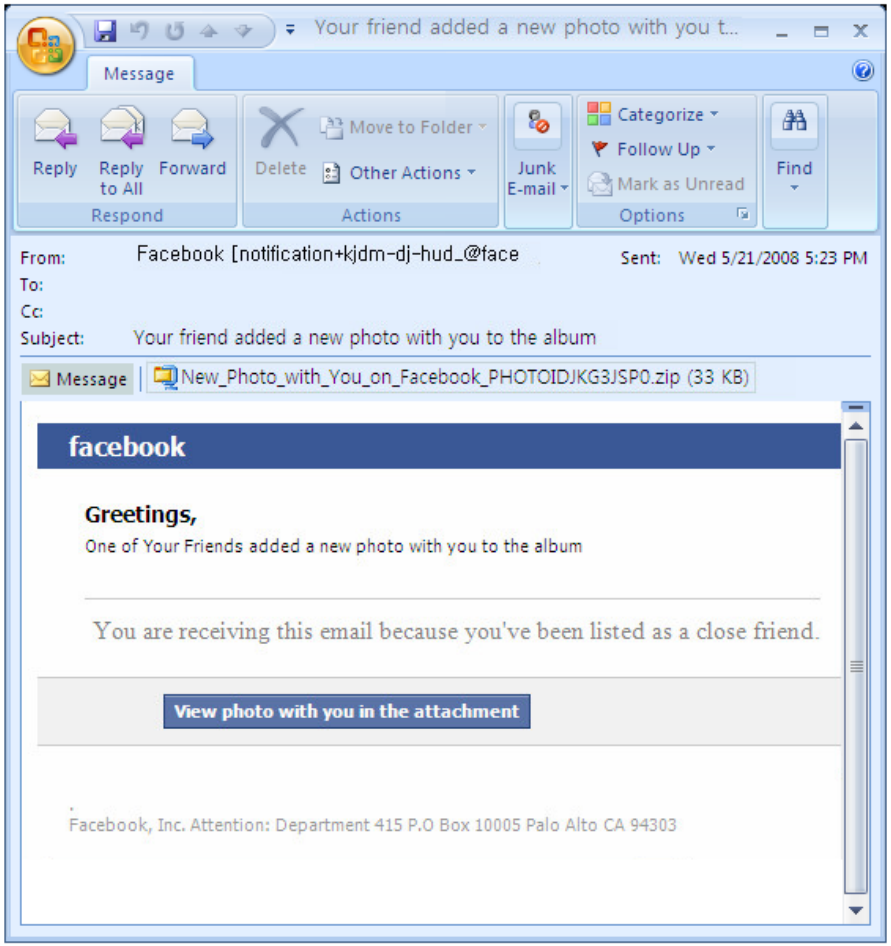


Spoofing = Masquerading

- **Phishing = Fabrication of information**
  - Creates a web site that looks like a real bank or other e-commerce site
- **Spoofing**
  - May involve sending on a network data packets that have false return addresses

Spoofing = Masquerading

- **Spreading malicious files masqueraded as Facebook image**
  - **INCA Internet response team detected malicious files disguised as sent from Facebook**



- [프리미엄] 반기문 총장, 가짜 페이스북 때문에 골치라는데... -- chosun.com 2014.01.05
- [소치] 푸틴의 '안현수 페북사진' 알고보니 가짜 – dongA.com 2014-02-18

Malware: Gauss, Flame, Stuxnet

- **Gauss: Nation-state cyber-surveillance meets banking Trojan** (cyber-weapons)
- **Middle Eastern Gauss malware could be state sponsored**
  - **Code linked to Flame and Stuxnet attacks**
    - "Gauss was created by the same 'factory' which produced Flame. This indicates it is most likely a nation-state sponsored operation,"
  - Gauss is designed to infect Windows systems and harvests browsing information and payment logins via PayPal, Citibank and a number of Lebanese operations such as the Bank of Beirut and Fransabank.
  - The payload is run by infected USB sticks and is designed to surgically target a certain system (or systems) which have a specific program installed
  - all running Debian Linux and listening on ports 22, 80, and 443 (as with Flame)
  - Gauss installs a new font, Palida Narrow, and the tool checks to see if this is installed as an indicator of infection.

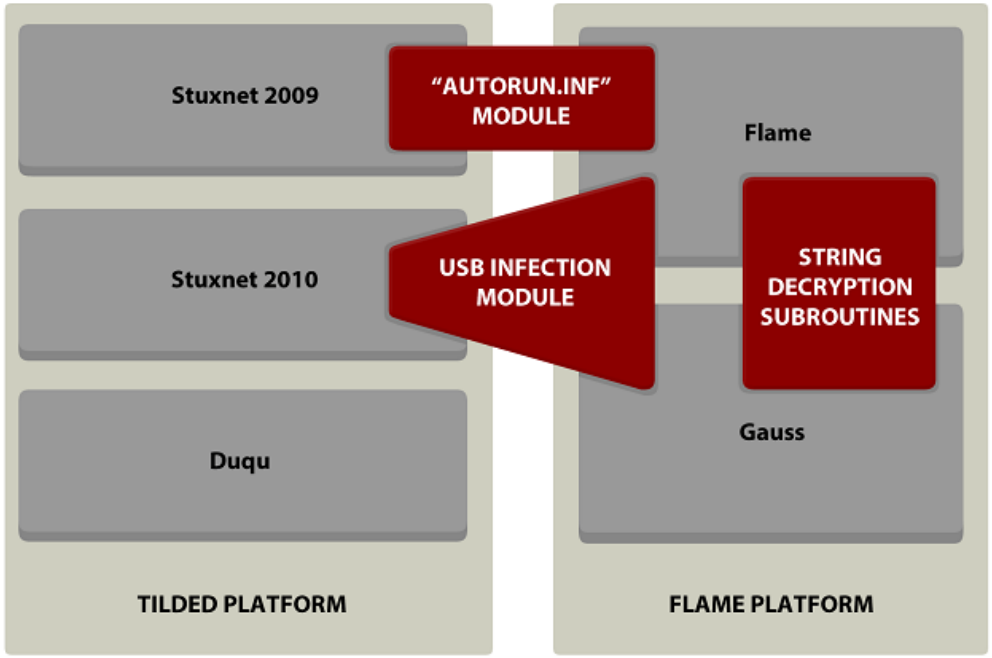
Malware: Gauss, Flame, Stuxnet

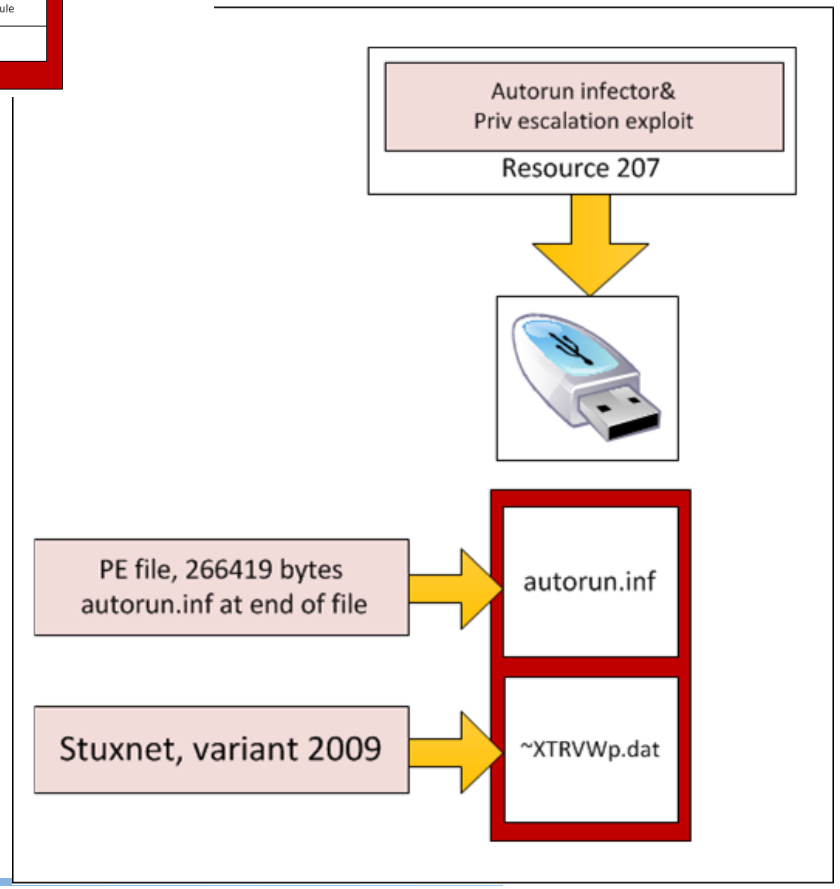
201 19840	Mrxcls.sys
202 14336	Small "siemens" dll
205 323	Config for mrxcls
207 520192	Autorun infector/Priv escalation exploit
208 298000	Big "siemens" dll
209 25	data
210 9728	PE template
221 145920	MS08-067 exploit module
222 102400	MS10-061 exploit module
231 10752	C&C comms module

Stuxnet 2009

Flame
atmpsvcn.ocx

The relationship of Stuxnet, Duqu, Flame and Gauss



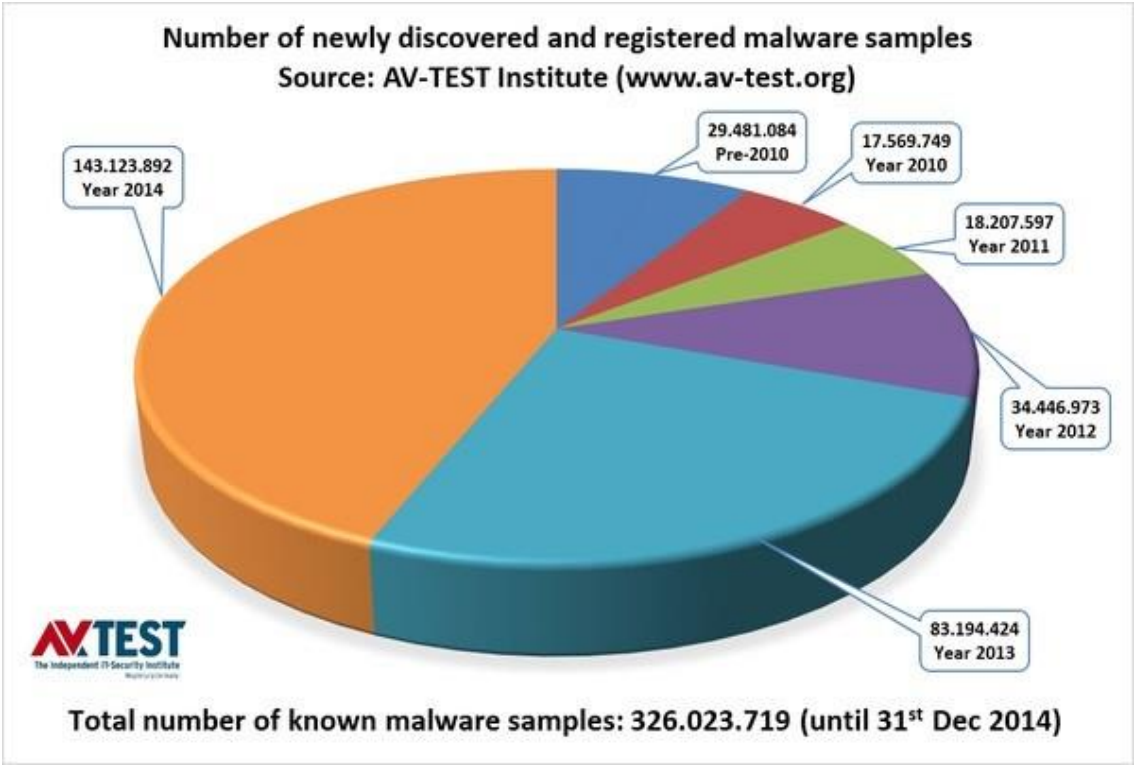


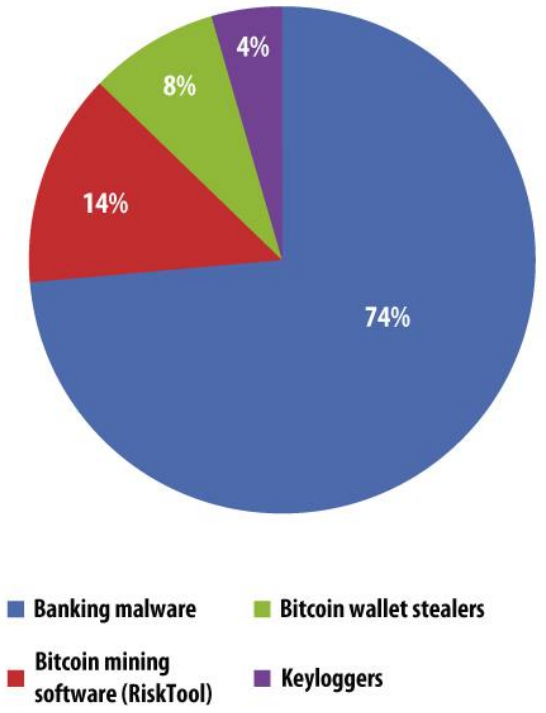
Malicious Software = Malware

- **The world's most dangerous software (2014-01-17)**
  - **a highly sophisticated malware program called Mask (more sophisticated than Flame)**
    - All the world believes that the U.S. and Israel jointly developed Flame, along with its earlier cousins Stuxnet and Duqu, in order to attack the Iranian nuclear program, and perhaps other Middle Eastern targets as well.
  - **Mask, like Flame, is principally a surveillance program.**
    - **It uses a rootkit, bootkit, and Windows, Mac OS X, and Linux versions of the malware**
    - **It steals files and keystrokes and encryption keys, and it was designed to operate for a long time undetected.**
    - There is evidence pointing to Android and iOS versions of the malware, as well, and The Mask also targets government entities, diplomatic offices, and embassies, research institutions, and activists across Europe, the Middle East, Africa, and the Americas, including victims in the US.

Mobile Malware

- **143 Million New Malware Samples Recorded in 2014**





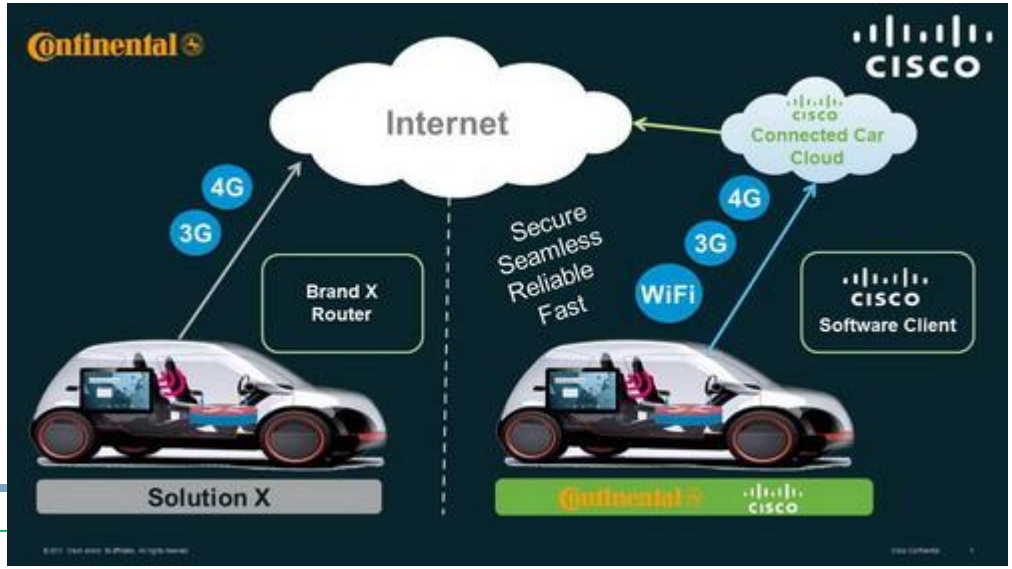
Other threats & attacks

- **Internet of Things (IoT)...poses new security risks (2014-01-12)**
  - **If the object is connected to the Internet, you will find it, and if it has an OS (operating system) you can hack it**
  - **Refrigerator among devices hacked in Internet of things cyber attack**
    - **Hackers managed to penetrate home-networking routers, connected multimedia centers, televisions and at least one refrigerator to implement their IoT attack. They created a botnet – a cyber attack that uses an unprotected platform to deliver malicious spam or phishing emails from a connected device (typically without the owner's knowledge).**
- Cyber attacks hit 67 targets: ministry (2013-07-04)
  - A total of 67 targets including public offices and companies came under cyber attacks on June 25 and the following days, the Korean government said Thursday.
  - The types of attacks include distributed denial of service (DDoS) and malicious codes to destruct hard disk drives.

Other threats & attacks

- Hack My Ride: Cyber Attack Risk on Car Computers
  - Increasingly sophisticated onboard computers may put cars in danger of cyber attacks
- Hackers to target and cyberattack high tech cars?
- Car hacking: Car cyberattack a possible theory behind journalist's death
- Connectivity in Cars Raises Cyber Attack Questions: Senator

- More than 20 Million Connected Cars to Ship Globally with Built-in Software-based Security Technology by 2020, According to ABI Research



OS and Security

Threats (STRIDE) vs. CIA

The STRIDE model describes the threats of violation of 6 information flow properties

Threat	Property
Spoofing identity	Authentication, Authenticity
Tampering with data	Integrity
Repudiation	Auditing
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

- Threats
  - Repudiation: “I didn’t send that email,” “I didn’t visit that web site,”
  - Rootkits, Rooting (Jailbreaking),
- Properties
  - Confidentiality: Data cannot be disclosed to unauthorized individuals / systems
  - Integrity: Data cannot be modified undetectably
  - Availability: Data must be available when needed
- Forensic

OS Security (from techopedia.com)

- OS security is the process of ensuring OS integrity, confidentiality and availability
  - OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.
  - OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.
- OS security allows different applications and programs to perform required tasks and stop unauthorized interference.
  - OS security may be approached in many ways, including adherence to the following:
    - Performing regular OS patch updates
    - Installing updated antivirus engines and software
    - Scrutinizing all incoming and outgoing network traffic through a firewall
    - Creating secure accounts with required privileges only (i.e., user management)

Operating System Concepts, 9th Ed

PART FIVE ■ PROTECTION AND SECURITY

Chapter 14 Protection

Chapter 15 Security

Operating Systems: Internals and Design Principles, 7/E

http://www.pearsonhighered.com/educator/product/Operating-Systems-Internals-and-Design-Principles/9780132309981.page

- **Security Issues**
  - **Chapter 3: Process Description and Control** (Rootkits, Stack overflow, Race condition)
  - **Chapter 7: Memory management** (Stack overflow, Ret2Libc, ..)

Chap. 14 Computer Security Threats

- Computer Security Concepts
- Threats, Attacks, and Assets
- Intruders
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits
- Summary

Chap. 15 Computer Security Techniques

- Authentication
- Access Control
- Intrusion Detection
- Malware Defense
- Dealing with Buffer Overflow Attacks
- Windows 7 Security
- Summary

SELinux (Security Enhanced Linux)

- **SELinux features** (source: http://drsalbertspijkers.blogspot.kr/2013/06/linux-kernel-security-it-is-necessary.html)
  1. Clean separation of policy from enforcement
  2. Well-defined policy interfaces
  3. Support for applications querying the policy and enforcing access control
  4. Independent of specific policies and policy languages
  5. Independent of specific security label formats and contents
  6. Individual labels and controls for kernel objects and services
  7. Caching of access decisions for efficiency
  8. Support for policy changes
  9. Separate measures for protecting system integrity (domain-type) and data confidentiality (**multilevel security**)
  10. Very flexible policy
  11. Controls over process initialization and inheritance and program execution
  12. Controls over file systems, directories, files, and open file descriptors
  13. Controls over sockets, messages, and network interfaces
  14. Controls over use of "capabilities"

SELinux

- **Pros and Cons**
  - Admin skill set (learning curve) - High
  - Complex and powerful access control mechanism - Yes
  - Detailed configuration required - Yes
  - GUI tools to write / modify rules set - Yes
  - CLI tools to write / modify rules set - Yes
  - Ease of use - No (often described as horrible to use)
  - Binary package - Available for most Linux distributions
  - System performance impact: None
  - Security Framework: Mandatory access controls using Flask
  - Auditing and logging supported - Yes
  - Typical user base - Enterprise users
  - Documentation - Well documented

* Source: Linux Kernel Security (it is necessary)

SELinux / AppArmor / Grsecurity

- New user / ease of use : Grsecurity
- Easy to understand policy and tools : AppArmor
- Most powerful access control mechanism : SELinux

Feature	SELinux	AppArmor	grsecurity
Automated	No (audit2allow and system-config-selinux)	Yes (Yast wizard)	Yes (auto traning / gradm)
Powerful policy setup	Yes (very complex)	Yes	Yes
Default and recommended integration	CentOS / RedHat / Debian	Suse / OpenSuse	Any Linux distribution
Training and vendor support	Yes (Redhat)	Yes (Novell)	No (community forum and lists)
Recommend for	Advanced user	New / advanced user	New users
Feature	Pathname based system does not require labelling or relabelling filesystem	Attaches labels to all files, processes and objects	ACLs

Security Enhancements for Android

- **SE for Android (http://selinuxproject.org/page/SEAndroid)**
  - Security Enhancements for Android™ (SE for Android) is a project to identify and address critical gaps in the security of Android.
    - Initially, the project is enabling the use of SELinux in Android in order to limit the damage that can be done by flawed or malicious apps and in order to enforce separation guarantees between apps.
    - However, the scope of the project is not limited to SELinux.
  - SE for Android also refers to the reference implementation produced by the project.
    - The current reference implementation provides a worked example of how to enable and apply SELinux at the lower layers of the Android software stack and provides a working demonstration of the value provided by SELinux in confining various root exploits and application vulnerabilities.
  - Android 4.3 is the first Android release version to fully include and enable the SELinux support contributed by the SE for Android project.

Lab Exercises (Hands-on experience)

- **Topics for practical training**
  - Password cracking
  - Backdoor
  - Threats and Protection associated Shared Library
  - Buffer Overflow (BoF) + Return to Library (Ret2Libc)
  - Packet capture using Wireshark
  - …

Summary of Security Threats

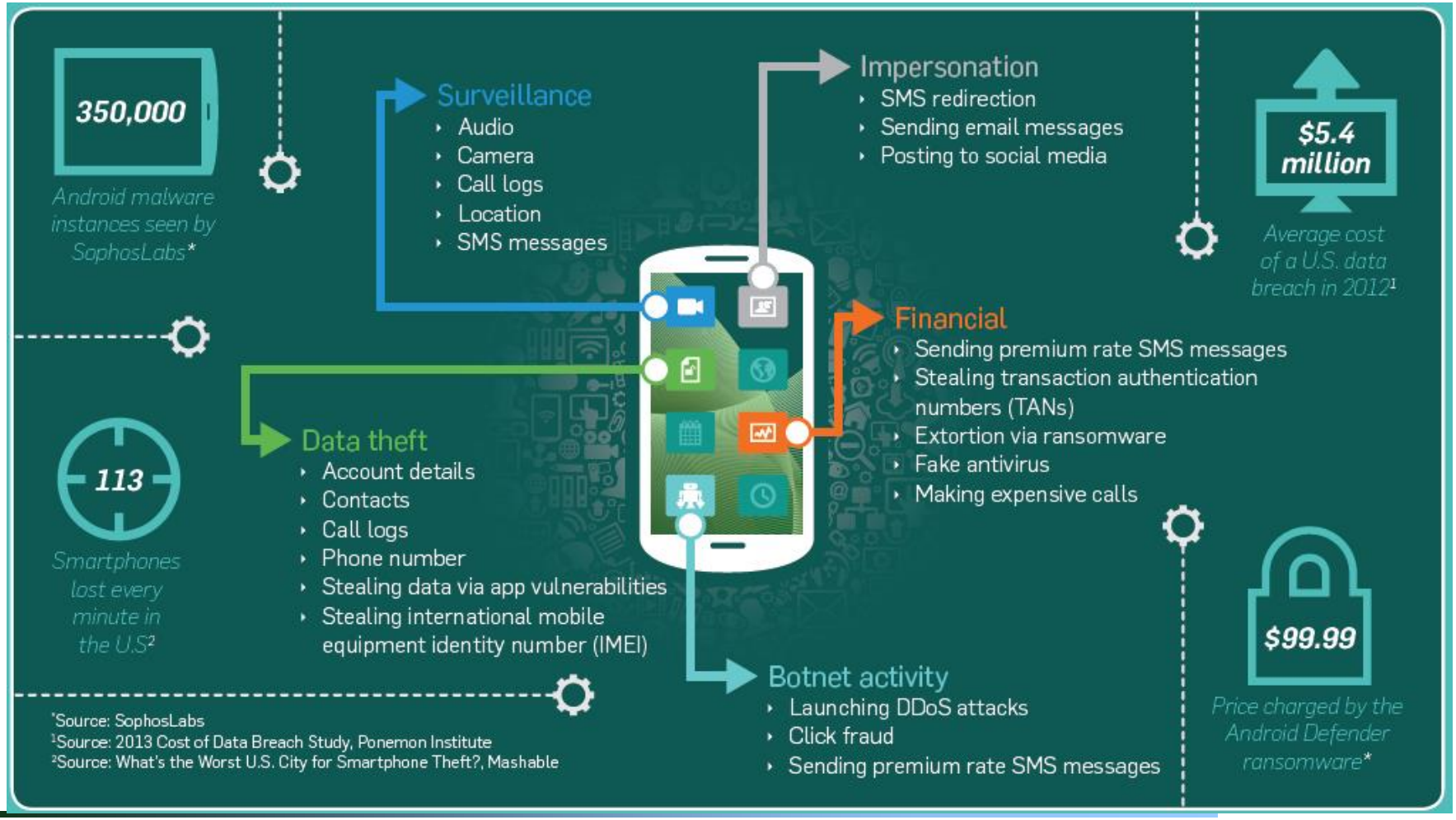
Technical Terminology is difficult.

Don’t worry, you will learn it in near future.

But, attention & eagerness are needed.

Security Threat Report 2014 (sophos.com)

- Android Malware: Mutating and Getting Smarter
  - **Anatomy of a Hacked Mobile Device: How a hacker can profit from your smartphone**



Security Threat Report 2014 (sophos.com)

- Linux: Pivotal Technology, Attracting Criminals
  - Linux is a targeted platform because Linux servers are so widely used to run websites and deliver web content.
- Mac OS X: A Year of Many Small Attacks
  - While we saw no high-profile attacks against Mac OS X this year, we did detect a steady stream of modest, creative and diverse attacks that make it wise for Mac users to keep their guard up
- Web-Based Malware: More Sophisticated, Diverse and Hidden
  - Dangerous, difficult-to-detect web server attacks and exploit kits broadened in 2013, leading to more drive-by attacks against vulnerable web clients.
- Targeted Threats to Your Financial Accounts
  - We are seeing more persistent, targeted attacks—and many seem to be aimed at compromising financial accounts.

Security Threat Report 2014 (sophos.com)

- Windows: The Growing Risk of Unpatched Systems
  - Starting in April 2014, no new patches will be available for Windows XP and Office 2003. Meanwhile, Windows patching has emerged as a significant issue in specialized markets such as point-of-sale and medical equipment.
- Spam Reinvents Itself
  - Yet another year of spam.
  - It isn't glamorous, but the security risk just never goes away.

What is Computer Security?

- Allow intended use of computer systems
- Prevent unintended use that may cause harm
- Protect information and systems from security threats

Korea sets out to train more cyber experts, hackers

‘White-hat hackers’ expected to play crucial role in fight against cyber attacks: experts

- The Korean government announced a comprehensive national cyber security plan on July 4.
  - Under the plan, policymakers plan to double the size of the domestic information security market to 10 trillion won ($8.76 billion) by 2017, according to the Ministry of Science, ICT and Future Planning.
- The ministry also said it would provide systematic training to foster 5,000 cyber security experts/professionals by 2017
  - Korea Information Technology Research Institute (KITRI) runs a special program called “Best of Best”
  - KISA’s “Cyber Security Elite Training” program
  - Korea University’s Cyber Defense Department

Samsung unveiled the Knox 2.0 security solution at the Mobile World Congress in Barcelona

- **Samsung pins high hopes on Galaxy S5, wearables (2014-02-27)**
  - **Devices become wearable, more sophisticated to attract new generation of users**
  - **The Knox 2.0, the mobile security solution installed on the latest Galaxy model, will also play a key role for Samsung to be able to retain the top position in the global mobile market as it will prove to be the most stable and safest mobile security platform**

Learn About Security

Make a Difference

How Can You Make a Difference?

- Be a more security-aware user
  - Make better security decisions
- Be a more security-aware developer
  - Design & build more secure codes & systems
- Be a more security-aware tester (defender)
- Be a security practitioner & researcher
  - Identify security issues
  - Propose new security solutions

War game sites (Training ground)

- **Domestic**
  - **Online Information security e-learning center (정보보호기술 온라인훈련장): http://www.sis.or.kr/ → Training (훈련공간)**
  - **Challenge: http://www.simples.kr/ → Community → challenge 보고서**
  - **Hacker School**
    - http://www.hackerschool.org/Sub_Html/HS_Community/index.html → 운동장 → Free Training Zone (FTZ)

- **International (Sites in Foreign countries)**
  - **Internet Security & Challenges (Net Force): http://www.net-force.nl/ → <challenges>**
  - **Hack This Site! -- http://www.hackthissite.org/**
  - **Reversers' playground (CrackMe site): http://crackmes.de/**
    - **A great site for testing your reversing skills**
  - **Think Devise Hack (tdhack.com):** a lot of challenges including cryptographic riddles, hackmes and SW applications to crack for both Windows and Linux

Security Expert

- Logical mind, Flexible thinker
- Eagle eyes
- Open ears
- Verbal skills
- Calm disposition
- Helping hand
- Gadget addiction

The 20 Coolest Jobs in Information Security

#1 Information Security Crime Investigator/Forensics Expert
#2 System, Network, and/or Web Penetration Tester
#3 Forensic Analyst
#4 Incident Responder
#5 Security Architect
#6 Malware Analyst
#7 Network Security Engineer
#8 Security Analyst
#9 Computer Crime Investigator
#10 CISO/ISO or Director of Security
#11 Application Penetration Tester
#12 Security Operations Center Analyst
#13 Prosecutor Specializing in Information Security Crime
#14 Technical Director and Deputy CISO
#15 Intrusion Analyst
#16 Vulnerability Researcher/ Exploit Developer
#17 Security Auditor
#18 Security-savvy Software Developer
#19 Security Maven in an Application Developer Organization
#20 Disaster Recovery/Business Continuity Analyst/Manager

Source: SANS
http://www.sans.org/20coolestcareers/

보안 직업군 프로젝트

Source: http://www.boannews.com/media/view.asp?idx=37409&kind=0

- 보안 컨설턴트
  - 보안기술 기반으로 경영 흐름과 융합보안 트렌드를 읽어야
  - [Interview] 이상훈 이글루시큐리티 컨설팅사업부2팀 팀장
- 악성코드 분석가
  - 악성코드와의 피 말리는 싸움 위해선 인내심과 집중력이 필수
  - [Interview] ASEC 분석1팀 한창규 팀장 & 김아영 연구원
- 모의해킹 전문가
  - 쉽게 뚫려서 많이 당황하셨어요? 이게 바로 회사의 보안 현실이죠!
  - [Interview] LG CNS 보안컨설팅팀 곽규복 차장 & 박태석 과장
- 보안 기술영업
  - 기술적 깊이와 함께 비즈니스 마인드까지 갖추고 싶다면 도전하라
  - [Interview] IBM Korea 박형근 부장 / 보안커뮤니티 SecurityPlus 운영자
- 보안관제사
  - 사이버세상 안전 위해 365일 24시간 해킹대응의 최전방에서 뛴다
  - [Interview] SK인포섹 김종현 보안관제팀장
- …

Certification

- **CCNA Security Certification**
  - **Cisco Certified Network Associate Security (CCNA Security)**
  - **http://www.cisco.com/web/learning/certifications/associate/ccna_security/**
- **CISSP (Certified Information Systems Security Professional)**
  - **https://www.isc2.org/CISSP/Default.aspx**
  - The CISSP exam is based on the following domains: Access control, Telecommunications and Network Security, Software Development Security, Operations security
  - **MGT414: SANS +S Training Program for the CISSP® Certification Exam**
- **CISA (Certified Information Systems Auditor)**
  - **http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx?utm_source=multiple&utm_medium=multiple&utm_content=friendly&utm_campaign=cisa**
- **GIAC Information Security Professional (GISP)**
  - **http://www.giac.org/certification/information-security-professional-gisp**

Certificate / License (of qualification)

- 정보보안기사 (정보보안 국가기술자격)
  - Written test:
    - System security, Network security, Application security, 정보보안일반, 정보보안관리 및 법규
  - Practical (Skill) test:
    - 정보보안실무
  - Schedule for examination
    - 1st : July 6th & Aug. 24th, 2013 for Written & Skill
    - 2nd : Oct. 26th & Dec. 7th, 2013 for Written & Skill
    - **3rd : Apr. 5th, 2014 for written test (Application period: Mar. 3rd~7th)**
- 정보보안산업기사: 정보보안 기사의 업무를 보조할 수 있는 기초 이론과 실무능력 수행

- [주간한국] 떠오르는 유망직종 정보보안전문가 '정보보안기사, 정보보안산업기사' 자격증으로 준비

Any questions?

- Hardships, The way of suffering
  - An unremitting effort, Sincerity, Diligence

- Expert, Specialist, Elite in Security

Summary

- Major threats: STRIDE
- Computer security: CIA
- Field experience study (Actual practice)
  - SecuInside 2015: CTB (Capture The Bugs) challenge
    - July 16th ~ 17th, Inchon Memorial, Korea Univ. (http://secuinside.com/2015/ctb_eng.html)
  - PoC 2015 (Power of Community: 10th Anniversary)
    - Nov. 5-6 Seoul (http://www.powerofcommunity.net/main.htm)
  - 제12회 해킹방어대회 문제구현등 훈련용콘텐츠 개발 (4천만원 입찰), 예선 대회는 2015년 10월 개최(?) – 본선은 12월 초(?) 개최
- Cyber Ethics is important
  - The 10th Hacking Defense Contest: July-01-2013
    - 정부 주최 '해킹방어대회' 4시간 만에 중단
  - "Sophisticated" British hacker faces 12 years in US jail for infiltrating Federal Reserve