Network Security and Intrusion Detection

Haipeng Dai

haipengdai@nju.edu.cn
313 CS Building
Department of Computer Science and Technology
Nanjing University

Course Personnel

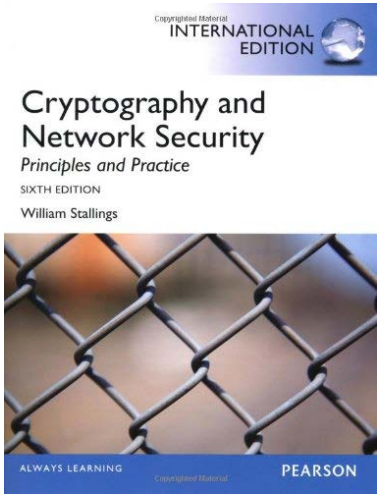
- Instructor
  - Dr. Haipeng Dai (戴海鹏)
  - Office hours Fri 9:00-11:30 am or by appt (313 CS Building)
  - Contact via email (haipengdai@nju.edu.cn)
- TA
  - Dr. Rui Xia (夏瑞)
  - Contact via email (xiarui0428@hotmail.com)
- Course Website (http://cs.nju.edu.cn/daihp/)
  - Assignments, reading materials, slides…

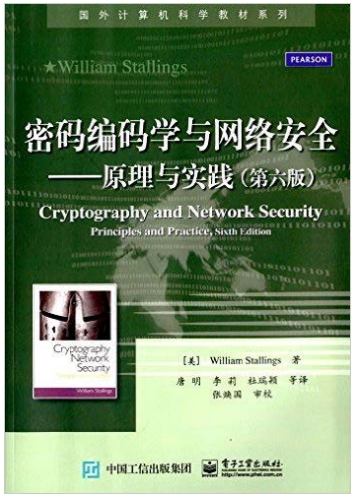
Course Textbook

- 《Cryptography and Network Security Principles and Practice》

《密码编码学与网络安全:原理与实践》(**第6版**)

William Stallings (作者)，张焕国 (合著者)，唐明 (译者)，李莉 (译者)，杜瑞颖 (译者)，等 (译者)，电子工业出版社，2015年。



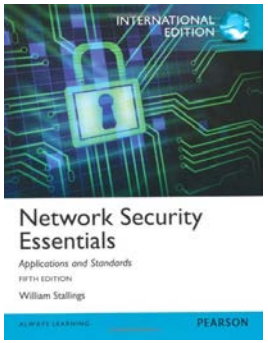


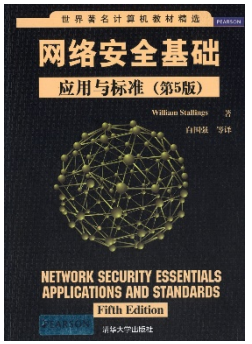
- What's new in the 6th edition?
  - Network access control, Cloud security, SHA-3, Key wrapping, Elliptic Curve Digital Signature Algorithm (ECDSA), RSA Probabilistic Signature Scheme (RSA-PSS), True random number generator……

References and Further Readings

- 《Network Security Essentials: applications and Standards》

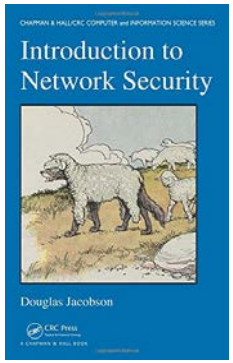
《网络安全基础:应用与标准》(第5版)
William Stallings (作者)，白国强 (译者)，等 (译者)，
清华大学出版社，2014年。

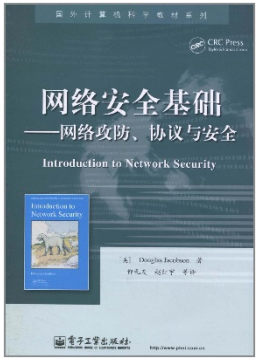




- 《Introduction to Network Security》

《网络安全基础:网络攻防、协议与安全》(第1版)
Douglas Jacobson (作者)，仰礼友 (译者)，
赵红宇 (译者)，等 (译者)，
电子工业出版社，2013年。





References and Further Readings

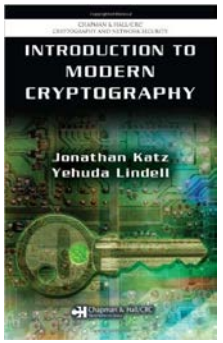
- 《Introduction to Modern Cryptography》

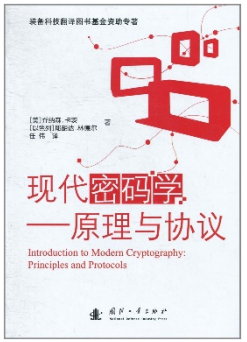
《现代密码学:原理与协议》（第1版）

Jonathan Katz (作者)，Yehuda Lindell (作者)，

任伟 (译者)

国防工业出版社， 2015年。



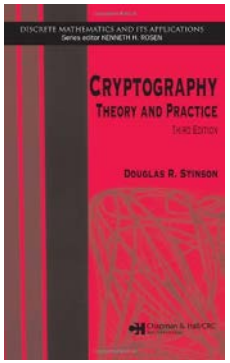


- 《Cryptography Theory and Practice》

《密码学原理与实践》（第3版）

Douglas R.Stinson (作者)，冯登国 (译者)

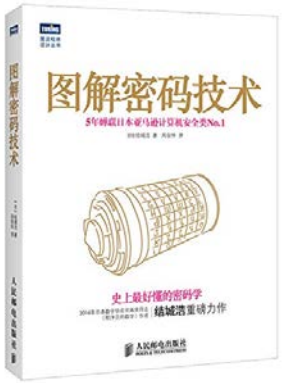
电子工业出版社，2013年。



References and Further Readings

- 《图解密码技术》

结城浩 (作者)，周自恒 (译者)
人民邮电出版社，2015年。



Online Courses

- 《Network and Computer Security》 MIT

http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/lecture-notes-and-readings/

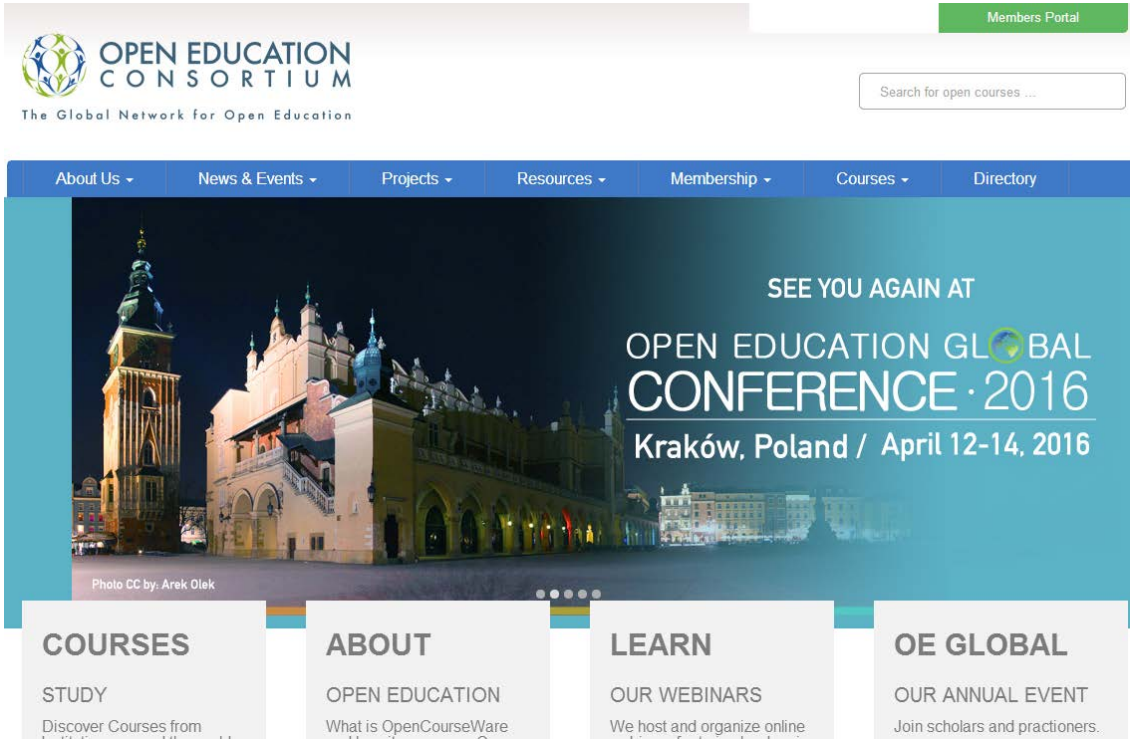
- 《Computer Systems Security》 MIT

http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm

Online Courses

- Open Education Consortium

http://www.oeconsortium.org/



Grading

- Grading:
  - Final Exam: 50%
  - Midterm Exam: 20%
  - Homework: 10%
  - Attendance: 10%
  - Paper presentation: 10% + 5~10% bonus

Midterm and Final

- Closed book, closed notes
- Each last 1 h 40 min
- We will have reviews in class before each

Academic Integrity

- What is and is not OK
  - I encourage you to work with others to learn the material but everyone must DO their work ALONE
  - Do not to turn in the work of others
  - Do not give others your work to use as their own
  - Do not plagiarize from others (published or not)
  - Do not try to deceive the instructor

- See the Web site
  - More guidelines on academic integrity
  - Links to university resources
  - Ask if in doubt

- You can always ask me or TA for help!

- Others:
  - "The student's behavior in the classroom shall be conducive to the teaching and learning process for all concerned."
  - "No student shall … interfere with the functions and services of the University (for example, but not limited to, classes …) such that the function or service is obstructed or disrupted. Students whose conduct adversely affects the learning environment in this classroom may be subject to disciplinary action through the Student Faculty Judiciary process."
  - …

Security Conferences

- IEEE Symposium on Security and Privacy
  - http://www.ieee-security.org/TC/SP-Index.html
- USENIX Security Symposium
  - http://www.usenix.org/events/sec10/
- ACM Conference on Computer and Communications Security (CCS)
  - http://www.sigsac.org/ccs.html
- Annual Network and Distributed System Security Symposium
  - http://www.isoc.org/isoc/conferences/ndss/10/
- Security papers are also published in many networking and system conferences: SIGCOMM, SIGMETRICS, SOSP, ICNP, INFOCOM, ICDCS, NSDI, Mobicom, DSN, Mobihoc, CoNext, etc.

Why study security?

- People attack systems and do damage
  - Why do they do it?
    - Financial motivation
    - Religious/political motivation
    - Industrial espionage
    - Angry employees
    - Bored teenagers
  - How do they do it?
    - Network attacks
    - Exploit vulnerabilities in applications and security mechanisms
    - Physical access
  - Whom do they attack?
    - Banks
    - Government agencies
    - E-commerce web sites
    - Hollywood
    - Universities (play ground)

How big is the problem?

- Internet attacks are increasing in frequency, severity, and sophistication
- Denial of service (DoS) attacks
  - Cost $1.2 billion in 2000
  - 1999 CSI/FBI survey 32% of respondents detected DoS attacks directed to their systems
  - Yahoo, Amazon, eBay, Microsoft, White House, etc., attacked

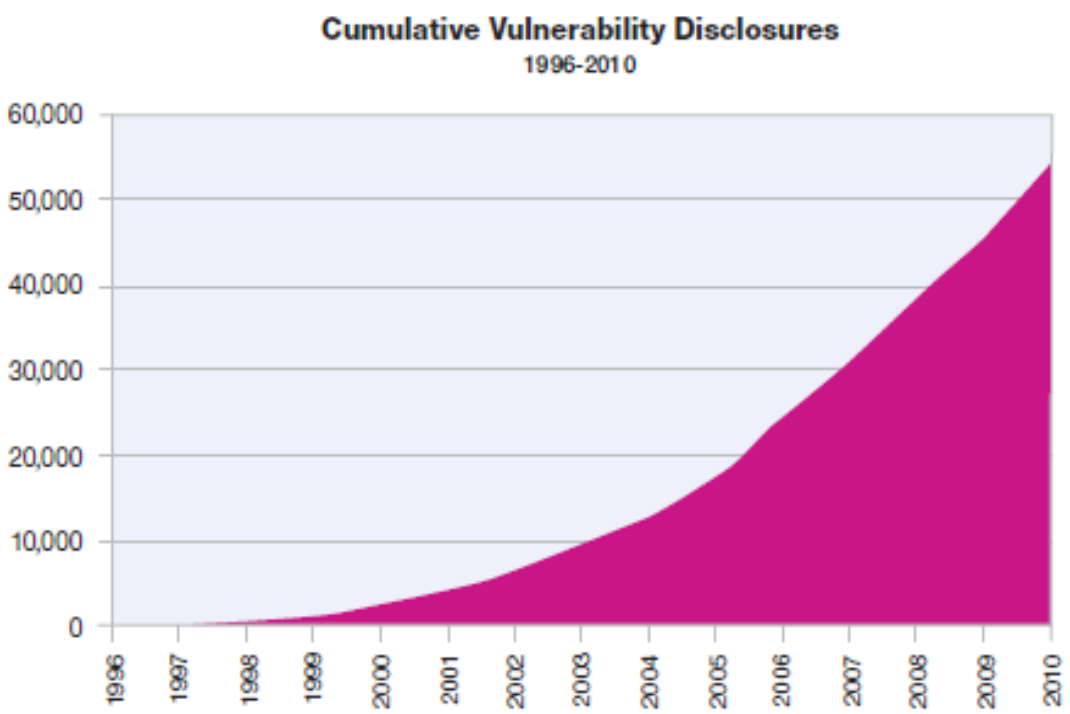
How big is the problem? (cont'd)

- In first half year of 2005, 237 million network attacks launched
  - IBM Global Business Security Index Report
- In 2005, U.S. businesses lost 67.2 billion dollars due to attacks
  - 2006 Computer Crime and Security Survey by FBI and CSI
- Virus and worms
  - Morris, Melissa, Nimda, Code Red, Code Red II, Slammer …
  - Cause over $28 billion in economic losses in 2003, growing to over $75 billion in economic losses by 2007.
  - Code Red (2001): 13 hours infected >360K machines - $2.4 billion loss
  - Slammer (2003): 10 minutes infected > 75K machines - $1 billion loss
- Security has become one of the hottest jobs even with downturn of economy

How big is the problem? (cont'd)

- MITRE tracks vulnerability disclosures

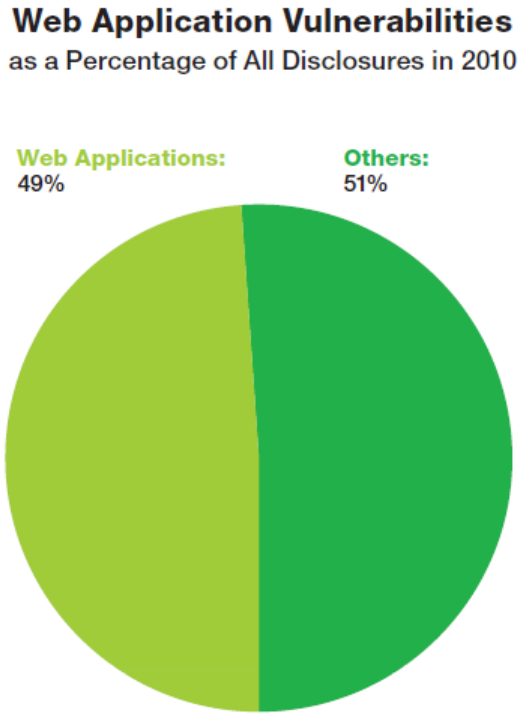
Cumulative Disclosures



Source: IBM X-Force, Mar 2011

Data: http://cve.mitre.org/

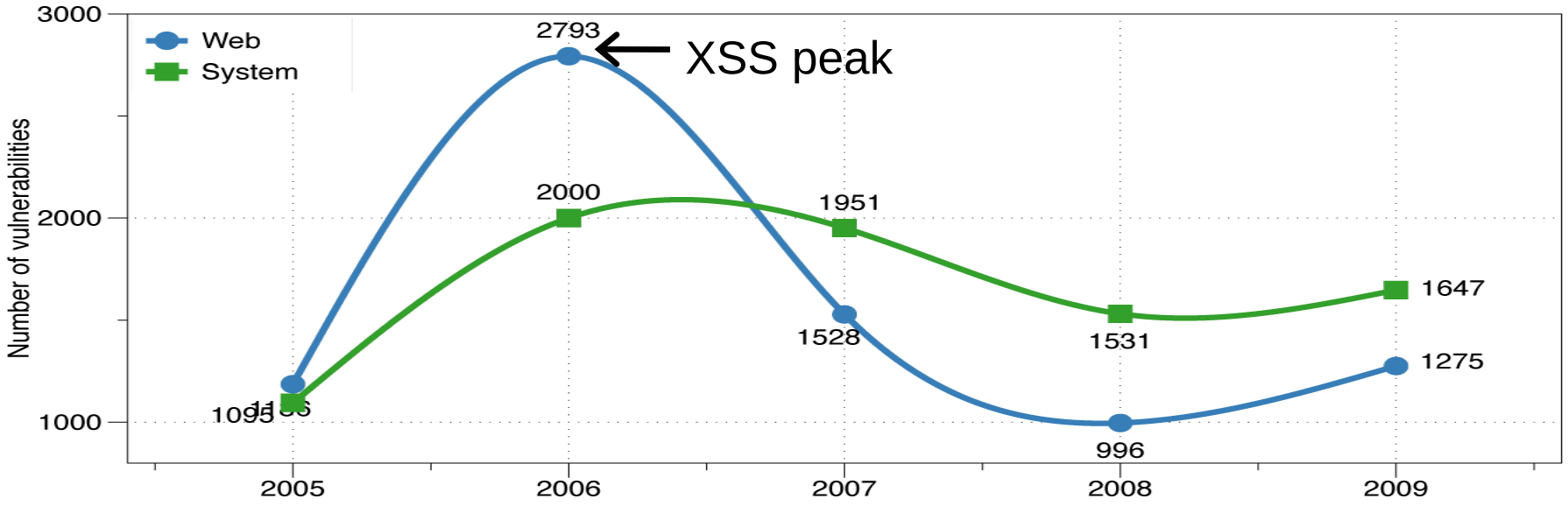
Percentage from Web applications



2010

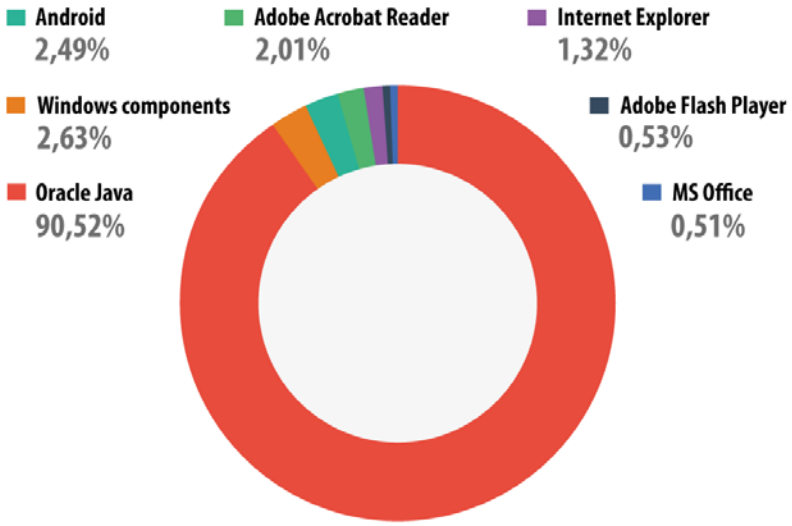
How big is the problem? (cont'd)

- Web vs. System vulnerabilities

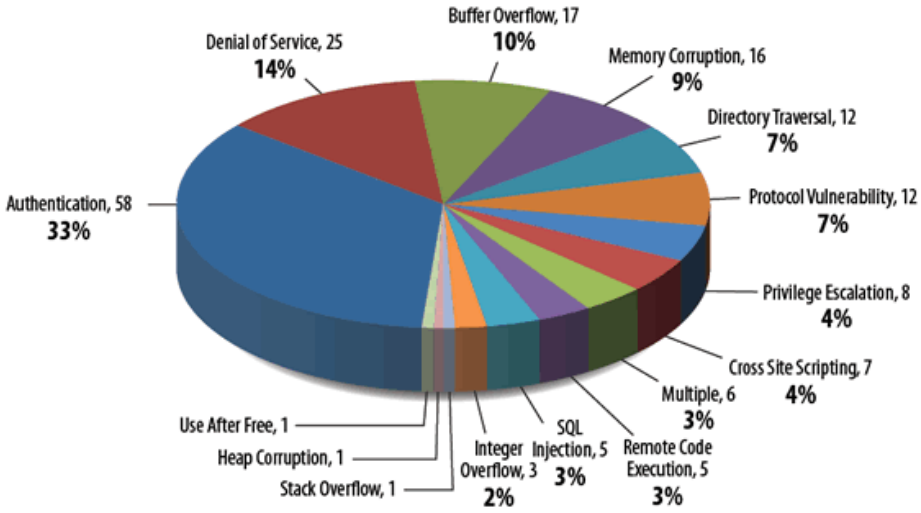


How big is the problem? (cont'd)

- Vulnerable applications being exploited



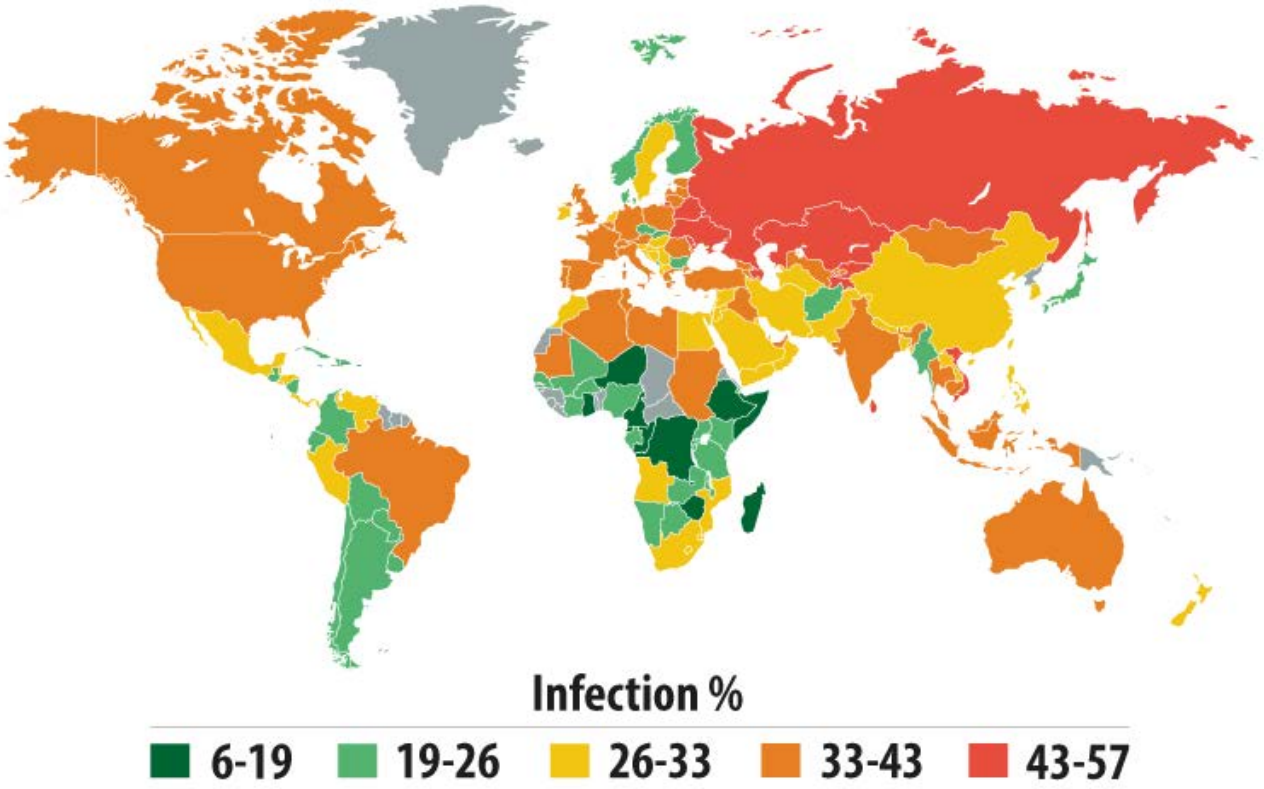
Source: Kaspersky Security Bulletin 2013



Source: ICS-CERT Monitor 2014

How big is the problem? (cont'd)

- Countries where users face the highest risk of online infection



Source: Kaspersky Security Bulletin 2013

How big is the problem? (cont'd)

Marketplace for Vulnerabilities

- Option 1: bug bounty programs
  - Google: up to $3133.7 in 2010, now up to $20K per bug
  - Facebook: up to $20K per bug
  - Microsoft: up to $150K per bug
  - Mozilla Bug Bounty program: 500$ - 3000$
  - Pwn2Own competition: $10-15K
- Option 2: vulnerability brokers
  - ZDI, iDefense: $2-25K

How big is the problem? (cont'd)

Marketplace for Vulnerabilities

- Option 3: gray and black markets
  - Up to $100-250K reported (hard to verify)
  - A zero-day against iOS sold for $500K (allegedly)

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Source: Andy Greenberg (Forbes, 3/23/2012)

How big is the problem? (cont'd)

- Several companies specialize in finding and selling exploits
  - ReVuln, Vupen, Netragard, Exodus Intelligence
  - The average flaw sells for $35-160K
  - $100K+ annual subscription fees
- Nation-state buyers
  - "Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too" -- NY Times (Jul 2013)

How big is the problem? (cont'd)

Marketplace for Stolen Data [Dell SecureWorks, 2013]

- Single credit card number: $4-15
- Single card with magnetic track data: $12-30
- "Fullz": $25-40
  - Full name, address, phone, email addresses (with passwords), date of birth, SSN, bank account and routing numbers, online banking credentials, credit cards with magnetic track data and PINs
- Online credentials for a bank account with $70-150K balance: under $300

Prices dropped since 2011, indicating supply glut

How big is the problem? (cont'd)

Marketplace for Victims [Trend Micro, "Russian Underground 101", 2012]

- Pay-per-install on compromised machines
  - US: $100-150 / 1000 downloads, "global mix": $12-15
  - Can be used to send spam, stage denial of service attacks, perform click fraud, host scam websites
- Botnets for rent
  - DDoS: $10/hour or $150/week
  - Spam: from $10/1,000,000 emails
- Tools and services
  - Basic Trojans ($3-10), Windows rootkits ($300), email, SMS, ICQ spamming tools ($30-50), botnet setup and support ($200/month, etc.)

Why does this happen?

- Lots of buggy software...
- Some contributing factors
  - Few courses in computer security
  - Programming text books do not emphasize security
  - Few security audits
  - C is an unsafe language
  - Programmers are lazy
  - Legacy software
  - Security mechanisms are difficult to use
  - Security is expensive and takes time
- Insider threat
  - Easy to hide code in large software packages
  - Difficult to discover hidden malicious code
  - Strict development rules and physical security help

Human Subjects

- Social Engineering
  - There are attacks that do not use computers, use human instead.
  - “Catch me if you can”

- Call system administrator
- Dive in the dumpster
- Online version
  - send trojan in email
  - picture or movie with malicious code

Example Security Incident 1

- Rob Harris case - slot machines
  - An insider: he worked for Gaming Control Board in the Electronic Services Division in Las Vegas.
- Malicious code in testing unit
  - when testers checked slot machines
    - downloaded malicious code to slot machine
  - was never detected
  - special sequence of coins activated “winning mode”
- Caught when greed sparked investigation
  - $100,000 jackpot

Example Security Incicent 2

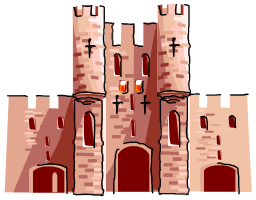
- The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January 2003 and disabled a safety monitoring system for nearly five hours
- The Slammer worm entered the Davis-Besse plant through an unsecured network of an unnamed contractor, then squirmed through a T1 line bridging that network and Davis-Besse's corporate network. The T1 line was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread.
- Luckily the plant was not operating at that time.

Example Security Incicent 3

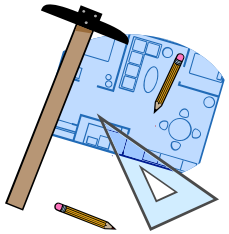
- Breeder's cup race
  - Upgrade of software to phone betting system
  - Insider, Christopher Harn, rigged software
  - Allowed him and accomplices to call in
    - change the bets that were placed
    - undetectable
  - Caught when got greedy
    - won $3 million

Network Defenses

People



Systems



Blueprints

Building blocks

End uses

Implementations

Protocols and policies

Cryptographic primitives

Password managers, company policies…

Firewalls, intrusion detection…

TLS, IPsec, access control…

RSA, DSS, SHA-1…

All defense mechanisms must work correctly and securely

Correctness versus Security

- System correctness:
  - System satisfies specification
  - For reasonable input, get reasonable output
- System security:
  - System properties preserved in face of attack
  - For unreasonable input, output not completely disastrous
- Main difference: active interference from adversary

Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
  - Higher-level protocols make mistaken assumptions
- Implementations are buggy
  - Buffer overflows are the “vulnerability of the decade”
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, impersonation, etc.

Good News

- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem" -- Bruce Schneier
  - Many security holes are based on misunderstanding
  - Other important factors: usability and economics