Secure Programming

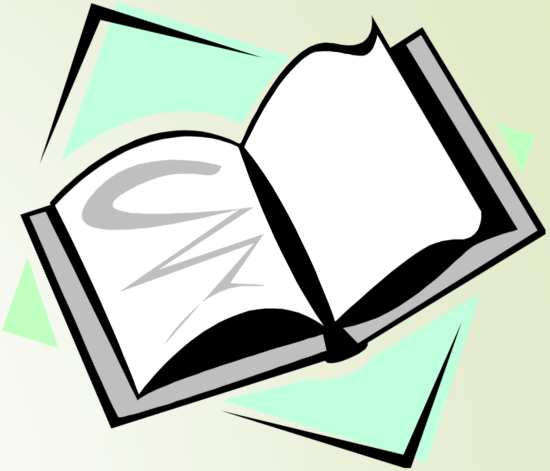
Introduction

Ahmet Burak Can

Hacettepe University

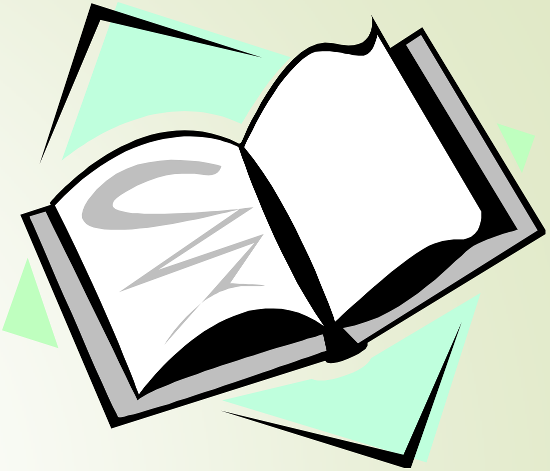
Course material

- Counter Hack Reloaded:A Step-by-Step Guide to Computer Attacks and Effective Defenses, Edward Skoudis, Tom Liston, Prentice Hall
- Hacking Exposed 7: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Osborne Media
- Secure Coding: Principles and Practices, Mark G. Graff, Kenneth R. Van Wyk, O'Reilly Media
- Software Security: Building Security, Gary McGraw, Addison-Wesley



Course material

- Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World, Michael Howard, David LeBlanc, 2nd ed. Edition, Microsoft Press
- Foundations of Security: What Every Programmer Needs To Know, Neil Daswani, Christoph Kern, and Anita Kesavan
- Security in Computing, Charles P. Pfleeger, 3th Edition
- And Internet resources..



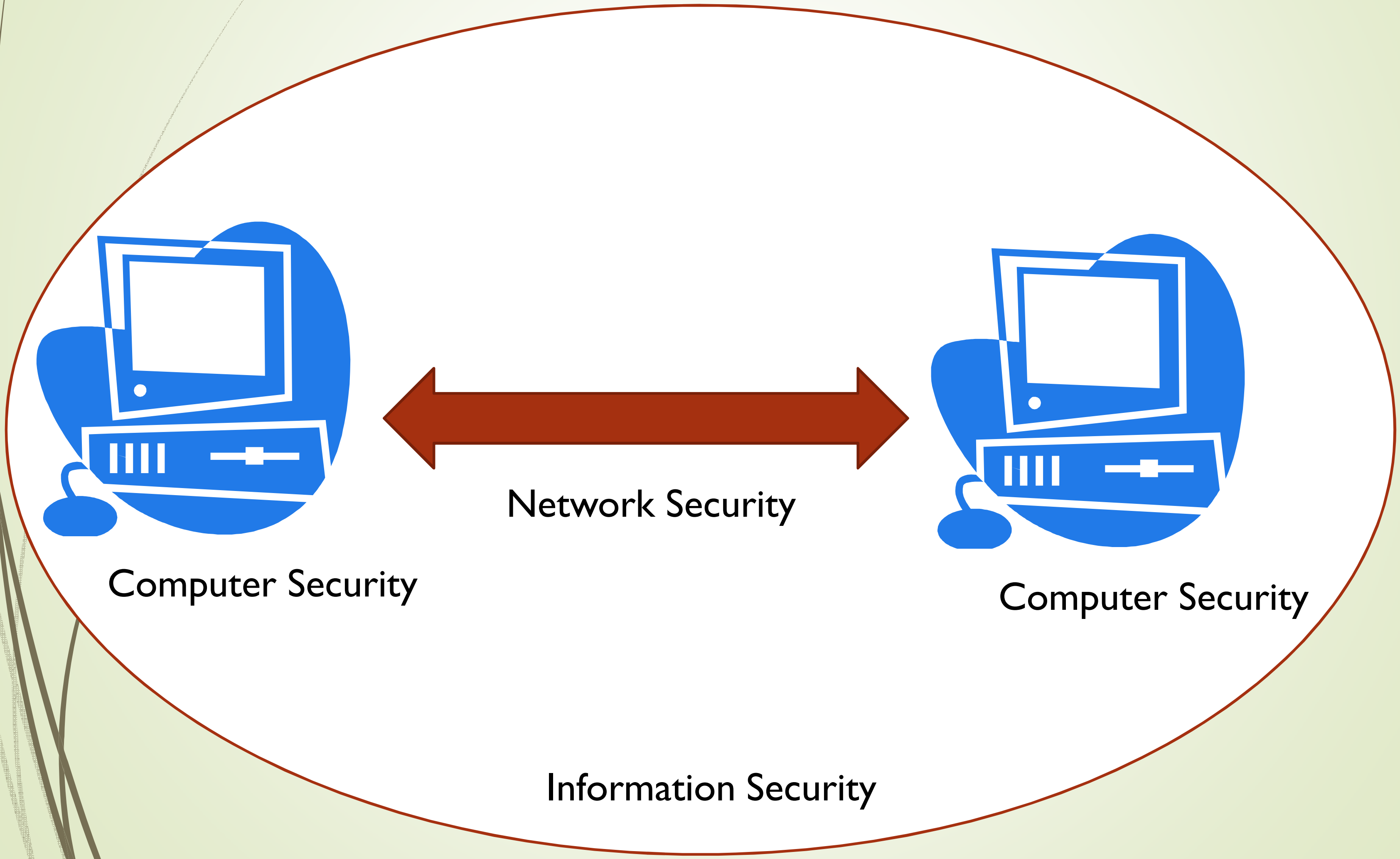
Contents

- Introduction to program security, fundementals of secure programming
- Attacks based on shell environment flaws
- Integer overflow attacks
- Buffer overflow attacks
- Input validation attacks, Format string attacks
- Links and race conditions, Temporary storage and randomness problems
- Canonicalization and Directory traversal problems
- Web environment and web applications
- Web application and session security, XSS, CSRF attacks,
- Security tests and static code analysis tools

Grading Policy

Midterm	45%
Final Exam	50%
Attendance	5%

Which Security Concept?



Computer Security

Network Security

Computer Security

Information Security

Security Goals

- Privacy (secrecy, confidentiality)
  - only the intended recipient can see the communication
- Authenticity (integrity)
  - the communication is generated by the alleged sender
- Authorization
  - limit the resources that a user can access
- Availability
  - make the services available 99.999…% of time
- Non-repudiation
  - no party can refuse the validity of its actions
- Auditing
  - Take a log of everything done in the system

Why Computer Security?

Computers are under attacks and suffer damages

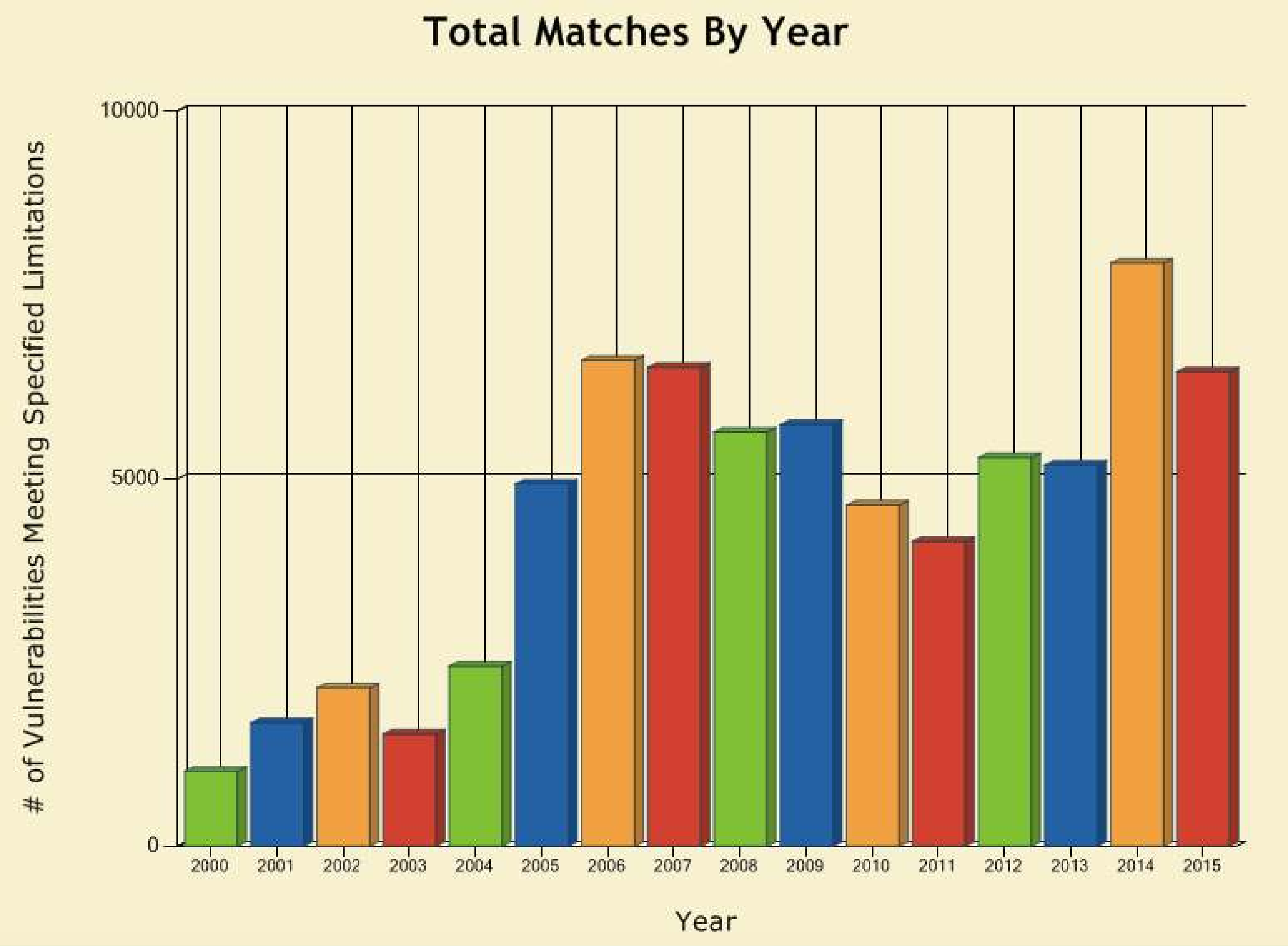
- Who are the attackers?
  - bored teenagers, criminals, organized crime organizations, rogue states, industrial espionage, angry employees, …
- Why they do it?
  - enjoyment, fame, profit, …
  - computer systems are where the moneys are

Computer Security Issues

- Computer worms
  - E.g., Morris worm (1988), Melissa worm (1999)
- Computer viruses
- Distributed denial of service attacks
- Computer break-ins
- Email spams
  - E.g., Nigerian scam, stock recommendations
- Identity theft
- Botnets
- Serious security flaws in many important systems
  - electronic voting machines
- Spyware

How big is the security problem?

CERT Vulnerabilities reported



CERT Vulnerabities in 2012

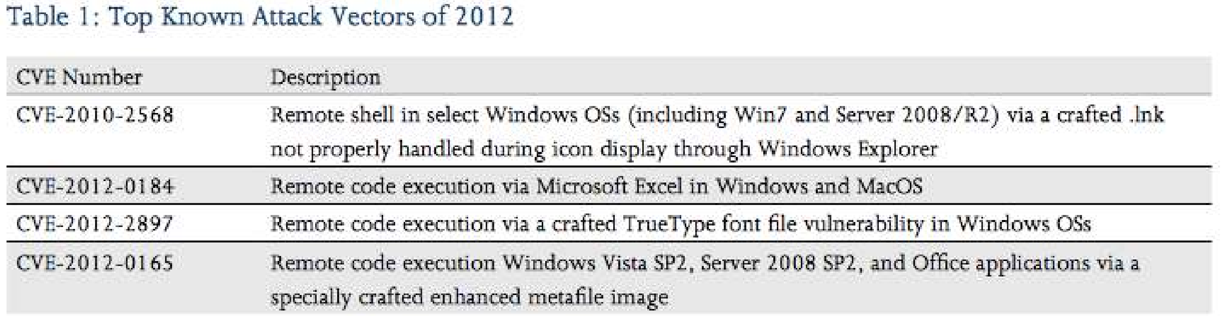
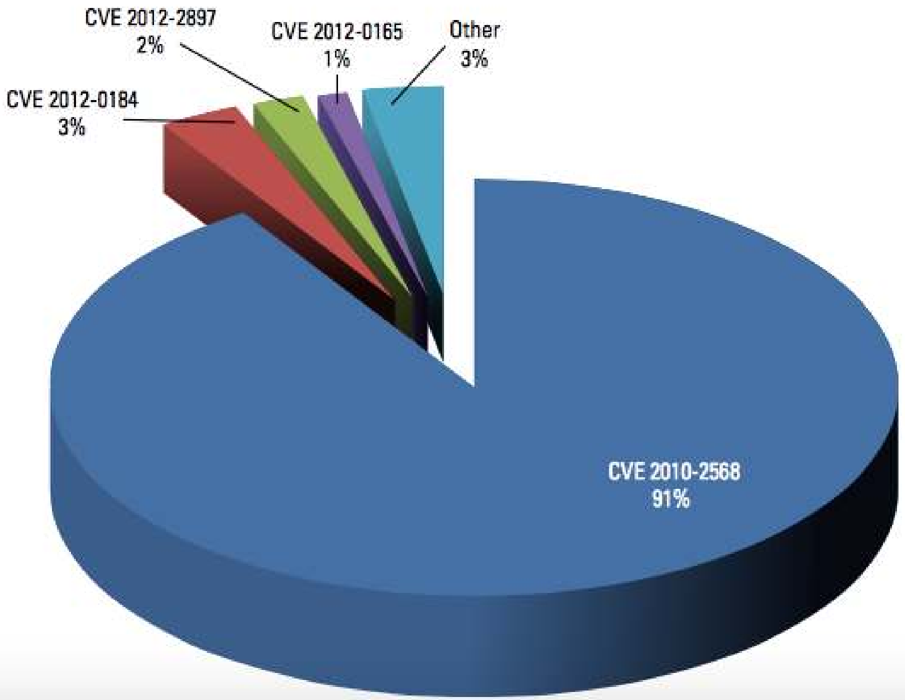


Table 1: Top Known Attack Vectors of 2012

CVE Number	Description
CVE-2010-2568	Remote shell in select Windows OSs (including Win7 and Server 2008/R2) via a crafted .lnk not properly handled during icon display through Windows Explorer
CVE-2012-0184	Remote code execution via Microsoft Excel in Windows and MacOS
CVE-2012-2897	Remote code execution via a crafted TrueType font file vulnerability in Windows OSs
CVE-2012-0165	Remote code execution Windows Vista SP2, Server 2008 SP2, and Office applications via a specially crafted enhanced metafile image



https://www.us-cert.gov/sites/default/files/US-CERT_2012_Trends-In_Retrospect.pdf

Why does this happen?

- Lots of buggy software & wrong configurations...
  - Awareness is the main issue
- Some contributing factors
  - Few courses in computer security
  - Programming text books do not emphasize security
  - Few security audits
  - Unsafe program languages
  - Programmers are lazy
  - Consumers do not care about security
  - Security may make things harder to use
  - Security is difficult, expensive and takes time

What is This Course About?

- Learn how to prevent attacks and/or limit their consequences.
  - No silver bullet; man-made complex systems will have errors; errors may be exploited
  - Large number of ways to attack
  - Large collection of specific methods for specific purposes
- Learn to think about security when doing things
- Learn to understand and apply security principles

Terminologies

- Vulnerabilities (weaknesses) : A flaw in software, hardware, or a protocol that can be leveraged to violate security policies
- Threats (potential scenario of attack)
- Attack
  - Exploit (n) - Code that takes advantage of a vulnerability
  - Exploit (v) - To use an exploit to compromise a system through a vulnerability
- Controls (security measures)

Security Principles

- Principle of weakest link
- Principle of adequate protection
  - Goal is not to maximize security, but to maximize utility while limiting risk to an acceptable level within reasonable cost
- Principle of effectiveness
  - Controls must be used–and used properly–to be effective. they must be efficient, easy to use, and appropriate
  - Psychological acceptability
- Principle of defense in depth
- Security by obscurity doesn't work

Layers of Computer Systems

- Computer systems has multiple layers
  - Hardware
  - Operating systems
  - System software, e.g., databases
  - Applications
- Computer systems are connected through networks
- Computer systems are used by humans

Why old software can become insecure?

- Security objectives or policies have changed
  - Laws have changed
  - Business model changed
  - Company processes changed
- Environment has changed
  - Configuration is out of date
  - Operating system has changed
  - Risks are different
  - Protections have changed (e.g., firewall rules)
  - Employees, units responsibilities have changed
- Vulnerabilities have been found
  - Exploits, worms, viruses exploit them
- Input has changed
  - e.g., old application made to work online (with a wrapper)
  - Protocol changed

Ethical use of security information

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - Do *not* try these at home
- Purpose of this class
  - Learn to prevent malicious attacks
  - Use knowledge for good purposes
- Learn about cyber crimes:
  - https://tr.wikipedia.org/wiki/Bilişim_suçları
  - http://www.atamer.av.tr/bilisim-suclari/

Law enforcement

- David Smith
  - Melissa virus: 20 months in prison
- Ehud Tenenbaum (“The Analyzer”)
  - Broke into US DoD computers
  - sentenced to 18 months in prison, served 8 months
- Dmitry Sklyarov
  - Broke Adobe ebooks
  - Arrested by the FBI, prosecuted under DMCA, stayed in jail for 20 days
- Onur Kıpçak
  - http://www.hurriyet.com.tr/bilgisayar-korsanina-135-yil-hapis-cezasi-daha-40038386