Secure Programming Techniques

Meelis Roos
mroos@ut.ee

Institute of Computer Science
Tartu University

spring 2014
Course outline

- Introduction
- General principles
- Code auditing
- C/C++
- Web
- SQL Injection
- PHP
- Shell scripts
- Java
Literature

- **OWASP** (*Open Web Application Security Project*) documents

- *Secure Programming for Linux and Unix HOWTO* — Creating Secure Software


- *Secure Programming with Static Analysis*, Brian Chess, Jacob West, Addison-Wesley Professional, 2007

- SecureProgramming.com
Homework

- Several homeworks
- Find the bugs and report
Introduction

- Scope of this course
- Why programs are insecure
- Security requirements
- General principles
Scope of this course

• Learn about secure *coding* practices in popular and widely used languages and environments

• Not about exploitation of vulnerabilities — only enough to see why the problems are relevant

• Not about designing the architecture of secure systems — there’s a different course for that

• Practical project is under different course code (MTAT.07.016, [http://courses.cs.ut.ee/2014/secprog-proj/](http://courses.cs.ut.ee/2014/secprog-proj/))

• Some lab exercises (you will need a laptop)

• Some Unix and Windows system programming background is also included
Dates and times

- Question: suitable dates for exams in June?
- Another question: secure programming techniques project time?
Why are programs insecure?

- Economic reasons — consumers do not select products based on real security
  - So implementing real security is unnecessary for selling
- Security measures affect usability and waste users’ time so a real security feature might waste more time and money on global scale than possible losses from bad security
- Marketing: don’t worry, be crappy!
  - Let’s go into production with it now and we can secure it later
Why are programs insecure?

- Programmers are not taught enough
- Programmers are lazy
- Many programmers are lousy programmers
- Programmers are not security experts
- Security costs more (time, money)
- C/C++ are hard to write securely
- No thought is given to multi-user systems
- Insufficient security models
- Formal verification is rarely used
- Users don’t care
- Lots of old software is in use
Security requirements

- So, what exactly does *secure* mean?

- General security goals as usual:
  - Confidentiality
  - Integrity
  - Availability

- We need more specific requirements to be usable in validating a program

- Example: as per Common Criteria (CC)
CC Functionality Requirements

- Auditability
- Non-repudiation
- Cryptography support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of security functions
- Resource utilization
- Access
- Trusted path
CC Assurance Measure Requirements

- Configuration management
- Delivery and operation
- Development
- Guidance documents
- Life-cycle support
- Tests
- Vulnerability Assessment
- Maintenance of assurance
General principles

- Security must be designed into the system from the beginning, not patched in later
- Security can be audited only relative to knowledge in specific point of time
- Enumerating badness does not work
- Paranoia is a virtue
- Many simple bugs can appear as vulnerabilities when the data to trigger it comes from another security domain (untrusted source)
- Complexity is your enemy
Outline of next topics

- Security features
- Open Source software and security
- Disclosure of vulnerabilities
- Top vulnerability classes
Security features

- Security features ≠ secure features
- Reliable software does what it is supposed to do
- Secure software does what it is supposed to do, and nothing else
Is Open Source good for security?

- More reviewers $\Rightarrow$ more errors are found
  - And fixed?
  - What makes people review the code?
  - Closed source programs can also have stringent review procedures
- Possibility of checking the quality of code
  - "No strcat comes through the door!"
  - "Oh, the scientists again!"
- More incentives to making the code clean
- Open source by itself does not guarantee quality!
  - Many open source projects never get beyond one-man stage
Open Source and security

- Attacker has more information than with closed source
  - He can reverse engineer anyway
- Attacker has less advantages over good guys
- Trojan horses — where do they come from?
- Chance of fixing if vendor does not care or is dead
  - Or pay someone to fix it
- Conclusion: open source has the potential of getting better over time
Disclosure of vulnerabilities

- **Prehistory:** report or don’t report, most vendors pretend nothing happened
  - False sense of security
- **Full disclosure**
  - Vendors need to start patching
  - Finder gets fame
- **Responsible disclosure**
  - Vendors are given some time to fix before disclosure
  - Coordinating fixes
  - Finder still gets fame
- **"No more free bugs"**
  - Selling of vulnerabilities
Secure Programming Techniques

Top vulnerability classes (CWE 2011)

1. Improper Sanitization of Special Elements used in an SQL Command (‘SQL Injection’)
2. Improper Sanitization of Special Elements used in an OS Command (‘OS Command Injection’)
3. Buffer Copy without Checking Size of Input (‘Buffer Overflow’)
4. Failure to Preserve Web Page Structure (‘Cross-site Scripting’)
5. Missing Authentication for Critical Function
6. Missing Authorization
7. Use of Hard-coded Credentials
8. Missing Encryption of Sensitive Data
Top vulnerability classes (CWE 2011)

9. Unrestricted Upload of File with Dangerous Type
10. Reliance on Untrusted Inputs in a Security Decision
11. Execution with Unnecessary Privileges
12. Cross-Site Request Forgery (CSRF)
13. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
14. Download of Code Without Integrity Check
15. Improper Access Control (Authorization)
16. Inclusion of Functionality from Untrusted Control Sphere
17. Incorrect Permission Assignment for Critical Resource
Top vulnerability classes (CWE 2011)

18. Use of Potentially Dangerous Function
19. Use of a Broken or Risky Cryptographic Algorithm
20. Incorrect Calculation of Buffer Size
21. Improper Restriction of Excessive Authentication Attempts
22. URL Redirection to Untrusted Site (‘Open Redirect’)
23. Uncontrolled Format String
24. Integer Overflow or Wraparound
25. Use of a One-Way Hash without a Salt