Computer Security

Introduction to G53SEC

Overview of Today's Lecture:

- Instructor Information
- Module Structure
- Grading
- Motivation for the Module
- Module Contents
- Textbook and Additional References
- Summary

Contact Information:

Name: Arash Habibi Lashkari (PHD of Information Security)

E-mail: a.habibi.l@gmail.com

Personal website: www.ahlashkari.com

Course Website:

http://www.ahlashkari.com/ahlashkari-Coursework/CS.asp

Module Structure

Theoretical Part – Lectures

- Given by me
- 2 +2 hours / week
- Lecture : Thursday 11-13
- LAB : Thursday 9:11

Grading:

1 hour written examination 40 %

(Contents from all lectures text and slides [as examples: Chapters from course textbook referenced during lectures also examinable])

Coursework 60 %

(three coursework that you can find detail in coursework file in the website and download it.) More about this explain in the class!

Motivation

- People protect their property and privacy for generations (Locks, Fences, Signatures, Seals, etc…)
- Big change
- Everything becoming electronic
- And Security?
- What about Future?

What will you learn

- What is computer/information security ?
- Why is it so important ?
- How to evaluate and measure it ?
- How to enforce it ?
- How to minimise its risk ?
- The bad guy’s point of view
- The victim’s point of view

Schedule:

Introduction to G53SEC & Security
Foundations of Security
Introduction to Coursework + TSG Presentation
Authentication and Identification
Access Control …
...and its Enforcement
Security Models
Security Evaluation
Fundamentals of Cryptography
Cryptographic Applications

Schedule continued:

Network Security
User Centred Security
Software Security
Bio-Inspired Security
Hardware Security
Software Exploitation
Mobile Security
Security in an Enterprise

Revision
Revision + Exam Tips

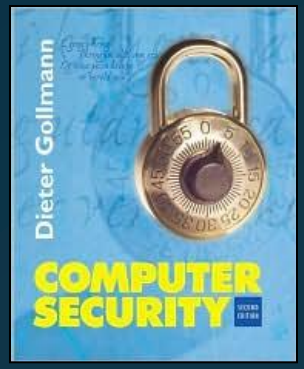
Resources

Course Text:

Computer Security – Dieter Gollmann 2nd edition (Amazon)

Security Engineering – Ross Anderson

(Available online)

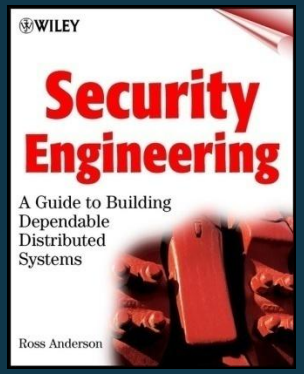


Additional Reading:

Secrets & Lies – Bruce Schneier

Computer Security: Art and Science –

Matt Bishop



Course Website (Links, Slides, etc…)

End of Part 1

Introduction to Security

Outline

- On Security
- Attacks and Attackers
- Security Management
  - Security Policies
  - Measuring Security
  - Standards
- Risk and Threat Analysis
  - Assets
  - Vulnerabilities
  - Threats
  - Risks
  - Countermeasures

A secure system is one which does not exist…

An almost secure system is one which is locked up in a nuclear bunker within an air locked titanium safe and disconnected from anything else in the world……and even such a system is not 100% secure!

- It is not about achieving complete security
- It is about minimising risk to systems
- Both from a technical as well as social point of view

On Security

- Original focus on multiuser systems
- Today focus on ubiquitous end systems
- Systems interconnected by networks
- Danger of possible attacks from *'un-trusted'* nodes
- Both remotely as well as locally (insiders)

- Primarily a management issue!

Attacks and Attackers

- Landscape is changing
- Script kiddies -> Organized crime
- Website defacement -> Personal data harvesting
- Peer appreciation -> Earning money
- Viruses -> Trojans and Denial-of-Service attacks
- Complexity of our systems is increasing
- Our understanding of the system’s complexity can’t keep up

Security

- *Reliability* – Accidental failures
- *Usability* – Operating mistakes
- *Security* – Intentional failures

1. '*Security is a people problem*'
2. Legal system defines boundaries of acceptable behaviour
3. Management responsible for security

Security Management

- Management responsible for assets
- Security measures must have clear full support of senior management
- Security awareness programs
  - – why security is important
  - - what is expected of each member
  - - which good practices should be followed
- User is not the enemy!
- Developers need even more awareness!

Security Policies

- State what should be protected
- And how this should be achieved

- Security Policy Objective
- Organizational Security Policy
- Automated Security Policy

Measuring Security

- Very difficult
- Measures only exist for some aspects of security

- Product Security
- System Security
- Cost of an Attack
- Cost of Assets

Standards

- Exist for specific industry branches
  - e.g. financial sector, government departments
- ISO 17799
  - Not a technical standard
  - Code of best practice
  - Encompasses many aspects of security
  - From policies to software and physical security

Risk and Threat Analysis

- Risk Analysis
  - All information assets
  - IT infrastructure
  - During development

Risk – *Possibility of an incident or attack to cause damage to your enterprise*

*Risk = Assets * Threat * Vulnerabilities*

Assets

- Software
- Hardware
- Data and Information
- Reputation

- Identification easy, valuation difficult
- Data, Information, Reputation – *difficult to measure*

Vulnerabilities

- Weaknesses of a system that could be accidentally or intentionally exploited to damage assets

- Badly configured accounts
- Programs with known flaws
- Weak access control
- Weak firewall configuration

- Can be rated according to impact

Threats

- Actions by adversaries who try to exploit vulnerabilities to damage assets

- Categorisation by damage done to assets
- Identification of source of attacks
- Analysis of attack execution (Attack Graphs)
- Can be rated according to likelihood

- Attack Graphs - formalized and structured
  - assessable, reproducible

Risk

Quantitative Risk Analysis

+ probability theory based on mathematical theory
- quality of results depends on quality of inputs
- not always feasible

Qualitative Risk Analysis

+ more applicable
- scaling based on judgements of security experts

Countermeasures / Risk Mitigation

- Risk analysis presents recommended countermeasures
- Risk analysis not always possible
- *Baseline protection* – security requirements for typical cases with recommended countermeasures

Summary

- Current security landscape
- Management is vital to security
- How security can be measured
- What is Risk and how it is analysed

End