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: Milena Radenkovic

E-mail: mvr@cs.nott.ac.uk

Room: B47

Course Website:

http://cs.nott.ac.uk/~mvr/G53SEC

Please contact me via e-mail before coming to see me in my office!

Module Structure

Theoretical Part – Lectures

- Given by me as well as various guest lecturers
- 2 hours / week
- Thursday 09:00 -10:00, Jubilee Campus, Exchange Building, C3
- Friday 12:00 – 13:00, Jubilee Campus, Exchange Building, C3

Practical Part – Coursework

- Assignments on protecting and identifying security vulnerabilities and improving of defences of hosts and networks (TBA)
- *Lab access*

Grading:

1 hour written examination 60 %

(Contents from all lectures examinable . Guest lectures can be used as examples but not examinable in detail.)

Coursework 40 %

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 risks ?
- The bad guy's point of view
- The victim's point of view

Resources

Course Text:

Computer Security – Dieter Gollmann 2nd edition (Amazon)

Security Engineering – Ross Anderson

(Available online)

Additional Reading:

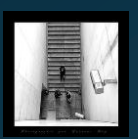
Secrets & Lies – Bruce Schneier

Computer Security: Art and Science – Matt Bishop

Course Website (Links, Slides, etc…)

End of Part 1

Introduction to Security

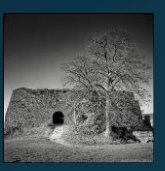


Outline

- 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 intricacies 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
- 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

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

Next Lecture: Foundations of Security – *What security actually is?*

End