Software Security
- an introduction

TDT60
06.09.2005
Information security

Organization
- Policy - rules
- Responsibility
- Information owner

People
- Users
- The insider threat
- The outsider threat
- Human error

Technology
- Hardware
- Software
- Communication
- Digital information

Confidentiality – Integrity - Availability
Software security – why is it important?

- Malicious code exploit software vulnerabilities
- Hackers exploit software vulnerabilities
- An increasing number of network-based/dependent systems
The traditional approach

• Defense
  – Anti-virus, firewalls, IDS, IPS, traffic analysis, network zones etc.

• Focus on security-functionality
  – Authentication, authorization, digital signing, PKI, secure communication, encrypted hard-drives etc.

• The problem is
  – Most defense mechanisms are software – and hence vulnerable to implementation mistakes
  – Security-functionality is part of software - and an often-used point-of-attack, but vulnerabilities may exist in other parts of software as well

Focus on fixing the symptoms – not the real problem itself!
What is software security about?

- A risk-based approach
- Requires knowledge about threats and vulnerabilities
  - to avoid common mistakes
- Design principles
  - to protect against unknown threats
- Focus on security throughout the software development and lifecycle process
  - Requirements
  - Design
  - Implementation
  - Testing
  - Maintenance