Engineering Software for Security

Owen Cheng
17-939A Class Presentation
November 28, 2001
Owen.Cheng@cs.cmu.edu

Outline

- Purpose
  - Motivation
  - Scope
- Terms and taxonomy
- Approach
- Maturation
- Research Paradigms

Purpose

- Examine
  - The evolution of principles and models
  - for systematic security design
  - to develop secure software
- Present progress on the maturation study
- Present scope and approach to obtain your opinions and feedbacks

What is Security?

- Security is a 10-headed beast
  - Broad field with many facets
  - Where does security and software engineering overlap?
- Random characterization of security engineering
  - Security is unseen, yet pervasive
  - Security design must take a holistic view
  - Security implementation must follow divide-and-conquer principle
  - One thing depends on the others
  - Human factors crucial to success of security measures
Motivation and Scope

- The process of designing for security in software development has been relatively ad hoc in practice.

- Holy Grail:
  - Given a security policy (or security requirements), automatically generate augmentation of software design with security measures.

- Scope: Principles, guidelines, and models
  - Principles for engineering security into software.
  - Guidelines for developing secure software.
  - "Security design recipe"?

Terms.2

- Computer security
  - "Broadly speaking, security is keeping anyone from doing things you do not want them to do to, with, or from your computers or any peripherals."
  - William R. Cheswick

- Information security
  - "The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use."
  - George McDaniel

Terms.3

- Security concerns (goals)
  - Confidentiality—protection from disclosure.
  - Usually stressed above all else.
  - Integrity—protection from modification.
  - Availability—protection from destruction.
  - Accountability—knowing who has had access.
  - Probably not as important.

- Security engineering
  - Identify security concerns.
  - Identify security features.
  - Determine approaches.

- Security policy
  - An informal description of the rules by which people are given access to information and/or resources.
  - Other types of policies: integrity, availability.

- Model
  - An expression of a security policy in a form that a system can enforce.
**Taxonomy**

- **Importance**
  - Provides a basis for systematic study
  - Usually a first step toward the development of principles and guidelines

- **Types**
  - Many are risk analysis based
    - E.g. Intrusion, Faults, Incidents, Vulnerabilities
  - Evaluation criteria based

- **Used as framework to describe**
  - Security faults
  - Security mechanisms
  - Function levels

**Security Taxonomy**

- SEI Barbacci et al’s Quality Attributes Report

- Principles and guidelines fall where?

**Approach**

- Examine principles and their applicability
  - Where are the principles targeted
  - Look for standardization

- Look for guidelines to apply the principles

- Examine security models and their support toward the realization of the principles
  - My problem
    - The space is too large
    - Scope of “model” not clean cut

**Data Points**

- Late 1980s–early 1990s: database security DP
  - 1975: OS Security DP
  - 1976: Bell LaPadula’s mandatory SM
  - 1972: Lampson’s discretionary SM

- 1976: Clark & Wilson’s SM
  - 1975: Chinese Wall SM

- 1988: Personal knowledge SM
  - 1989: Chinese Wall SM
  - 1990: Chinese Wall SM

- 1991: Cryptographic protocols DP
  - 1992: Liability-based DP
  - 1995: Cryptographic protocols DP
  - 1996: Clinical information systems DP

- 2000: Quantitative security DP
  - 1999: Wireless networks security issues
Some Trends

- System scale trends
  - OS
  - Network
  - Internet
  - Wireless network
- Granularity of protection
  - Resources & processes
  - Files
  - Individual fields of data

Evaluation Criteria

- Standardization of guidelines
- Provide evaluation for commercial products
- Orange book inflexible, but CC too general

Maturation

- Security design principles started coming out as early as the 1970s
- (Internal exploration??)
- 1980s marks external exploration
  - Standardization of evaluation criteria
- Evidence of popularization sparse
  - Lack of success finding developer experience reports on applying principles

Research Paradigm

- Principles papers
  - Questions:
    - Methods/Means
      - How can we do X?
      - What is a better way of doing X?
  - Results:
    - Qualitative or description model
      - Here’s a set of principles
  - Validations:
    - Experience as a qualitative model
    - Persuasion
Mission (Im)possible?

- Unfinished business
  - Sort out relationships (if any) between models and principles
  - Identify maturity phase transitions
- Send in paper outline
- Write report

THE END

- Questions/comments