Carnegie Mellon
Software Engineering Institute

Reusable Security Requirements

RE'2003 RHAS'03 Workshop
12 September 2003

Donald Firesmith
Acquisition Improvement Team
Acquisition Support Program
Software Engineering Institute (SEI)
Carnegie Mellon University
Pittsburgh, PA 15213

© 2003 by Carnegie Mellon University

In a Nut Shell

- Similar Assets, Attackers, and Threats
- Security requirements at higher level than security mechanisms (countermeasures for vulnerabilities)
- Standard types of security requirements
- Standard criteria in terms of subfactor of security quality factor, asset, threat, attacker, and situation
- Standard measures for security subfactors
- Parameterized requirements templates includes criteria and required measure

© 2003 by Carnegie Mellon University

Similar Assets, Threats, & Attackers

Assets:

- Data, software, and hardware components, communications, services, and personnel.

Threats:

- Theft, vandalism, unauthorized disclosure, destruction, fraud, extortion, espionage, trespass, etc.

Attackers:

- Crackers, disgruntled employees, international cyber-terrorists, industrial spies, governmental spies, foreign military, etc.

© 2003 by Carnegie Mellon University

Requirements vs. Architecture

- Security requirements at a higher level of abstraction than security architectural mechanisms (countermeasures).
- Many ways to meet same requirement.
- Consider identification and authentication:
  - Who you say you are (user ID)
  - What you know (password)
  - What you have (smart card)
  - Who you are (biometrics)
- Security requirements are more limited than the mechanisms used to implement them

© 2003 by Carnegie Mellon University

Types of Security Requirements

Use Quality Model of factors, subfactors, criteria, and measures.

Small number of Security Quality Subfactors:

- Access Control (Identification, Authentication, and Authorization)
- Immunity
- Integrity
- Intrusion Detection
- Nonrepudiation
- Privacy
- Security Auditing
- Survivability
- Physical Protection

© 2003 by Carnegie Mellon University

Standard Security Criteria

Standard criteria parameterized in terms of :

- Security Subfactor
- Asset Protected
- From Threat
- By Attacker Type
- Under Situation (e.g., mode of operation)

© 2003 by Carnegie Mellon University

Standard Measures

Each security subfactor has a small number of associated measures:

- % of users identified and authenticated
- % of communications with integrity intact per unit time while under attack
- % of communications remaining private per unit time while under attack

© 2003 by Carnegie Mellon University

Parameterized Rqmts Templates

Reusable parameterized requirements templates for each security subfactor:

- **Criteria**
- **Minimum required measure**

Templates are reusable, not individual requirements.

The key is determining the appropriate values for the parameters:

- **Asset based threat and potential vulnerability analysis**
- **Impact times probability**

© 2003 by Carnegie Mellon University

Example Reusable Integrity Template

Reusable Requirements Template for one of several common quality criteria for the integrity quality subfactor for the security factor:

"The [application / component / data center / business unit] shall protect the data it transmits from corruption (e.g., unauthorized addition, modification, deletion, or replay) due to [unsophisticated / somewhat sophisticated / sophisticated] attack during execution of [a set of interactions / use cases] as indicated in [specified table]. [Table of interactions / use cases versus minimum acceptable measurement level]."

© 2003 by Carnegie Mellon University

Example of Resulting Integrity Requirements

"The Global Personal Marketplace (GPM) system shall protect the data it transmits from corruption (e.g., unauthorized addition, modification, deletion, or replay) due to unsophisticated attack during execution of the Buyer use cases as indicated in the following table."

Global Personal Marketplace (GPM) Buyer Use Cases	Minimum Transmissions Protected from Corruption
Buyer Buys Item at Direct Sale	99.99%
Buyer Modifies Bid on Item	99.99%
…	…
GPM Notifies Buyer of Acceptance of Sealed Offer	99.9%

Unsophisticated attack is defined elsewhere in terms of attack type and resources.

© 2003 by Carnegie Mellon University

Conclusion

- Security requirements come in standard types with common types of contents.
- Templates can be (and have been) developed to create security requirements with standardized contents and formats.
- This has the potential to greatly increasing the quality and completeness of security requirements.
- Check out my personal website for numerous examples: www.donald-firesmith.com

© 2003 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Contact Information

Donald Firesmith
Senior Member of the Technical Staff
Acquisition Improvement Team
Acquisition Support Program
Telephone: 412-268-6874
Email: dgf@sei.cmu.edu

U.S. Mail:
Software Engineering Institute (SEI)
Carnegie Mellon University
Pittsburgh, PA 15213-3890

World Wide Web:
http://www.sei.cmu.edu/
http://www.donald-firesmith.com/

© 2003 by Carnegie Mellon University