



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**

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 12 SEP 2003		2. REPORT TYPE		3. DATES COVERED 00-00-2003 to 00-00-2003	
4. TITLE AND SUBTITLE Reusable Security Requirements				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



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**



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.



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**



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**



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)



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**



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**



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].”



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.”

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

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%



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**



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/>