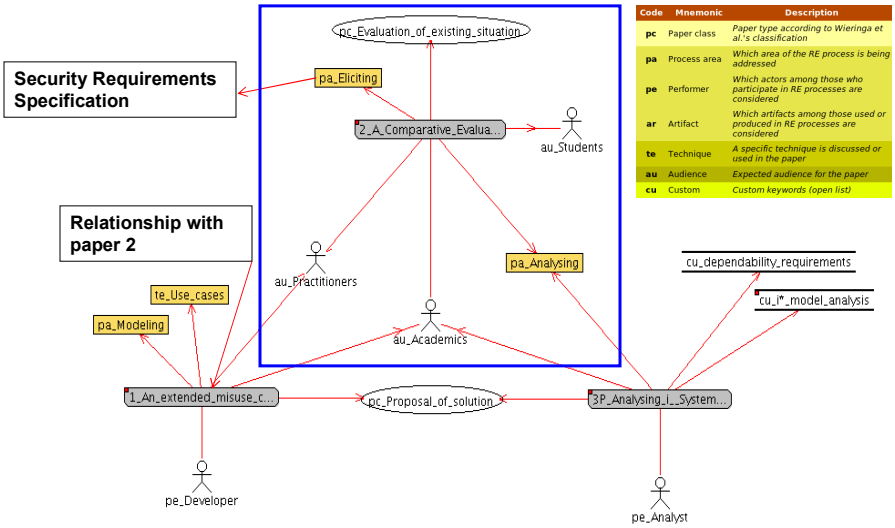
A Comparative Evaluation of Three Approaches to Specifying Security Requirements

Mamadou H. Diallo, Jose Romero-Mariona,
Susan E. Sim, and Debra J. Richardson

Donald Bren School of Information and Computer Sciences
University of California, Irvine
444 Computer Science Building
Irvine, 92697-3425, USA
{mdiallo, jromerom, ses, djr}@ics.uci.edu

A Comparative Evaluation of Three Approaches to Specifying Security Requirements



Motivation and Outline

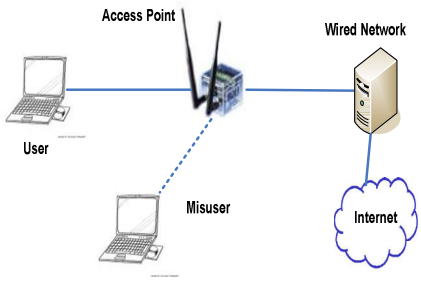
- Exponential increase of threats and vulnerabilities in software systems
- Current practices address security after systems' implementation
- Security needs to be addressed at the requirements phase
- Evaluation and comparison of three security specifications methods
  - Common Criteria, Misuse Cases, Attack Trees
- Example Application
  - Wireless Hotspot System
- Evaluative Criteria
  - Learnability, Usability, Solution Inclusiveness, Clarity of Output, Analyzability
- Evaluators' Experience
  - Two Graduate Students
  - Intermediate level of requirements knowledge

Security Requirements Methods Used

- Common Criteria
  - Developed by the US National Institute for Standards and Technology
  - Composed of three parts:
    - Introduction and general model, Security functional requirements, Security assurance requirements
  - Security Functional Requirements
    - Security Environment, Security Objectives, Security Requirements
- Misuse Cases
  - Describe scenarios from the point of view of the attacker
  - Both use cases and misuse cases can be described in single diagram
- Attack Trees
  - Models attacker's decision process in a tree
  - Can be represented textually or graphically

Wireless Hotspots

- System Model
  - Wireless computers (user or misuser), Access point, Internet
  - The vulnerabilities of the IEEE 802.11 Mac-layer
- Some Security Threats
  - Deauthentication/disassociation attacks
  - Power saving mode attack
  - Time window attack
  - Virtual carrier sense attack
  - "Evil twin" attack
- Some Solutions to these Threats
  - Delay effect deauthentication messages
  - Use data encryption
  - Control time window for short interframe space
  - Control duration of received frames
  - Use identity authentication systems



Results: Common Criteria

Security Environment
T1: Deauthentication attack
T2: Power saving mode attack
T3: Time window attack
T4: Virtual carrier sense attack
T5: Evil twin attack

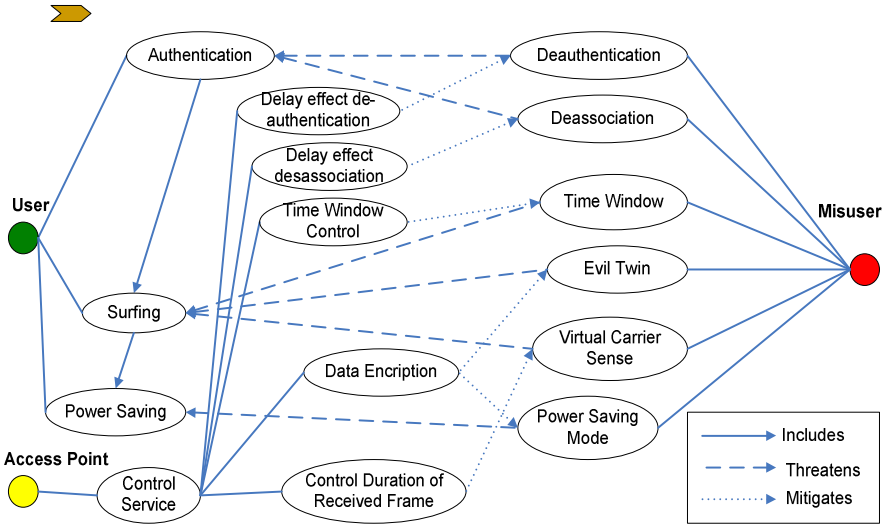
Security Objectives
O1: Delay effect deauthentication messages
O2: Control time window for SIFS
O3: Control duration of received frames
O4: Use data encryption
O5: Use identity authentication systems

Map SE and SO
T1 | O1, O4
T2 | O4
T3 | O2, O4
T4 | O3, O4
T5 | O4, O5

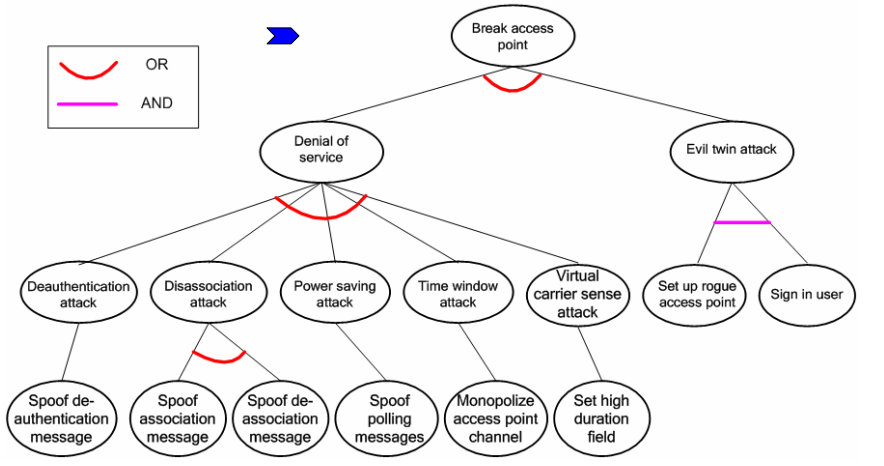
Map SO and SR
O1 | R31, R32, R33
O2 | R01, R02, R10, R11
O3 | R41, R42, R33
O4 | R10, R11, R41, R42
O5 | R22, R23, R41, R42

Security Requirements (CC Components)
0. Communication:
R01: Enforced proof of origin (FCO_NRO.2)
R02: Enforced proof of receipt (FCO_NRR.2)
1. Cryptographic support:
R10: Cryptographic key generation (FCS_CKM.1)
R11: Cryptographic operation (FCS_COP.1)
2. Identification and authentication:
R21: User authentication before any action (FIA_UAU.2)
R22: Unforgeable authentication (FIA_UAU.3)
R23: User identification before any action (FIA_UID.2)

Results: Misuse Cases



Results: Attack Trees



Analysis and Comparison

	C. Criteria	Misuse Cases	Attack Trees
Learnability	Difficult to learn – large documents	Simple to learn – based on use cases	Simple to learn – based on scenarios
Usability	Difficult to use	Simple to use – based on use cases	Simple to use – based scenarios
Solution Inclusiveness	Solution included	Solution included	Solution not included
Clarity of Output	Clear output – use tables	May be difficult to read for large systems	Clear output – use tree
Analyzability	Easy to analyze	Easy to analyze	Difficult to analyze

Since none of the techniques is an ideal technique, combining them might increase the confidence in specifying security requirements

Summary

- **Which quality features are addressed by the paper?**
  - Requirements elicitation with focus on security
  - Analysis and comparison of existing techniques
- **What is the main novelty/contribution of the paper?**
  - Critical analysis and comparison of three security requirements specification techniques: Common Criteria, Misuse Cases, Attack Trees
- **How will this novelty/contribution improve RE practice or RE research?**
  - RE practice: The study can guide designers in selecting security requirements specification techniques
  - RE research: The study can assist researchers when developing new security requirements methods
- **What are the main problems with the novelty/contribution and/or with the paper?**
  - The study reflects only our view and experience with the three methods
- **Can the proposed approach be expected to scale to real-life problems?**
  - The approach is expected to scale to real-life problems

Questions?