

Using Trust Assumptions in Security Requirements Engineering

Charles Haley
Robin Laney
Jonathan Moffett
Bashar Nuseibeh

Security Requirements Group – The Open University

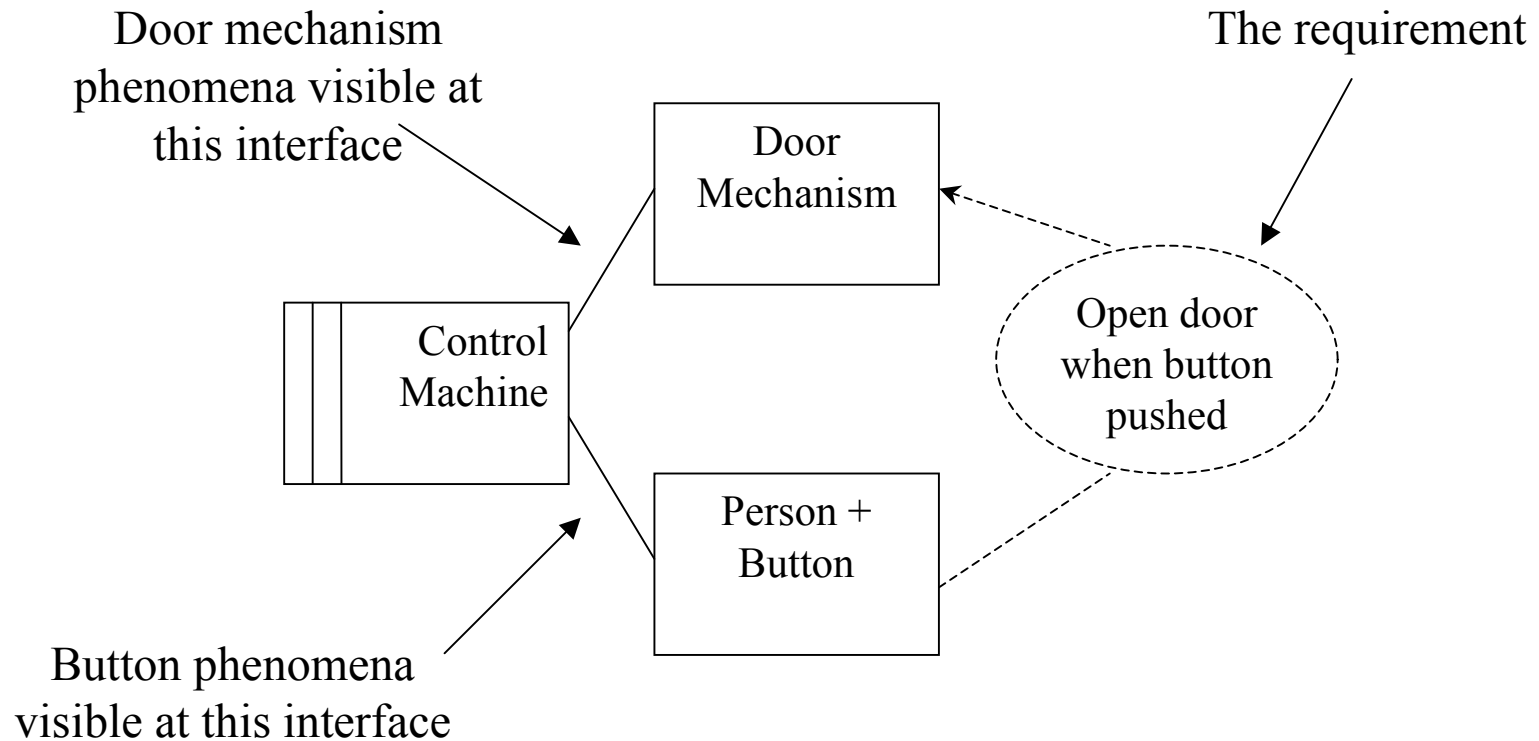
Requirements Engineering meets Security Engineering

- **Security Engineering** – focuses on designs and solutions
- **Requirements engineering** – focuses on problems, but lacks focus on security requirements
- So ... **Security Requirements Engineering** focuses on:
 - analysing security problems
 - specifying security requirements
 - relating security requirements to security solutions
- The next 9 minutes focus on the early stages of analysing security problems using:
 - Explicit representation of **Trust Assumptions**

Analysis: Requirements to Specifications

- Requirements are *optative*
 - describing the desired outcome/behaviour
- Specifications describe visible phenomena:
 - Phenomena of given domains are *indicative* – they exist
 - Phenomena of designed domains are *optative* – they should exist in the future
- Requirements are satisfied by the interplay of phenomena visible at domain edges

Example: An Internal Door Control



Security Requirements

- Represented as *constraints* on functional requirements
 - Constrain *operations* on *assets* by *actors*
 - Constraints are optative

- Constraints are satisfied by
 - Restrictions on phenomena (behavior restrictions)
 - Optative *trust assumptions* about the context of the problem

Trust Assumptions

- A domain trusts that it can *depend* upon some properties of another domain to help satisfy a security constraint
- Represents a *contract* between the domains
 - The depended-upon domain is trusted to fulfill its obligation “competently and honestly”
- The depended-upon domain may not be in the immediate problem context

Trust Assumption Example

- Using the door example presented earlier
 - Add a constraint *only members of the XXX family may pass through an inside door*
 - Add the long-term existence of a security guard at each outside door, charged with ensuring *only members of the XXX family may enter the building*

Trust Assumption Example (...)

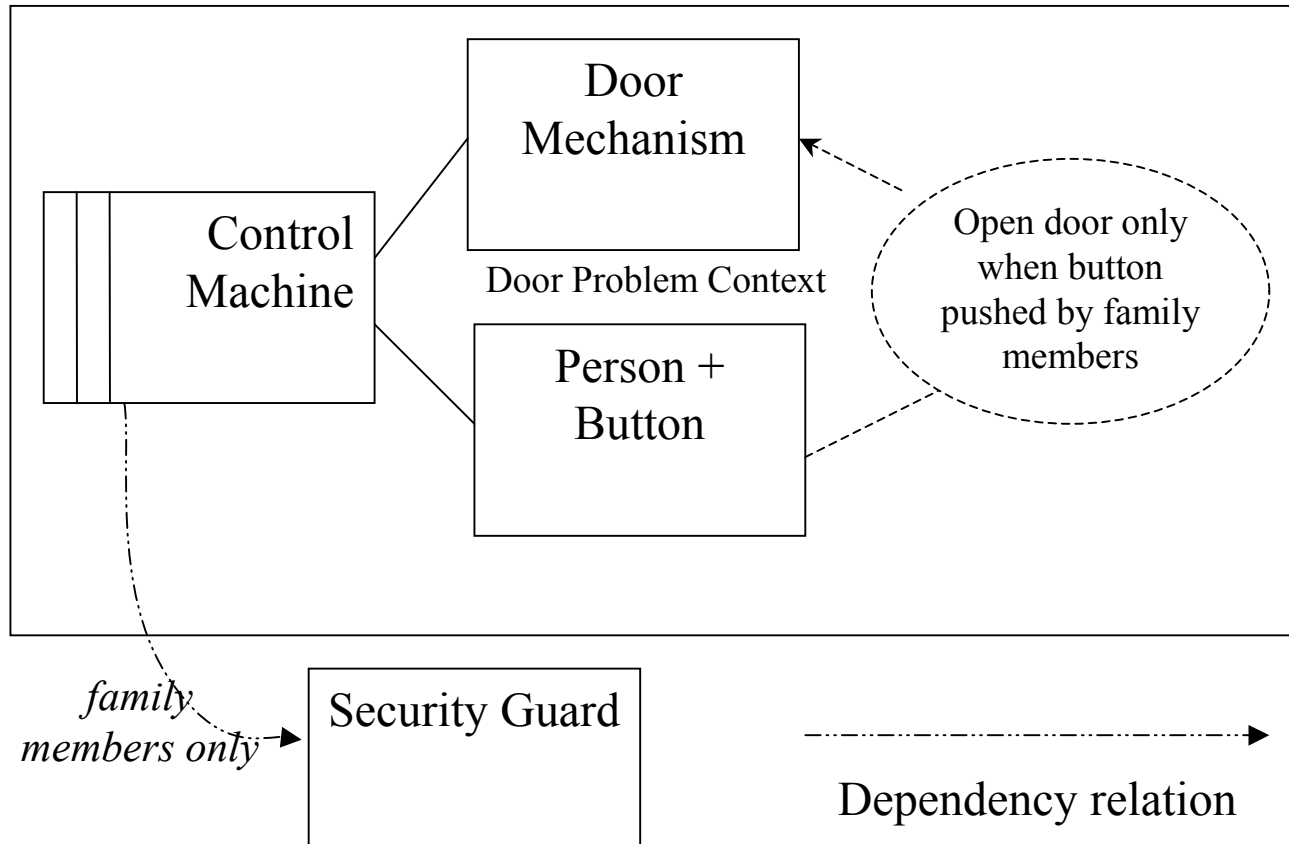
- Analyst has (at least) two choices
 - Choice 1: Verify at each inner door that the person is a family member
 - Choice 2: Trust that the security guard limits the occupants of the building to family members

- Each choice creates trust assumptions
 - Choice 1: the information used to verify family membership comes from a trusted source
 - Choice 2: the security guard does the job properly

Trust Assumption Example (...)

- In choice 2, the security guard is not directly involved in the solution
 - There is no direct exchange of phenomena between the guard and the door mechanism
- The security guard *is* part of the context
 - One cannot understand the solution without knowledge of the guard
- Thus a relation exists between the door controller and the guard

Trust Assumption Example (...)



Trust Assumptions and Risk

- Trust assumptions are just that – assumptions
 - There is some probability that the assumption will not hold
 - The higher this probability, the higher the risk
 - This probability, along with the cost associated with misplaced trust, quantifies the level of risk

Trust Assumptions & Vulnerability

- A *vulnerability* is exploited by an *attacker* to realise a *threat*
- Therefore trust assumptions represent a class of vulnerabilities
 - The assumption may be invalid
- Must determine whether the level of risk introduced by an assumption is acceptable

Conclusions

- Security requirements constrain operations on assets by actors
- Trust assumptions indicate which domains in a context help satisfy a security requirement
 - May enlarge (or reduce) the context
- Assumptions point to vulnerabilities and help determine the associated risks