

Presentation of the paper

Charles B. Haley, Robin C. Laney, Jonathan D. Moffett, and Bashar Nuseibeh, "The Effect of Trust Assumptions on the Elaboration of Security Requirements," in *Proceedings of the 12th International Requirements Engineering Conference (RE'04)*. Kyoto Japan: IEEE Computer Society Press, 6-10 Sep 2004, pp. 102-111.

# Trust Assumptions

---

Charles B. Haley  
Robin C. Laney      Bashar Nuseibeh  
The Open University

Jonathan D. Moffett  
University of York

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Outline of Presentation

---

- ▣ Research Context
- ▣ Motivation
- ▣ Background
- ▣ Trust Assumptions
- ▣ Related & Future Work

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Research Context

---

- This work is part of a larger project to:
  - Better understanding of security requirements & their impact on a system
  - Improve identification of security requirements
    - Business goals to security requirements
    - Security requirements to system behavior
  - Support expression of arguments that system behavior will satisfy security requirements

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Motivation: Satisfaction Arguments

---

- Question
  - How do we show that a system's behavior will satisfy the security requirements?
- Proposition – *satisfaction arguments*
  - A set of conditions sufficient to show that a system will satisfy a security requirement
- Issues
  - What is a security requirement?
  - What are the conditions?
  - What is level of confidence in an argument?
  - How deep/broad must one analyze/argue?

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Motivation: Scope of Analysis

---

- Is the analysis context complete?
  - Do indicative properties of unmentioned domains have a security role?
  - Can the analyst trust the stated properties of included domains to be indicative?
- Choice to trust is a choice to limit scope of analysis
  - A 'box' need not be opened
- Choice to limit scope is a choice to trust
  - Properties are assumed complete & indicative

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Motivation: Choices to Trust

---

- Analysts' choices to trust
  - Are often implicit
  - Play a large role in security requirements
    - Does one trust the administrators? The business processes? The door locks? The COTS vendors?
  - Can result in unquantified risks
- These choices are *trust assumptions*

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Background: Security Requirements ...

---

- Are usefully represented as constraints on function/behavior
- Are operationalizations of security goals
  - Business goals + assets + threats → security goals
- Are specific to the functional context
  - Security goals + functional context → security requirements
- Reanalysis required if context changes

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Background: Security Requirements

---

- Defining security requirements as constraints on function assists with satisfaction arguments
  - Can argue on basis of behavior
- Must ensure sufficient information is available to argue satisfaction
- Must choose scope of analysis wide enough to demonstrate sufficiency
  - But narrow enough to permit finishing

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

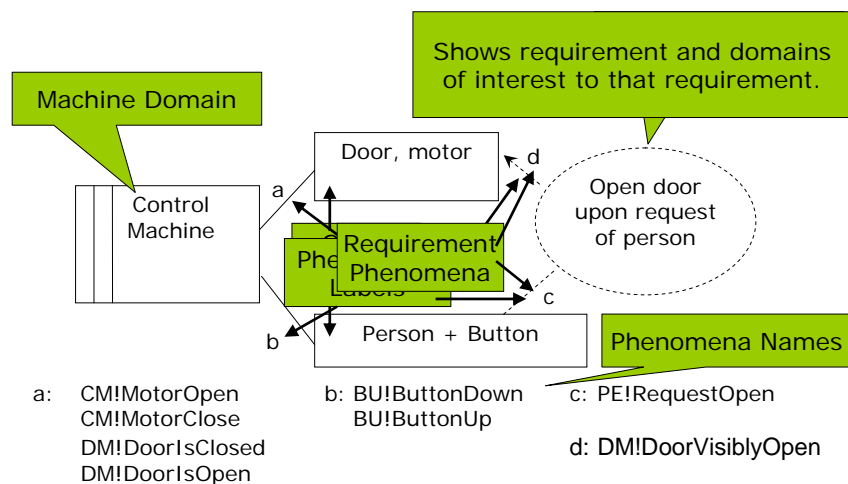
## Background: Threat Descriptions

- Represent security goals in the avoid form
- Avoid (abuse of asset to/can cause harm)
  - Abuse: action violating security principle
    - E.g. expose, alter, destroy, etc.
  - Asset: something of value to stakeholders
    - The target of the abuse
  - Harm: an undesired outcome
    - A result if the asset is abused
- Represent as tuple (action, asset, harm)

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Background: Problem Frames



RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Trust Assumption - Definition

---

- Analyst *assumes* that the membership or specification of a domain can depend on certain stated properties, up to some stated level, in order to satisfy a security requirement.
- Analyst *trusts* the *assumption* is true.

Trust: a “quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context” [Grandison & Sloman].

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Trust Assumptions - Purpose

---

- Assist with expression of security requirement *satisfaction argument*
  - *Positive* argument: the SR is satisfied.
    - Assertion that domains have desired properties
  - *Negative* argument: no contradictions.
    - Assertion that domains have no undesired properties
- Document the analyst's choice to trust & level of confidence in choice
- Thereby explicitly limiting scope of analysis

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Effect of Trust Assumptions

---

- Restricts the dependent domain
  - Membership
    - who or what makes up the population or content of the domain
  - Behavior
    - Valid phenomena
    - Valid interplay of phenomena
- TAs 'define away' potential vulnerabilities

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Trust Assumptions & Risk

---

- TA not valid → potential vulnerabilities
  - Vulnerabilities *might* exist if trust is misplaced
  - Not statement that vulnerabilities *do* exist
- Confidence in TA → confidence that hypothesized vulnerabilities do not present significant risk

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Trust Assumptions & Risk

---

- Attacks exploit vulnerabilities
  - Two risk analysis measurements: risk & impact of successful attack
- Confidence in trust assumption and risk analysis measures are independent
- May need to use both to decide to accept the trust assumption
  - Hypothesize vulnerabilities.
  - If not confident vulnerabilities are mitigated, then analyze risk

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Anatomy of a Trust Assumption

---

- Identification of the dependent domain
- List restrictions
- Explanation of restrictions
- Preconditions
- Justification
- Security requirements satisfied
- Confidence/risk

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Anatomy: List Restrictions

---

- What the trust assumption restricts
  - membership of the dependent domain
  - phenomena on the interfaces of domain
  - or some combination

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Anatomy: Explain Restrictions

---

- If restriction of domain membership
  - describe the membership of the domain before & after application of the restriction
- If restriction of phenomena
  - describe the restriction and its effect on the existence/interplay of phenomena.
  - assert that some phenomena will not appear on an interface, or will only occur in a specific sequence or interchange

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Anatomy: Preconditions & Justification

---

- Preconditions
  - List of trust assumptions that must be valid or domains / domain properties that must exist for this TA to be valid
- Justification
  - Why the TA believed valid
  - Hypothesized risks specific to this TA
  - Risks if preconditions are not honored

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Anatomy: Satisfaction & Confidence

---

- Satisfaction
  - Security requirements partially or completely satisfied by this TA
- Confidence/risk
  - Quantification of confidence the TA is valid

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Enumerating Trust Assumptions: General Approach

---

- Use business goals to determine assets
  - Then enumerate threats (threat descriptions)
  - determining security goals
- Describe problem using problem frames
- Add security requirements (constraints on function) to problem to satisfy security goals
- Develop satisfaction argument
  - Two (non-exclusive) choices to overcome flaws in satisfaction argument
    - Modify problem
    - Add trust assumptions

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Example: SET Framework

---

- Industry standard for authorizing credit card payment
- Intended to (amongst other things)
  - Prevent disclosure of credit card information to untrusted parties (e.g. merchants)
  - Verification of authorizing party (e.g. the customer)

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## SET Framework Process

---

### □ Uses

- Digital certificates to validate purchaser
- Encryption to hide info from third parties
- Digitally signed purchase authorizations

### □ Rough process

- Customer & merchant agree on purchase
- Merchant provides purchase token
- Customer signs token and card info, passes through merchant to payment gateway
- PG pays merchant

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Example Security Requirement

---

### □ Business goal: reduce credit card fraud

- Asset: money

### □ Threat description

- (Exposure, Card information, Loss of money)

### □ Function under analysis

- Authorize Payment

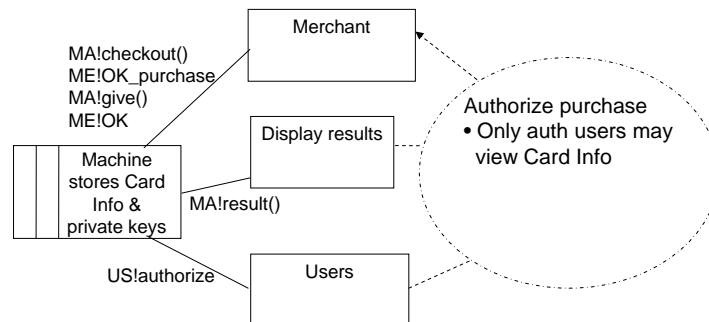
### □ Security requirement (constraint)

- Only authorized/trusted parties are permitted to see credit card information

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Example: Partial PF Diagram



RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

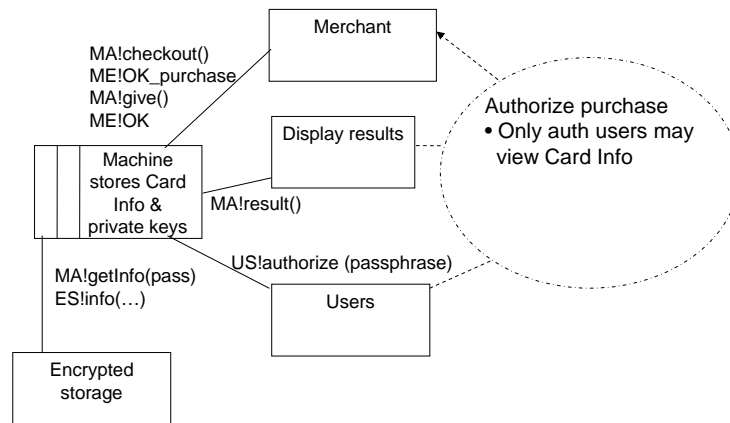
## Satisfaction Argument

- Two trust assumptions considered
  - 'Users' contains only authorized parties
  - 'Machine' cannot expose card information
- Risks behind assumptions
  - Is machine secured?
  - Can 'foreign' programs run on machine?
- Negative satisfaction argument fails
  - Trivial to demonstrate inconsistencies

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Altered PF Diagram



RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Satisfaction Argument

- Two trust assumptions considered
  - 'Users' will not reveal passphrase
  - Bad guys cannot read card info from machine's memory during authorization process
- Mitigations of risks of trust assumptions
  - User has incentive to not reveal passphrase
  - Information in memory for short time
- Negative satisfaction argument?
  - Are risks acceptable?

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Related Work

---

- Our work captures analyst's decisions
- Complements other work, e.g.
  - *i*\* & Tropos: trust assumptions are behind *i*\* leaf tasks, and in Tropos trust definitions and conditions
  - KAOS: trust assumptions are embedded in expectations (non-software agent behavior) and domain axioms
- Our work is not trust management/modeling, e.g.
  - Grandison (inter-agent trust management), Obreiter (inter-agent reputation management), Gans et al (inter-agent distrust modeling) Giorgini et al (inter-agent trust modeling)

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University

## Future Work

---

- Better traceability between security requirements and trust assumptions
  - Invalidation of the satisfaction argument
- Better support for risk/cost-based analysis
  - By using the quantification of trust
  - In choosing how to alter problems
  - In accepting the risk behind trust assumptions
- Use of TAs within other RE frameworks
- The aspectual nature of 'responsibilities' within satisfaction arguments

RE'04, 9 Sep 2004

Security Requirements Group  
The Open University