Chapter 4: Security Requirements

Raimundas Matulevičius
University of Tartu, Estonia, rma@ut.ee
Goal

• Introduce what are security criteria
• Define what are security requirements
  – How they can be classified, specified and represented
Security Risk Management
Domain Model
Outline

• Security criteria
• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation
• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
Outline

• Security criteria

• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation

• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
Security Criterion

- Property or constraint on business assets that characterises their security needs
- Act as indicators to assess the significance of a risk

- **Confidentiality** – a property of being made not available or disclosed to unauthorized individuals, entities or processes

- **Integrity** – a property of safeguarding the accuracy and completeness of assets
  - **Accuracy** could be threatened by (unauthorised or undesirable) update or tampering
  - **Completeness** could be threatened using altering or deletion

- **Availability** – a property of being accessible and usable upon demand by an authorised entity

© Springer International Publishing AG 2017
Security objective

• Defined using security criteria on business assets
  – Confidentiality of the technical plans
  – Integrity of the structure calculation process
  – Availability of ticket booking service
Outline

• Security criteria

• **Security requirements**
  – **Definition**
    – Classification
    – Specification
    – Representation

• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
What are requirements?

[Jackson 2001; Easterbrook, 2004]
What are requirements?

[Jackson 2001; Easterbrook, 2004]

- **Domain Properties:**
  - things in the **application domain** that are true whether or not we ever build the proposed system

- **Requirements:**
  - things in the **application domain** that we wish to be made true by delivering the proposed system
    - Many of which will involve phenomena the machine has no access to

- **A Specification:**
  - is a description of the behaviours that the **program** must have in order to meet the **requirements**
    - Can only be written in terms of shared phenomena!
Security requirement

- **Security requirement** is a condition over the phenomenon of the environment that we wish to make true by installing the system in order to mitigate risks
Security requirement

• A requirement defining **what level** of security is expected from the system with respect to some type of threat or malicious attack
  • what you require?
    – Different from the **security objective** (criterion)
      • not why it is needed?
    – Different from the choice of **security controls** (design)
      • not how to achieve it?
Security requirement

• A requirement defining **what level** of security is expected from the system with respect to some type of threat or malicious attack
  
  • what you require?
    – Different from the **security objective** (criterion)
      • not why it is needed?
    – Different from the choice of **security controls** (design)
      • not how to achieve it?

• **Related concepts:**
  
  – **Security**: malicious / Intended harm
  – **Safety**: accidental harm
  – **Dependability**: more general concept covering both safety, security and several other concepts
    • Availability, reliability, robustness, survivability…
  – **Privacy**: sometimes considered as a subcategory of security, but sometimes also in conflict
Objectives of Security requirements

• Ensure that users and applications
  – are identified and that their identities are properly verified
  – can only access data and services for which they have been properly authorised

• Detect attempted intrusions by unauthorised persons and applications

• Enable security personnel to audit the status and usage of the security mechanisms

[Firesmith, 2003]
Objectives of Security requirements

- Ensure that
  - unauthorized malicious programs do not infect the application or component
  - communications and data are not intentionally corrupted
  - parties to interactions with the application or component cannot later repudiate those interactions
  - confidential communications and data are kept private
  - applications survive attack
  - system (people and application) are protected against destruction, damage, theft, or surreptitious replacement
  - system maintenance does not unintentionally disrupt the security mechanisms

[Firesmith, 2003]
Outline

• Security criteria
• Security requirements
  – Definition
  – Classification
    – Specification
    – Representation
• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
Taxonomy of Security requirements

Identification requirements

- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements

Privacy requirements

System maintenance security requirements

- Physical protection requirements
- Survivability requirements
- Security auditing requirements
- Nonrepudiation requirements

© Springer International Publishing AG 2017
Identity requirements

**Identification requirements**

Extent to which a system **identifies** its externals before interacting with them

**Id.1:** The ERIS shall identify Football Federation Employees before allowing them to use its functions

**Id.2:** The ERIS shall identify Team Representatives before allowing them to use its functions

**Id.3:** The Football Federation shall identify Football Federation Employees before allowing them to enter
Authentication requirements

Extent to which a system shall **verify** the identity of its externals before interacting with them.

**Auth1:** The ERIS shall verify the identity of Football Federation Employees before allowing them to use its functions.

**Auth2:** The ERIS shall verify the identity of Team Representatives before allowing them to use its functions.

**Auth3:** The Football Federation shall verify the identity of Football Federation Employees before permitting them to enter.
Authorisation requirements

**Authorisation requirements**

- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Privacy requirements

Specifies the **access and usage** privileges of authenticated users

**Autho1:** The ERIS shall allow each Football Federation Employee to obtain access to his personal account information.

**Autho2:** The ERIS shall not allow Team Representative to *change* the Game reports.

**Autho3:** The ERIS shall not allow other external systems to *change* data
Immunity requirements

Extent to which a system shall protect itself from infection by unauthorised undesirable programs

Imm1: The ERIS shall protect itself from infection by scanning the entered data

Imm2: The ERIS shall notify the Administrator if malware is detected during a scan
Integrity requirements

Extent to which a system shall ensure that its data and communications are not intentionally corrupted via unauthorised creation, modification, or deletion

**Inte1:** The ERIS shall prevent unauthorised corruption of emails sent to Team Representatives

**Inte2:** The ERIS shall prevent unauthorised corruption of data collected from Team Representatives
Intrusion detection requirements

Extent to which a system shall **detect and record attempted access or modification** by unauthorised individuals

**Intr1:** The ERIS shall detect attempted accesses that fail identification requirements.

**Intr2:** The ERIS shall detect attempted accesses that fail authentication requirements.

**Intr3:** The ERIS shall detect attempted accesses that fail authorisation requirements.

© Springer International Publishing AG 2017
Privacy requirements

Extent to which a system shall keep its sensitive data and communications private from unauthorised individuals and programs

Pr1: The ERIS shall not store personal information about the Football Federation Employee

Pr2: The ERIS shall not allow unauthorised individuals access to communications

Pr3: The ERIS shall not allow unauthorised programs access to communications
Nonrepudiation requirements

Extent to which a system shall prevent a party to one of its interactions from denying having participated in all or part of the interaction

**NonR1**: The ERIS shall store tamper-proof records of the following information about each game: *game information*, *umpires*, *game report*, and *confirmation*.
Security auditing requirements

Extent to which a system shall enable security personnel to **audit** the status and use of its security mechanisms

**Aud1**: The ERIS shall collect the status of its security mechanisms every Friday at 18:00 h.

**Aud2**: The ERIS shall organize the status of its security mechanisms every Saturday at 18:00 h.

**Aud3**: The ERIS shall summarise the status of its security mechanisms every Sunday at 12:00 h.
Survivability requirements

- **Extent to which a system shall survive the intentional loss or destruction of its component**
  - **Sur1**: The ERIS shall not have a single point of failure.
Physical protection requirements

Extent to which a system shall protect itself from physical assault

- **Phy1**: The Football Federation shall protect its hardware components from physical damage
- **Phy2**: The Football Federation shall protect its hardware components from theft
- **Phy3**: The Football Federation shall protect its hardware components from surreptitious replacement
System maintenance security requirements

Extent to which a system shall prevent authorised modifications from accidentally defeating its security mechanisms

Main1: The ERIS shall not violate its security requirements as a result of updating data.
Main2: The ERIS shall not violate its security requirements as a result of updating hardware.
Main3: The ERIS shall not violate its security requirements as a result of the updating of a software component.
Taxonomy of Security requirements

[Firesmith, 2003]

Identification requirements

Authentication requirements

Authorisation requirements

Immunity requirements

Integrity requirements

Intrusion detection requirements

System maintenance security requirements

Physical protection requirements

Survivability requirements

Security auditing requirements

Nonrepudiation requirements

Privacy requirements
Taxonomy of Security requirements

[Firesmith, 2003]
Outline

• Security criteria
• **Security requirements**
  – Definition
  – Classification
  – **Specification**
  – Representation

What are criteria for writing good requirements?
Do not write like this

[Alexander and Stevens, 2002]

• Ambiguity – or
  – The ERIS system shall also be able to generate visible or audible caution or warning signal for the attention of security or business analyst

• Multiple requirements – and, or, with, also
  – The warning indicator shall light up when an ERIS intrusion is detected and the current Football Federation Employees workspace or Game report data shall be saved
Do not write like this

[Alexander and Stevens, 2002]

• Let-out clauses

  *if, when, except, unless, although, always*

  – The fire alarm shall always be sounded *when* the smoke in Football Federation building is detected, *unless* the alarm is being tested *when* the antivirus is deployed

• Long rumpling sentences

  – Provided that the designated Game report input signals from the specified mobile devices are received in the correct order by the way which the ERIS is able to differentiate the designators, the security solution should comply with the required framework to indicate the desired security states
Do not write like this

[Alexander and Stevens, 2002]

• Speculation
  *usually, generally, often normally, typically*
  – *Umpires and Team Representatives normally require early indication of intrusion into ERIS*

• Vague, undefinable terms
  *user-friendly, versatile, approximately, as possible, efficient, improved, high-performance, modern*
  – *Security-related messages should be versatile and user-friendly*
  – *The OK status indicator shall be illuminated as soon as possible after ERIS security self-check is completed*
Do not write like this

[Alexander and Stevens, 2002]

• Wishful thinking

100% reliable/ safe/ secure. Handle all unexpected failures. Please all users. Run on all platforms. Never fail. Upgrade to all future situations.

– The gearbox shall be 100% secure in normal operation
– The network shall handle all unexpected errors without crashing
Do not write like this

[Alexander and Stevens, 2002]

• System design:
  no names of components, materials, software objects/procedures, database fields
  – The antenna shall be capable of receiving FM signals, using a copper core with nylon armoring and a waterproof hardened rubber shield

• Mix of requirements and design:
  no references to system, design, testing, or installation
  – The user shall be able to view the current selected channel number which shall be displayed in 14pt Swiss type on an LCD panel tested to standard 657-89 and mounted with shockproof rubber washers

© Springer International Publishing AG 2017
Avoid system design elements

**Identification** requirements should not be specified in terms of

- **Who you say you are:**
  - Name, user identifier, or national identifier
- **What you have:**
  - Digital possessions such as a digital certificate
  - Physical possessions such as an employee ID card, a hardware key, or a smart card enabled with a public key infrastructure (PKI).
- **Who you are:**
  - Physiological traits (e.g., finger print, hand print, face, etc)
  - Behavioral characteristics (e.g., voice pattern, signature style)

**Authorisation** requirements should not be specified in terms of

- Authorization lists or databases
- Person vs. role-based vs. group-based authorization
- Commercial intrusion prevention systems
- Hardware electronic keys
- Physical access controls (e.g., locks, security guards)

**Integrity** requirements should not be specified in terms of

- Cryptography
- Hash Codes

© Springer International Publishing AG 2017
Good requirements

[Alexander and Stevens, 2002]

• Use simple direct sentences
  – Security analyst should be able to view ERIS status.

• Use a limited vocabulary
  – Security analyst should be able to change the infected ERIS component in less than 12 h; or
  – Security analyst should be able to reconfigure the infected ERIS component in less than 12 h
Good requirements

[Alexander and Stevens, 2002]

• Identify the type of user who wants each requirements
  – The Football Federation Employee shall be able to …

• Focus on stating result
  – … view game reports …

• Define verifiable criteria
  – … after 2 h after the game.
Criteria for writing good requirements

[Alexander and Stevens, 2002]

- **What**, not how (external observability)
  - Avoid premature design or implementation decisions
- **Understandability, clarity** (not ambiguous)
- **Cohesiveness** (one thing per requirement)
- **Testability**
  - Somehow possible to test or validate whether the requirement has been met, clear [acceptance criteria](#)
  - Often requires quantification, this is more difficult for security than e.g. for performance
    - *The response time of button press should be max 2 s.*
    - *The security of function F should be at least 99.9%*
Outline

• Security criteria

• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation

  • Text-based security requirements
  • Graphical modelling languages
  • Formal specification
Security Requirements Engineering

[Mellado et al., 2010]

• **Techniques**
  – Misuse cases [Sindre and Opdahl, 2005]
  – Mal-activity diagrams [Sindre, 2007]
  – SecureUML [Basin et al., 2006]
  – UMLsec [Jürjens, 2005]
  – Agile security requirements engineering [Peeters, 2005]
Security Requirements Engineering

[Mellado et al., 2010]

• **Frameworks**
  - Specification based framework [Hussein and Zulkernine, 2007]
  - Problem domain ontology [Lee et al., 2006]
  - Framework for security requirements engineering: representation and analysis
    [Haley et al., 2008; Moffett and Nuseibeh, 2003]
  - Security-by-ontology: a knowledge-centric approach
    [Tsoumas et al., 2006]
  - Building security requirements with [Viega, 2006]
Security Requirements Engineering

[Mellado et al., 2010]

• **Processes**
  
  – CC-based security engineering process [Mellado et al., 2007, 2008]
  
  – Security requirements for software product lines: a security domain requirements engineering process
  
  – Threat modeling as a basis for security requirements [Myagmar et al., 2005]
  
  – Software requirements and architecture modelling for evolving non-secure applications into secure applications [El-Hadary and El-Kassas, 2014]
  
  – Requirements reuse for improving systems security [Shin and Gomaa, 2007]
  
Methods
- KAOS extension to security [van Lamsweerde, 2004]
- Secure Tropos [Asnar et al., 2011; Giorgini et al., 2005; Mouratidis et al., 2007, 2010]
  - Security constraint management
  - Trust, ownership and delegation management
  - Goal risk-driven assessment
  - A three-layer security analysis framework
- SQUARE [Mead et al., 2005]
- SREBP [Ahmed and Matulevičius, 2013, 2014]
Formal specification techniques

• Specify system requirements in terms of formulae in math/logic

• **Advantages:**
  – Precise
  – Can (sometimes) prove that the system is correct

• **Disadvantages:**
  – Very time-consuming
  – Hard to understand for stakeholders who are not specialists

• Can only be used for smaller parts of systems, e.g., highly critical parts where a huge investment is feasible
Outline

• Security criteria
• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation

• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
Safety domain model

**Safety** is characterised as *unintentional* happening

![Safety domain model diagram](image)

[Firesmith, 2003]
Safety domain model

- **Asset** is anything of value that should be protected from accidental harm
- **Safety goals** state the importance of achieving a target level of safety

[Firesmith, 2003]
Safety domain model

- **Safety risk** is the potential harm to an asset due to accidents based on the vulnerabilities

[Firesmith, 2003]
Safety domain model

- **Safety policy** is a quality policy that mandates a system-specific quality criterion for safety or one of its subfactors.
- **Safety requirement** is specified in terms of a system-specific criterion and a minimum mandatory level of an associated quality metric that is necessary to meet safety policies and to mitigate the safety risks.

[Firesmith, 2003]
Outline

• Security criteria
• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation
• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation
Summary

• Security criteria
• Security requirements
  – Definition
  – Classification
  – Specification
  – Representation
• Related (to Security) Requirements
  – Safety
  – Privacy by minimisation