Lecture 6: Security Criteria and Requirements

Security Risk Management Domain Model
Outline

- Security criteria
- Security requirements  
  - Definition  
  - Classification  
  - Specification  
  - Representation
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

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

What are requirements?

• 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!
What is a 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?

• vs. related concepts:
  – Security: malicious / Intended harm
  – Safety: accidental harm
  – Dependability: More general concept covering both safety, security and several other concepts (e.g., availability, reliability, robustness, survivability …)
  – Privacy: sometimes considered as a subcategory of security, but sometimes also in conflict

Why are security requirements important?

• Sometimes tempting to ignore security
  – users / customers don’t know much about security anyway and therefore don’t know what to require

• BUT: discovery of security problems in later stages (e.g., design, coding, testing) can cause costly redesign

• In case of IT outsourcing, the security requirements are the only security you’ve got
  – Even if another company is then responsible for the technical security, it may be your problem if, e.g., confidential company data are stolen
Objectives of Security Requirements

• Ensure that users and client applications are identified and that their identities are properly verified

• Ensure that users and client applications can only access data and services for which they have been properly authorized

• Detect attempted intrusions by unauthorized persons and client applications

• Ensure that unauthorized malicious programs (e.g., viruses) do not infect the application or component

• Ensure that communications and data are not intentionally corrupted

• Ensure that parties to interactions with the application or component cannot later repudiate those interactions

• Ensure that confidential communications and data are kept private

Objectives of Security Requirements

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

• Ensure that applications and centers survive attack, possibly in degraded mode

• Ensure that centers and their components and personnel are protected against destruction, damage, theft, or surreptitious replacement
  – due to vandalism, sabotage, or terrorism

• Ensure that system maintenance does not unintentionally disrupt the security mechanisms of the application, component, or center
Outline

• Security criteria

• Security requirements
  – Definition
  – Classification
    – Specification
    – Representation

Taxonomies of security reqs

• Firesmith, 2003:
  – Identification & authentication
  – Authorization
  – Immunity
  – Integrity
  – Intrusion detection
  – Nonrepudiation
  – Nonreputation
  – Privacy
  – Security auditing
  – Survivability
  – Physical protection
  – System maintenance security
Identification requirements

• Extent to which a business, application, or component shall identify its externals before interacting

1. The application shall identify its client applications before allowing them to use its capabilities
2. The application should identify the employee by scanning his employee card data
3. The application shall identify its human users before allowing them to use its capabilities
4. The application shall not require an individual user to identify himself or herself multiple times during a single session

• 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., fingerprint, hand print, face, etc)
    • Behavioral characteristics (e.g., voice pattern, signature style)

Authentication requirements

• Extent to which a business, application, or component shall verify the identity of its externals before interacting

1. The application shall verify the identity of its users before allowing them to use its capabilities
2. The application shall verify the identity of its users before allowing them to update their user information
3. The application shall verify the identity of its client applications before allowing them to use its capabilities
4. The application shall verify the identity of the user by checking the entered social security number before allowing him to change his password

• Should NOT be specified in terms of
  – Who You Know:
    Last four digits of your social security number, mother’s maidenname, etc
  – 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., fingerprint, hand print, face, etc)
    • Behavioral characteristics (e.g., voice pattern, signature style)
Authorisation requirements

- **Access and usage privileges of authenticated users and client application**
  1. The application shall allow each customer to obtain access to all of his or her own personal account information.
  2. The application shall **not** allow any customer to access any account information of any other customer.
  3. The application shall allow customer service agents to automatically email a new customer password to that customer’s email address.
  4. The application shall not allow one or more users to successfully use a denial of service (DoS) attack to flood it with legitimate requests of service.

- **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)

Immunity requirements

- **Extent to which an application or component shall protect itself from infection by unauthorized undesirable programs**
  1. The application shall protect itself from infection by scanning all entered or downloaded data and software for known computer viruses, worms, Trojan horses, and other similar harmful programs.
  2. The application will use the Kaspar antivirus program to detect and disinfect all known viruses and Trojan horses.
  3. The application shall disinfect any file found to contain a harmful program if disinfection is possible.
  4. The application shall notify the security administrator and the associated user (if any) if it detects a harmful program during a scan.

- **Should **not** be specified in terms of**
  - Commercial antivirus programs
  - Firewalls
  - Prohibition of type-unsafe languages that may allow buffer overflows that contain malicious scripts
  - Programming standards
Integrity requirements

- Extent to which an application or component shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion
  1. The application shall prevent the unauthorized corruption of emails that it sends to customers and other external users
  2. The application shall prevent the unauthorized corruption of data collected from customers and other external users
  3. The application shall prevent the unauthorized corruption of communications passing through networks that are external to any protected data centers
  4. All the data needs to be encrypted using RSA algorithm before passing them to the communications channel

- Should not be specified in terms of
  - Cryptography
  - Hash Codes

Security requirements

- Privacy requirements
  - Extent to which a business, application, or component shall keep its sensitive data and communications private from unauthorized individuals and programs
    - The application shall not store any personal information about the users

- Survivability requirements
  - Extent to which an application shall survive the intentional loss or destruction of a component
    - The application shall continue to function (possibly in degraded mode) even if a data center is destroyed

- Physical protection requirements
  - Extent to which an application shall protect itself from physical assault
    - The data center shall protect its personnel from death, injury, and kidnapping
Security requirements

• **Intrusion detection requirements**
  – Extent to which an application or component shall detect and record attempted access or modification by unauthorized individuals
    • The application shall detect and record all attempted accesses that fail identification, authentication, or authorization requirements

• **Nonrepudiation requirements**
  – Extent to which a business, application, or component shall prevent a party to one of its interactions from denying having participated in all or part of the interaction
    • The application shall make and store tamper-proof records of the following information about each order received from a customer and each invoice sent to a customer:
      – The contents of the order or invoice;
      – The date and time that the order or invoice was sent;
      – The date and time that the order or invoice was received;
      – The identity of the customer

Security requirements

• **Security auditing requirements**
  – Extent to which a business, application, or component shall enable security personnel to audit the status and use of its security mechanisms
    • The application shall collect, organize, summarize, and regularly report the status of its security mechanisms

• **System maintenance security requirements**
  – Extent to which an application, component, or center shall prevent authorized modifications from accidentally defeating its security mechanisms
    • The application shall not violate its security requirements as a result of the upgrading of a data, hardware, or software component
Outline

- Security criteria
- Security requirements
  - Definition
  - Classification
  - **Specification**
  - Representation
Do not write like this

• Ambiguity – or
  – *The same subsystem 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 lamp shall light up when system intrusions is detected and the current workspace or input shall be saved*

---

Do not write like this

• Let-out clauses
  *if, when, except, unless, although, always*
  – *The fire alarm shall always be sounded when the smoke is detected, unless the alarm is being tested when the antivirus is deployed*

• Long rumpling sentences
  – *Provided that the designated input signals from the specified devices are received in the correct order where the systems is able to differentiate the designators, the security solution should comply with the required framework of Section 3.1.5 to indicate the desired security states*
Do not write like this

• 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

---

Do not write like this

• Speculation  
  *usually, generally, often normally, typically*
  
  – Users normally require early indication of intrusion into the system

• 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 lamp shall be illuminated as soon as possible after system security self-check is completed
Do not write like this

• 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.

Good requirements

• Use simple direct sentences

  – Security analyst should be able to view system status

• Use a limited vocabulary

  – Security analyst should be able to change the infected component in less than 12 hours
  – Security analyst should be able to reconfigure the infected component in less than 12 hours
Good requirements

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

• Focus on stating result
  – … view storm clouds by radar …

• Define verifiable criteria
  – … at least 100 km ahead.
  – **Acceptance criterion:** Aircraft flying at 800km/h at 10.000 meters towards a known storm cloud indicated by meteorology satellite report; storm cloud is detected at a range of at least 100 km.

Criteria for Writing Good Requirements

• **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 function F should be max 2 seconds"
    • "The security of function F should be at least 99.9 %"
Outline

- Security criteria
- Security requirements
  - Definition
  - Classification
  - Specification
  - Representation

Security requirements techniques

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

A systematic review of security requirements engineering
Mellado et al., 2010

• Techniques

  – Misuse Cases
  – Mal-activity Diagrams
  – SecureUML
  – UMLsec
  – Agile security requirements engineering

• Frameworks

  – **Specification** based framework
  – **Problem domain ontology**
  – Framework for security requirements engineering: representation and analysis
  – **Security-by-ontology**: a knowledge-centric approach
  – Building security requirements with **CLASP**
Security Requirements Engineering
A systematic review of security requirements engineering
Mellado et al., 2010

• Processes

  – KAOS extension to security
  – CC-based security engineering process
  – Security requirements for software product lines: a security domain requirements engineering process
  – Threat modeling as a basis for security requirements
  – Software requirements and architecture modelling for evolving non-secure applications into secure applications
  – Requirements reuse for improving systems security
  – Holistic security requirement engineering

• Methods

  – Secure Tropos
    • Security constraint management
    • Trust, ownership and delegation management
    • Goal risk-driven assessment
    • A three-layer security analysis framework
  – Modeling security requirements
  – SQUARE
  – SREBP
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

**Message to Take Home**

- Security criteria
- Security requirements
  - Definition
  - Classification
  - Specification
  - Representation