EITP20: Secure Systems Engineering — Final Exam Study Questions
Lund University

Karl Hallsby

Last Edited: March 11, 2020

Contents

1 Design Process

- Which are the steps involved in the overall design process of a secure system?
  - Describe the relationship between the different steps?
- In which way do a use-case description assist in the secure system design process?
- What is a threat analysis?
- What is the main purpose of performing a threat analysis?
- Can you give example of threat analysis approaches?
- What is the purpose of a security requirements list?
  - Can you list input sources for deriving security requirements?
  - Which are the duties of the security engineering in the security requirements gathering process?
- Can you elaborate on the main differences between security requirements and other system requirements?
- Please list at least three different "types" of security architectures?
  - Explain the main differences between the different listed types?
- Which are the main steps preceeding the actual secuirty design step?
- Explain the main design choices that need to be done at the security design process.
- List and explain different type of security evaluations that typically are done "in house"
- List and explain different type of security evaluations that typically are done by external experts
- What is a pen test and what is the purpose of such test?
- What is a protocol analysis tool and what is the purpose of using such tool?
- What is the Common Criteria (CC) standard?
  - List the 7 evaluation levels defined in CC and explain the main differences between the levels?
  - List the three different system documents part of a CC and describe their main purpose.
- What is CISSP?

2 Threat Analysis and Security Requirements

- List three different typical security threats to an IT system?
- What is the first step in an attack tree threat analysis process?
- Make an attack tree based analysis of a BankID system
- List three well established threat assessment methodologies
- Spell out the acronym STRIDE
  - Explain the meaning of the six different concepts in STRIDE
  - Give examples of attacks for the six different concepts in STRIDE
- Which are the three basic steps in STRIDE?
- Which are the two main activities in a MITRE TARA security analysis
  - Which are the main input sources to these two analysis activities?
  - The output of these two activities are stored in special databases. What is the name of these two databases?
- Describe briefly the different steps performed during a TARA CTSA
- Spell out the acronyms CAPEC, CWE and CVE

  - What does CAPEC contain and how it is used in a TARA analysis?
  - What does CWE contain and how it is used in a TARA analysis?
  - What does CVE contain and how it is used in a TARA analysis?

- Describe briefly the different steps performed during a TARA CRRA
- Where can one find TTP mitigation solutions?
- Which are the four different mitigation types?
- Which are the steps used to obtain a final ranking table for countermeasures?
- How do one select final TARA recommendations based on a countermeasure ranking table?
- Which are the three mandatory parts of a TARA TTP recommendation?
- Which are the different input sources to the security requirements derivation process?
- Which are the main outputs from the attack tree, the STRIDE and the TARA process respectively which are used to derive high-level security requirements?
- Give example of high level security requirements for a Bank ID system
- Give example of low level security requirements for a Bank ID system
- Describe a four step approach for security requirements identification and documentation

3 Security Architectures

- Describe what constitutes a security architecture and give some examples.
- The Sherwood Applied Business Security Architecture (SABSA) consist of 5 layers and one cross layer.
  - Describe the different layer views and list the names of the different layers.
  - Give examples of questions the different SABSA architecture views are supposed to answer
- Which are the three different types of security services in a logical security architecture?
  -
  - List and explain examples of services part of the non-prevention type of security services.
- Describe each of the different prevention security services in more details.
  -
  - Give example of at least four different entity security services and how they contribute to security prevention.
  - Give example of at least four different communication security services and how they contribute to security prevention.
  - Give example of at least four different application level security services and how they contribute to security prevention.
  - Give example of at least four security management services and how they contribute to security prevention.
- Draw a picture showing the relations between major different security services from a systems point of view.
- A logical security architecture can be created using a six steps methodology:
  - Describe each of the different steps
  - What is the end result?
  - Give an example of a logical security architecture
- What is a physical security architecture?
- A physical security architecture when using the SABSA include making a mapping to physical security mechanisms
  - Describe what is meant by a “Naming and registration” mechanism and give examples
  - Describe what is meant by a “Storage and runtime” mechanism and give examples
  - Describe what is meant by a “Physical security” mechanism and give examples
  - Describe what is meant by an “Authentication and session” protection mechanism and give examples
  - Describe what is meant by a “User interface and naming” mechanism and give examples

  - Describe what is meant by a "Authorization and access control" mechanism and give examples
  - Describe what is meant by a "Monitoring and incident" mechanism and give examples
- What must in addition to the security mechanisms be specified in the physical security architecture?
- Give example of platform security solution that can be used to build solutions meeting a logical security services and can be used to protect the chosen physical security mechanism?
- For the SSO logical security architecture given at the lecture, perform the following:
  - Identify the main physical security mechanisms needed in the corresponding physical security architecture.
  - Identify the main platform security components needed to fulfil the architecture
    * Suggest concrete platform security mechanisms to use for the physical realization.

4 Security Design

- Can you list four different principles upon which a security design should be based?
  - Give a motivation for each of the listed design principles
- Describe the process steps to perform when going from a security architecture to a design specification
- What is typical the role of unique identities in security systems?
  - Give example of three different widely used identity types?
- What is the problem from privacy perspective with using fixed identities?
  -
  - Describe two different methods for avoiding the identity privacy problem in a system design
- What is a digital certificate and how it is used?
  -
  - Which are the most important data fields in an X.509 certificate?
- Which is the far most used authentication principle over http?
  - Describe the different steps in an HTTP basic authentication
  - Under which circumstances can basic authentication be used
  - How are typically basic authentication treated at the server side and what is the main reason for using this type of storage?
- Describe the principles behind hardware token based authentication
- What is the rationale behind two factor authentication?
- What are the main differences between:
  - TLS server authentication
  - TLS client certificate authentication
  - TLS pre-share key authentication
- Explain the main principle behind an object security scheme
  - How does it differs from a session protection scheme like TLS or IPsec?
- What does RBAC and ABAC stand for with respect to access control systems?
  - Explain the main differences between RBAC and ABAC
- What is the purpose with an access token?
  - What does a SAML assertion contain?
- How can a Hardware Security Module (HSM) assist in protection of cloud data storage?
- List a couple of widely used commercial server anti-virus tools

- How can the security of a Docker container be enhanced beyond using default configurations?
- How can a Web design be made to make "clickjacking" less likely?
- What is the main difference between key provisioning of a public key system compare to a symmetric key-based systems?
  - What are the key issues to consider when making a public key issuing design?
  - Which are the key issues to consider when making a symmetric key issuing design?
- List the three main different intrusion detection principles and explain how they work on high level
- What is syslog and how is it typically used?
- What is the main risks with a debug interface (like JTAG) and how should it be treated in a product design to avoid these risks?
- Which are the three different most severe attacks threats against smart card designs and which are the typical countermeasures?
- Give three examples of widely used NIST security standards and what they specify?
- What does IETF stand for?
  - Give example of two well-knows IETF security standards and explain what they specify?
- Which type of security standards are done by IEEE and 3GPP respectively?
- What is the difference between public industry bodies and industry standards?
- What is meant by a cancellable biometric protection scheme?
  - Describe how to achieve a cancellable biometric matching system
  - Which alternative biometrics protection approaches can be used?

5 Security Evaluation

- What is the purpose with a security review and when should it be performed?
- At which four main levels do you typically perform a security evaluation?
  - At which occasion should they be done?
- Mention three different aspects to consider at an architecture "sanity check" review
  - For each aspect, list what should be considered?
- Mention three different aspects to consider at an architecture business review
  - For each aspect, list what should be considered?
- What do you perform during a security requirements review?
- Mention four different aspects to consider at a design review
  - For each aspect, list what should be considered?
- Describe a process for issuing and security testing of a software product
  - What is the role in the process for the security officer, the security architect, the security master and security penetration tester respectively?
- Give examples of things to consider during a performance review of a design?
- What is the purpose of trying to "measure" the security of a design?
- A simple security measurement takes three basic security characteristics into account:
  - Which three characteristics are then measured and how to you combine the measurements to get an overall measurement of a system?

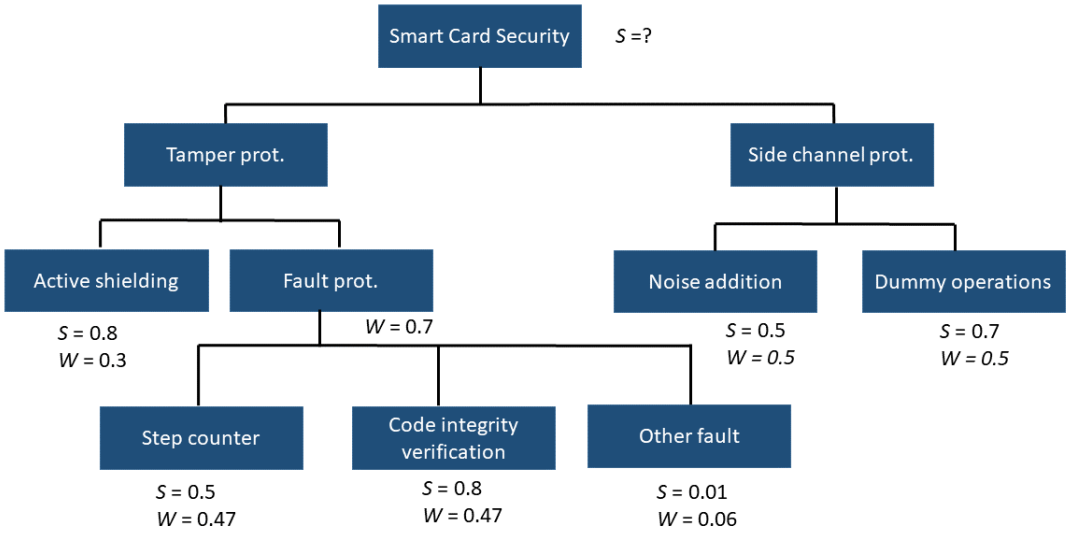

Figure 5.1: Smart Card Security System

- Consider the smart card security system in Figure 5.1. Assume the side-channel and physical channel break are equal important and the overall smart card security is the minmum strength of the two nodes. Calculate the smart card security score using the weighted weakest link approach.
- How can the sensitivity for a certain security component be calculated?
- What is a CVE database? Which organizations maintain global CVEs?
- Which are the tree basic categories for which CVE scoring is based
  - Briefly explain each of the three categories and which security aspects are considered for each of them?
- A communication product have three different categories of weaknesses, buffer overflow, TPM weaknesses, and authentication weakness with the CVE list below. Calculate an overall vulnerability score for the product (use the NIST CVE database to obtain the individual scores).
  - Buffer overflow: CVE–2019–2304, CVE–2019–2242, CVE–2019–10572
  - TPM: CVE–2019–16863, CVE–2018–6622
  - Authentication: CVE–2019–3768, CVE–2019–5108,CVE–2019–17627, CVE–2018–5389
- Explain the terms TOI, PP, ST and EAL used in CC evaluations.
- What is the purpose with the PPs?
- What is the main differences between the different EAL levels?

6 Protocol Analysis

- What is mutual authentication?
- Which attacks are typically applicable to an authentication protocol?
- What is a man-in-the-middle attack? How could you prevent it?
- What is a replay attack? How could you prevent it?
- What is a reflection attack? How could you prevent it?
- What is a labeled multiset rewriting rule? What are l, r, a?

- What is a state agent fact $St\_R\_s(A, id, \ldots)$?
- What are In and Out facts? What are Send and Recv action facts? When do you have them?
- What is a protocol rule? What is an action fact?
- What is fresh rule? What is $Fr()$ fact?
- What is infrastructure rule? How do you write the key generation for PKI? How can you generate private/public keys and publish public keys using Fr, Ltk, Out, PK facts?
- What is an initialization rule? How do you write the initialization rule for a given protocol (e.g. a public key-based protocol)? What is Create action fact?
- What is the meaning of well-formedness? How could you write protocol rules that are well-formed?
- How can you write protocol rules for a given protocol?
- Assume that you are given a public key-based protocol. How could you write the initialization and protocol rules for it? How could you prepare the protocol and split the roles?
- What is protocol instrumentation? What is a claim event $Claim\_claimtype(A, t)$?
- What is secrecy?
- How is the role instrumentation for secrecy? What is $Claim\_secret(A, M)$? Where do you place the hexagon for secret (M) in role instrumentation for secrecy?
- What is a compromised agent? When an agent is honest? What are Honest and Rev action facts?
- How can you verify if secrecy claims hold for a given protocol? (See examples in slides 31–34 of lecture 9. See also an exercise here).
- What is forward secrecy?
- How can you find out that a given protocol provides forward secrecy? (See examples in slides 36–37 of lecture 9).
- How is the role instrumentation for authentication? What are $Claim\_commit$ and $Claim\_running$ events? Where do you place Commit and Running hexagons when A wants to agree with B? Where do you place them when B wants to agree with A?
- How do you model a protocol using Tamarin? How do you write a labeled multiset-rewriting rule in Tamarin?
- What are linear and persistent facts in Tamarin? When do you use ! or ˜ or $ in Tamarin?
- What does $\langle x, y \rangle$ mean in Tamarin?