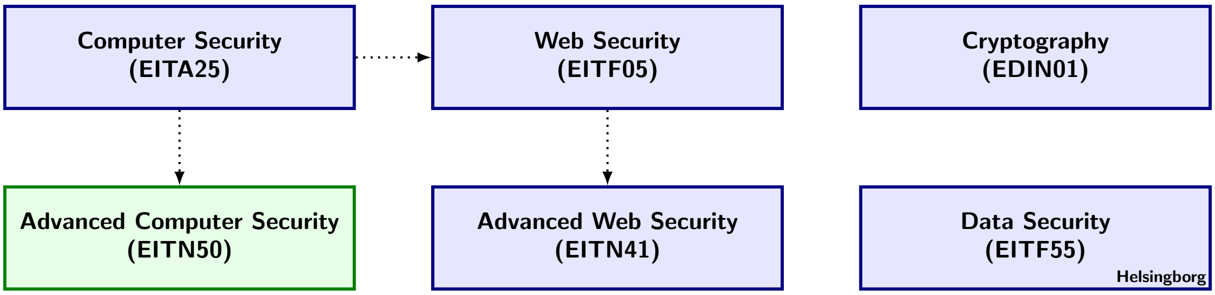
Advanced Computer Security 2017

Department of Electrical and Information Technology
Lund University

Project: Trusted Camera

Learning goals:

- Apply and test insights on trusted computing technology.
- Analyze potentials threats and design counter measure.
- Develop skills to analyze a security design.
- Develop skill to document a security design.


Computer Security (EITA25)

Web Security (EITF05)

Cryptography (EDIN01)

Advanced Computer Security (EITN50)

Advanced Web Security (EITN41)

Data Security (EITF55)

Helsingborg

Preparations

This project concerns a design of a surveillance camera that is mounted in a building. The design concerns how the camera can be made into a trusted product, that is a product that is capable to protect its operation and the data it streams. To prepare yourself for this project do the following:

- Read the course slides on trusted computing technologies.
- Read information on Common Criteria and EAL2 level,
- Read the entire project description (this document) before you begin.

It is of course helpful that you pass the quiz Trusted Computing in EIT Elearning (`http://elearning.eit.lth.se/moodle`).

Instructions for Project Approval

- Indicate on the front page your group number in addition to your name(s).
- Indicate the version date of this document upon which you base your work an report.
- Structure your report document as described in the section ”Documentation”.
- IMPORTANT: You have to submit the project report to the server at `https://eitn50.eit.lth.se:3119/`. There you (the group leader) will find the page for uploading your reports. Note that your initial password is your personal number and the username is your STIL identifier. Change the initial password after you have logged in the first time. After login read the instructions and information (information there overrides any instructions/information in this document) After login, you upload your report, NOT LATER THAN Oct 19, 23.59, in PDF form. The submission should be anonymous and the pdf file should NOT carry any of your group members names. After this deadline, the server will select two reports for peer-review by your group. You can download the reports that you should review and grade from the server. You enter your peer-review results into the server not later than the given report date, that is likely about one week later. You can, after this 2nd deadline, make improvements to your report based on the comments of from the two groups the reviewed your report. At that point you should add, at the end of your report, an improvement sheet with a summary of the changes you made to your report. Send this final report to `ben.smeets.lu@analys.urkund.se` and MARK it with your group number.
- A review is to be written densely on at most one A4 page. Verify that the report clearly states your design choices, the TOE, and considered requirement such that you or another student is able to review the report. Give encouraging feedback on the good parts, and identify the major points of improvement. You may check for structure, language, technical correctness, readability, and so on. Be constructive, do not nit-pick. Suggest ways of improving the report.
- The grading criterions are given in the ”Documentation” section.

Document change history

Table 1 shows updates of this document. See to it that you have always the latest. Old versions of this report can be found using the link structure below. `http://www.eit.lth.se/fileadmin/eit/courses/eitn50/Project_TC/Project_TC_2017_10_04.pdf`

Version	**Comment**
2017-10-04	preliminary version for 2017. Grading instructions TBD

Table 1: Document version history

1 Introduction

The purpose of this project is to study a "real case" problem that requires security mechanisms in its solution. The project aims at going through the analysis and design stages of the development process.

There are several functional requirements on the product that we list below that you have to take into account.

- The camera streams its data with SRTP, [6] which requires a key.
- One must be able to securely update the firmware of the camera.
- The camera should have a unique, cryptographically strong, identity that is programmed during camera manufacturing.
- The camera has a flash memory that stores the firmware and configuration data as well as 1 hour of recorded video with the latest 60min of video.
- User information and data stored on a camera sent in for repair should not be accessible for repair personnel.
- When the camera is decommissioned, it should be easy for the user to make stored user information and data stored unreadable (or wiped).
- The camera should have a management interface through which one can get attested information of what firmware is loaded and the hash of the key used to protect to recorded video and the SRTP channel.
- Camera housing should have a tamper sensor that detects that the camera has been opened.
- Take into consideration that the product may be delivered from the factory with functional errors/bugs. Hence it must be necessary to handle HW fixes (SW patches that overcome HW problem) and or fixes in permanent code in the device (e.g. pathes to ROM code functions).

Note that through so-called function pointers or patches of function call one can realize a jump to routines that patch HW bug.

There are several threats that one considers to be crucial and one is required to design protection for.

- Bugs in the (remote) management interface that allows one to insert executable foreign code.
- Loading of unauthorized firmware.
- Loading of SRTP keys of incorrect receiver.
- Opening camera device and replace flash memory contents with own code and configuration.
- Dishonest device repair personnel.
- Misuse of JTAG debug interface.
- Loss of key or compromised camera (fallen into the hands of a stranger).

In addition, the logistics of handling keys should not only be secure but also cheap to operate. Likewise production steps should be fast since we deal with a product that we believe will be sold in vary large number of quantities.

You likely need to make choices if your product is a consumer product or is intended for professional use (or both). Such choices may likely have impact on how need to cope with threats. Explain your choices. You can add hardware and takeout some components to meet your wishes. Adding HW increases costs and removing reduces costs but you may loose the capability to implement a protection feature.

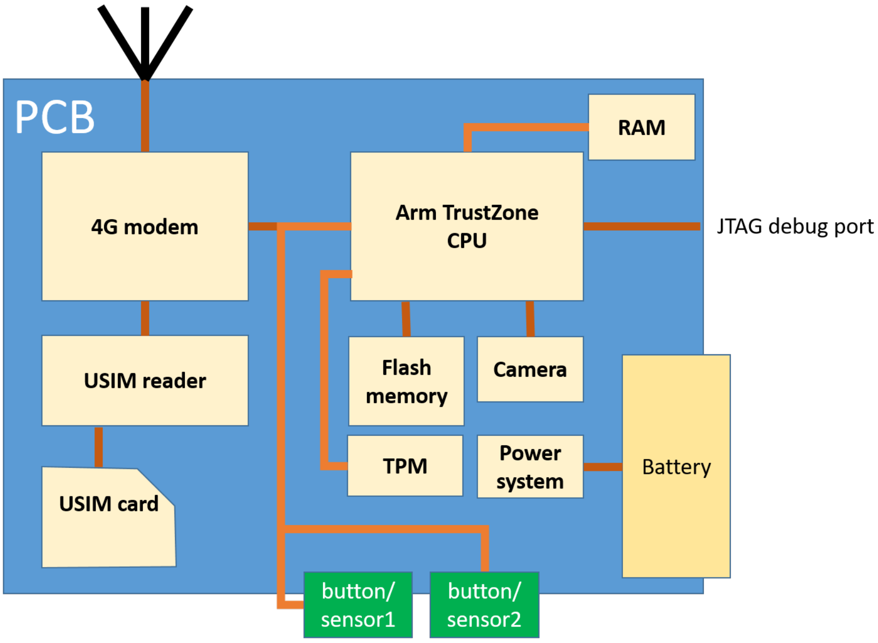


Figure 1: Trusted Camera components

Where you are missing information to complete your design you may/have to fill-in the missing parts yourself. Be prepared to motivate your choices.

2 Project Description

We have a battery driven camera device that has the following components: camera, PCB board with flash memory, RAM, ARM TrustZone CPU, TPM, JTAG debug interface, LTE subsystem with USIM card reader, and special Flash to hold an ID. The battery is connected via a power management system, see Figure 1. You can assume that the battery is normally connected to a charger and that the battery lasts for 3 days of operation or recording and transmission.

Based on the requirements you should come up with an architecture/desing of the camera device that meets the security, production and maintenance requirements. You have to document the design and your motivations in the projects report. In your design you can use various features from course material presented thus far but you make use other insights too.

3 Documentation

The expected final documentation output is a report bundle in the form of a pdf-file, about 9-11 A4 pages long, as specified below. Of these page, 3-4 pages concern the review and correction process.

- Front page with the names of the group members. (1 page)
- Description of your product and considered design requirements (0.5 page)
- Assumptions for your product that affect security (0.5 page)
- High-level architectural overview. (2-3 pages)

- Security evaluation of the design and short summary (2 pages)
- Peer-reviews of your report. (2 pages)
- Improvement sheet for the final version. (1-2 pages)

Pictures are excluded from the page count.

You are encouraged to use a TeX editor (Texmaker[1], TeXnicCenter[2],. . .) to write the report and compile the report bundle above into a single pdf-file. This is particularly encouraged if one or more of your group members have never used TeX before.

The first part is a short *high-level* architectural overview that explains how your design is *structured.* The level of your description is the important focus here. Motivate your design choices. Do not go into insignificant details. Upon reading your architectural overview, the reader should clearly, correctly and quickly understand the structure of your system. You are required to draw an image to illustrate this structure (half page).

Your main challenge here is to use your technical writing ability to explain technical details in a way that is easily absorbed and not so easily misunderstood. Keep your description at a high structural level. Only include details if they are important from a security perspective.

The intended audience for this part should be a student in your program that has only taken the Basic Computer Security course. Upon reading your description, the reader should understand the structure and main points of your protection system.

This part should contain your Target Of Evaluation (TOE) and Security Target (ST). Here you can be informal and not follow the Common Criteria style of naming.

The second part is a short *Security evaluation* of your design that explains what types of protection you use and why. The list of security consideration should list all attack types and major security issues you can think of and explain if, why and/or how it is or is not applicable to your system. For each attack/issue, explain clearly and concisely what you have done to protect your solution. Or briefly explain why no protection is needed. Your report should clearly contain a description that gives the motives of your security related design choices.

Do not forget the consequences for design choices for the manufacturing and repair costs.

Your evaluation should contain a table which row wise lists the threats that you considered and as columns your countermeasures. If a countermeasure is relevant to protect against a threat you mark this row-column position with on 'X'.

3.1 What You Should Think About

The focus of this course is on computer security and platform security in particular. Write so other groups can understand.

3.2 Grading instruction

NOT READY

You have to grade two reports. For the grading you use the following template that is given in table 2. The sum of the grades have to be entered in the review report. Later this will be mapped to 'VG', 'G', or 'U'(= not passed). This mapping is TBD.

[1] http://www.xm1math.net/texmaker/

[2] http://www.texniccenter.org/

item	**Grade instructions**
Report structure	follows instruction = 2, doesn't = 0
Design Assumptions	clearly described = 2, unclear = 1, absent = 0
Product use considerations	clearly described = 2, unclear = 1, absent = 0
TOE description	clearly described = 4, unclear = 2, absent = 0
Security Evaluation details	clearly described = 4, unclear = 2, absent, too few = 0
Design evaluation overview	stated = 2, two or more errors= 1, many errors or absent = 0
Summary	stated = 2, unclear = 1, absent = 0

Table 2: Grading template

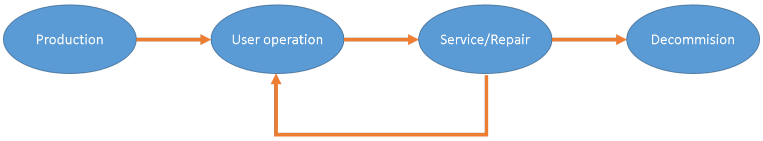


Figure 2: Simple Life cycle for the camera product.

4 Resources

- Literature on TPM 1.2.
- Common Criteria approach to the use of an ST as a way to define what the TOE is; [1] through [3] or [4]. You do not have to understand all the details but sort of pick up the idea to structure your design and analysis.
- Course slides on connections security and trusted computing.

5 Hints

Here are some useful hints.

Hint 1: First read quickly through the references what a TOE is. That should basically do and will help you to structure your security analysis. If you want to read more you can, for example, look at [1] through [3].

Hint 2: Make a small figure that shows the life-cycle of the device as shown in Figure 2.

Hint 3: Make a table of threats to your TOE and number these threats. Then make a list of protection features in your design and make a matrix with threats as rows and protection features as columns. Then indicate by a "X" if a a protection feature protects against a threat. Check that all rows contain at least one "X". Try to limit yourself to the threats that are important. Often one can find many variants of threats that are rather the same or use a common principle. In such a case take then only one of the variants as threat in your table. On may expect here maybe not more than 10 to 20 threats.

Hint 4: You likely have to make assumptions to fill in details that you need. Keep a record of these assumptions. It will help you later to check if you haven't missed anything of importance and is will help you to answer questions when you do the presentation.

References

[1] Slides on CC, https://www.cs.utexas.edu/%7Ebyoung/cs361/lecture77.pdf

[2] Slides on Protection Profile https://www.cs.utexas.edu/%7Ebyoung/cs361/lecture78.pdf

[3] Slides on Security Target (ST): https://www.cs.utexas.edu/%7Ebyoung/cs361/lecture79.pdf

[4] CC Introduction http://www.fmv.se/Global/Dokument/Verksamhet/CSEC/ccintroduction.pdf

[5] Sectra lecture on CC at Linkping University:
https://www.ida.liu.se/ TDDC90/literature/slides/TDDC90-CC.pdf

[6] https://tools.ietf.org/html/rfc3711

6 Appendix: Target of Evaluation

When giving an security analysis of a system one can apply the methodology used in the Common Criteria standard. An important step is the determination and specification of a Security Target (ST) and the Target of Evaluation (TOE). Common Criteria has a well-defined approach how to establish an ST and a TOE. The references contain some light-weight descriptions of the mind set of how to arrive at an ST and TOE. Read these references to grasp the essence, rather than trying to understand all of it. Especially when aiming at a high level of assurance Common Criteria becomes very cumbersome. In this project we just use the ideas and you do not have to, nor are encouraged, to follow Common Criteria by the book.

Yet, think of the TOE as the definition of the system from a security perspective telling what parts of the actual systems are considered in the security analysis. In this process one not only describes the system components that are considered but one equally defines a) assumptions made in the design and analysis and b) conditions and assumptions that are purposely left out of considerations or that are assumed to be valid. An example of the latter could be ”the opening of ASICs and their reverse engineering” is not considered to be a threat to the TOE. Here one must balance between being ambitious to include essentially all possible threats and being very narrow by placing many threats as part of the assumed environment that are not addressed. Very often one sees in an ST that environmental aspects like training of involved personnel is mentioned as something that is assumed to have taken place.

Depending on the CC evaluation level that one is aiming for the strictness of the analysis and the amount of documentation will increase. But even at EAL2 which we sort of aim for here the amount of work can be considerable if the TOE is taken to cover a large system. Therefore often a TOE is only taken as consisting of a security critical subsystem.

In this project use common sense to arrive at a ST and TOE and document your motives so you can later provide answers on the choices you made.