JÖNKÖPING UNIVERSITY
School of Engineering

Anmälan om examensarbete – Datateknik 15 hp

Registration final thesis work – Computer Engineering 15 credits

Studenter/*Students*

Namn student 1 *Name student 1* Adina Valjakka	Namn student 2 *Name student 2* Anton Ahlinder
Personnummer *Personal number* 20000409-7705	Personnummer *Personal number* 19961012-5099
Program *Programme* Datateknik. inbyggda system	Program *Programme* Datateknik. inbyggda system
Mobilnummer *Mobile number* 0704539743	Mobilnummer *Mobile number* 0729755051
E-post *E-mail* vaad19uj@student.ju.se	E-post *E-mail* ahan19tp@student.ju.se
Jag kan tänka mig skriva på engelska[1]: *I am open to writing in English* Ja *Yes, if required*	Jag kan tänka mig skriva på engelska[1]: *I am open to writing in English* Ja *Yes, if required*
Jag uppfyller förkunskapskraven[2] enligt kursplan: *I fulfil the prerequisites[1] indicated in the course syllabus* Ja *Yes*	Jag uppfyller förkunskapskraven[2] enligt kursplan: *I fulfil the prerequisites[1] indicated in the course syllabu* Ja *Yes*

Företag/organisation *Company/organisation*

Namn *Name* Click or tap here to enter text.
Kontaktperson *Contact person* Click or tap here to enter text.
Mobilnummer eller växelnummer *Mobile number or switchboard* Click or tap here to enter text.
E-post *E-mail* Click or tap here to enter text.

JÖNKÖPING UNIVERSITY
School of Engineering

Projektbeskrivning - Mer information under rubrik ”Förklaring projektbeskrivning”

Project description - More information under heading ”Explanation project description”

Examensarbetets titel (preliminär) *Title of final thesis work (preliminary)*

We do not wish to do our actual thesis on this topic, just to pass the assignment

Security in embedded systems: An inductive qualitative study on security practices in embedded development.

Ämne/huvudområde *Subject area/main field of study* (För Dmp/Dis: Datateknik *Computer Engineering*)

Computer Engineering

Sammanfattning *Executive Summary*

This thesis aims to investigate design guidelines and methodologies for ensuring security in embedded systems. This includes to research what cybersecurity standards a developer within embedded systems needs to follow to ensure security in their design; and to answer the following questions:

- Which guidelines and methodologies should be followed when designing an embedded system with the purpose of withstanding software and hardware attacks?
- What makes an embedded system secure?

Företagets/organisationens mål *The objective of the company/organisation*

Click or tap here to enter text.

Problemformulering *Background*

Embedded systems can be vulnerable to security threats due to their characteristics. Due to embedded systems' resource constraints and design limitations, such as power, memory, and processing, implementing security measures presents challenges. Physical exposure of the hardware also contributes to the challenges of incorporating security measures in the design of an embedded system. Many modern embedded systems store or access sensitive data, which makes security a vital part in their design. The monetary value of data, the potential for serious harm, and the connectivity and interoperability of embedded systems, including mission-critical ones, make embedded systems popular targets for cyber attacks (BlackBerry QNX n.d). Many machines that utilize embedded devices are also connected to the internet. As a result, hackers are able to gain unauthorized access to them and run malicious code. An embedded device that has been hacked can sometimes affect other connected components, and/or completely disable an embedded system (Secure code warrior 2021).

The current research of cybersecurity within embedded systems focuses on common attacks with malicious intent and countermeasures. There is a gap in research of design principles and methodologies that developers can follow to ensure security in their embedded systems. This thesis will investigate guidelines and methodologies to follow when designing an embedded system, from a security perspective, and provide the reader with an overview of methods that can be used in the design-process to limit the risk of security breaches.

BlackBerry QNX n.d., *Ultimate guide to embedded systems security*, accessed 14 November 2021, https://blackberry.qnx.com/en/embedded-system-security/ultimate-guide/

Secure code warrior 2021, *Why end-to-end security is important in embedded systems*, accessed 14 November 2021, https://www.securecodewarrior.com/blog/embedded-systems-security

Syfte och forskningsfrågor *Purpose and research questions*

The purpose of this thesis is to investigate and establish which design methods and guidelines should be taken into account when developing an embedded system with security in mind.

An embedded system that downloads and executes applications is most vulnerable to attacks caused by malicious software, such as viruses and trojan horses (Ravi, Raghunathan, Kocher & Hattangady, 2004). The use of electronic devices, such as cell phones, extends beyond the private sphere to offices, government agencies, and even the military. These embedded devices contain valuable and sensitive information, which means they are at risk of being attacked on a daily basis (Elmiligi, Gebali & El-Kharashi 2016). In order to identify the correct requirements for an embedded design early, the developer should be aware of what guidelines and methodologies should be followed in the design-process to ensure the security of the system. Thus the first research question is:

[RQ1] Which guidelines and methodologies should be followed when designing an embedded system with the purpose of withstanding software attacks?

Malicious software is not the only threat to the integrity of embedded systems. Due to the module often being installed in areas accessible to anyone they are also susceptible to a wide variety of physical security breaches such as invasive attacks, timing attacks and power attacks (Fournaris & Sklavos, 2014). The embedded system devices that are traditionally designed and built primarily for reliability, performance, and real-time responsiveness do not have adequate protection against attacks (Fournaris, Pocero & Koufopavlou 2017). Therefore the second research question is:

[RQ2] Which guidelines and methodologies should be followed when designing an embedded system with the purpose of withstanding physical attacks?

By evaluating the answers to the previous research questions we will be able to create a collection of security related methodologies and guidelines. By using these guidelines, it will be easier for developers to implement the design of an embedded system correctly. Hence the third research question is:

[RQ3] What makes an embedded system secure?

Elmiligi, Gebali, F., & El-Kharashi, M. W. (2016). *Multi-dimensional analysis of embedded systems security.* Microprocessors and Microsystems, 41, 29–36. https://doi.org/10.1016/j.micpro.2015.12.005

Fournaris, & Sklavos, N. (2014). *Secure embedded system hardware design – A flexible security and trust enhanced approach.* Computers & Electrical Engineering, 40(1), 121–133. https://doi.org/10.1016/j.compeleceng.2013.11.011

Fournaris AP, Pocero Fraile L, Koufopavlou O. *Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: a Survey of Potent Microarchitectural Attacks*. Electronics. 2017; 6(3):52. https://doi.org/10.3390/electronics6030052

Ravi, Raghunathan, A., Kocher, P., & Hattangady, S. (2004). *Security in embedded systems: Design challenges*. ACM Transactions on Embedded Computing Systems, 3(3), 461–491. https://doi.org/10.1145/1015047.1015049

Metod *Method*

To answer the research questions an inductive qualitative theoretical research will be conducted. The decided method of research will be a literature review of the current countermeasures used to prevent security breaches in embedded systems. The data collected from the review will be analyzed with the intention of finding similarities in design. These similarities will then be compiled into guidelines and methodologies to be followed when developing embedded systems.

By using an inductive approach, new theories for guidelines and methodologies will be proposed towards the end of the research process, as a result of observations within the current field of research. Qualitative data from existing research will be used to develop new guidelines and methodologies based on analysis and interpretation of the data.

Relevans för ämnet/huvudområdet *Relevance to the main field of study*

The topic of design guidelines and methodologies for ensuring security in embedded systems builds on the content of the following courses within our education programme:

- Microcontrollers
- Electronic interfaces
- Digital electronics with VHDL
- Object-oriented software development

The courses listed above gave us knowledge in how to develop embedded systems and software design patterns, and have provided us with a foundation to conduct research within the topic of design guidelines and methodologies for embedded systems.

Feedback:

- Too big
- Security? What does it mean?
- Subset of embedded applications, motivate why you chose that one, critical, 90% of market?

- Inga ja/nej research questions
- Inga benchmarks