FOM Hochschule für Oekonomie & Management

Hochschulzentrum Düsseldorf

Exposé

in the study course Wirtschaftsinformatik - Business Information Systems

to obtain the degree of

Bachelor of Science (B.Sc.)

on the subject

An Infrastructure for a Challenge-Response based Authentication System using Physical Unclonable Functions

by

Luis Pflamminger

Advisor:	Prof. Dr. Bernd Ulmann
Matriculation Number:	538276
Submission:	2022-08-31

Contents

List of Abbreviations

PUF	Physical Unclonable Function
CRP	Challenge-Response Pair
RFID	Radio-Frequency Identification
POC	Proof of Concept

1 Problem Statement

The thesis is part of a research project concerned with developing an authentication system that makes use of Physical Unclonable Functions (PUFs) for asserting identities. Authentication is the act of establishing a persons identity by having them prove that they are, who they say they are [cp. 1, p. 398].

In today's electronic access control systems, digital keys are used for authentication. They are stored in a database and assigned to a physical entity like a person's fingerprint or a smart card. This approach can be problematic, as the digital key is not directly bound to the physical object. If an attacker were to gain access to the key, they could use it to create a copy of the physical entity and gain access. [cp. 2, p. 81]

A solution to this might be PUFs, which are physical devices, instead of digitally stored keys. During manufacturing, certain uncontrollable production tolerances lead to each device differing slightly from every other. This introduces unique characteristics and a certain variability and randomness into every PUF, which can be used to create a unique fingerprint of every device without the need for a digital key. While the variation is measurable, it is considered impractical to create an identical physical copy of a PUF, because it is deemed impossible to gain full control of the tolerances and imitate the slight variations of another PUF, that were introduced in manufacturing. [cp. 2, p. 81]

The physical characteristics of PUFs have to be measured to be able to infer an identity from them. This is done using a Challenge-Response Pair (CRP). The challenge is some input given to the PUF, which uses it to generate an output (the response), leveraging its unique characteristics. For the same challenge, each individual PUF will therefore generate a different response. By previously generating and recording specific CRPs or using neural networks to evaluate a response to a given challenge, the authenticity of a given PUF can be established. [cp. 2, p. 81]

This thesis focuses on the infrastructure behind a challenge-response based authentication system using PUFs. This includes designing a database for storing the required data, specifying a protocol for communication between the components, developing a backend for generating and sending challenges to the PUF and evaluating the responses, among other things. Because of this focus the thesis has been titled:

An Infrastructure for a Challenge-Response based Authentication System
using Physical Unclonable Functions

2 Research Questions

It is hard to define specific research questions for this thesis, as more literature research is necessary to understand, which components the infrastructure consists of and what the main challenges are going to be. Looking at the project overall, this thesis should mainly answer the following question, which is closely related to the problem statement and title:

> *RQ1: What does the infrastructure for an authentication system using PUFs for physical access control look like?*

Extending this overarching question, many different subquestions related to the individual components and their relationship could be asked. Some of them might be:

> *RQ1.1: Which components are needed as part of the infrastructure?*
> *RQ1.2: How should the required data be organized in the database?*
> *RQ1.3: How is data transferred between components?*

This is definitely not a final set of questions, but rather a look at what the exact research questions in the final thesis may look like.

As implementing a prototype is also part of the thesis, in addition to the conceptual design, a second overarching question is this:

> *RQ2: How can a functional prototype for the proposed infrastructure concept be implemented?*

There is another aspect of this thesis, which is the evaluation of existing concepts and research on the topic. It is not planned to make this a seperate research question, as it is not an end in itself, but rather a means to answer *RQ1* and *2*.

3 Relevance and Existing Research

The earliest paper about PUFs found on Google Scholar was published in 2004 and has been cited over 100 times. Furthermore, Google Scholar lists over 650 results for papers published in 2022 alone, that mention PUFs. This shows that the technology has only been conceptualized quite recently and has become incredibly relevant in today's research.

[3] seems to be the most cited paper on PUFs and shows how the technology can be used for authentication of physical devices using integrated circuits.

[4] is another well received paper, which explains possible applications for PUFs in authentication scenarios and gives an overview of the different types of PUFs. [5] additionally goes into the design of PUF based Radio-Frequency Identification (RFID) devices and outlines a basic challenge-response infrastructure.

A problem that many of these solutions face, is that the CRP are explicitly stored in a database. An attacker with access to this data would be able to circumvent the entire authentication system, as they would know both challenge and response. [6] and [7] propose protocols that do not require storing CRPs explicitly by verifying the responses using cryptographic methods or neural networks.

The papers mentioned above are only a small set of papers that were found during literature research thus far, which was mostly focused on the basics of PUFs. The bulk of literature research still has to be completed using the methodology outlined in the next section. [2] is a review article published in 2020 containing references a wide variety of other research on the topic, which is going to be examined. Additionally, papers about other relevant fundamental topics such as database design need to be found and studied.

4 Approach and Methodology

To achieve the research goal of designing and implementing an infrastructure, each of the sections are approached differently.

In the fundamentals section, literature research is used to gain insight about the current state of scientific research and to build the basis for the conceptualization and implementation stages. As there are many different topics like database design or challenge-response protocols to cover and the review of existing literature is not the main goal of the thesis, a full systematic literature review will not be conducted. The approach to literature research is described in the following.

The main sources for finding literature will be the EBSCO Discovery Service, IEEEE Xplore, the ACM Digital Library, Springer Link and Google Scholar. This should cover the most important sources for scientific literature in the field. The first step will be to gain a good understanding of existing PUF based authentication systems and their components. From there, search terms are developed dynamically depending on the required knowledge. Titles and abstracts of the most cited and relevant papers are scanned to find the papers and books providing the most relevant information. Additionally, if current review articles are found for a given topic, snowballing might be used to find additional relevant information.

As this thesis is part of a research project developing a full Proof of Concept (POC) for a PUF based access control system, some project specific knowledge will be required. An example for this is understanding the specific protocols of the locking systems, that are used in the project's POC. As this knowledge is held by experts in the research group and external partners, expert interviews could be conducted to be able to better apply the general knowledge from literature research to the specific problem space.

Once the required knowledge has been gathered, the conceptualization phase begins. Here, the existing solutions discovered in the research for each part of the infrastructure have to be evaluated based on the requirements of the project. An approach to this would be to define evaluation criteria and create a weighted sum model for each component, but this will get very complex. Another approach might be to take the most fitting ideas from each existing approach and combining them into a system which fits the concrete problem found in the research project. The benefit of this is reduced complexity and more flexibility, but it could lead to "gut feeling" decisions, which would reduce the scientific rigidity of the thesis. More reading has to be done about which is the best choice. While reading, the design science research approach was discovered. [8] It could offer interesting methodologies that could be used in the thesis, but has not yet been evaluated enough.

The goal for the implementation section of the thesis is to create a prototype. Therefore, a language capable of rapid prototyping like Python is most likely going to be selected. Some components of the finished system, like the neural networks and PUFs, are not part of this thesis. Because of this, they are not going to be part of the prototype implementation and mock implementations of their interfaces and responses will have to be created. Unit tests could be implemented to evaluate the finished prototype and to better understand possible edge cases.

5 Structure

This section outlines a rough structure for the thesis. Take into account that this is based on the currently limited knowledge about the topic and is subject to change.

1. **Introduction**: Contains motivation, problem description, research goals, methodology and structure.
2. **Fundamentals**: Will mostly consist of literature research and aims to give an understanding of what the current state of scientific research on the following topics is:
   - Challenge-Response Protocols
   - Database solutions for access control systems
   - Neural Networks in relation to PUFs
     This point will not go into the design of the neural networks itself as it's beyond the scope, but rather examine the infrastructural requirements that neural networks used to evaluate PUFs have in terms of data size, computational power and other aspects.
   - Other Components

   It gives a basis for the conception and implementation sections of the thesis.
3. **Conception**: Will contain the conceptualization of the infrastructure, likely including:
   - Requirements for the proposed solution
   - Specification of a Challenge-Response Protocol
   - The concrete design of a database schema, unifying the requirements for challenge-response, neural networks and access control systems in one schema.
   - Description of other components, like a backend for response evaluation
   - Orchestration and interaction between components
4. **Implementation**: Will go over the implementation of a prototypical infrastructure.
5. **Evaluation**: Here, the proposed solution will be analyzed in terms of performance, possible security risks, limits and potentials for improvement.
6. **Conclusion**

6 Goal and Expected Outcome

Some personal goals for the thesis are the following:

1. Answer the selected research questions

2. Propose an infrastructure that offers value to the research team and can be used in the final POC for the system

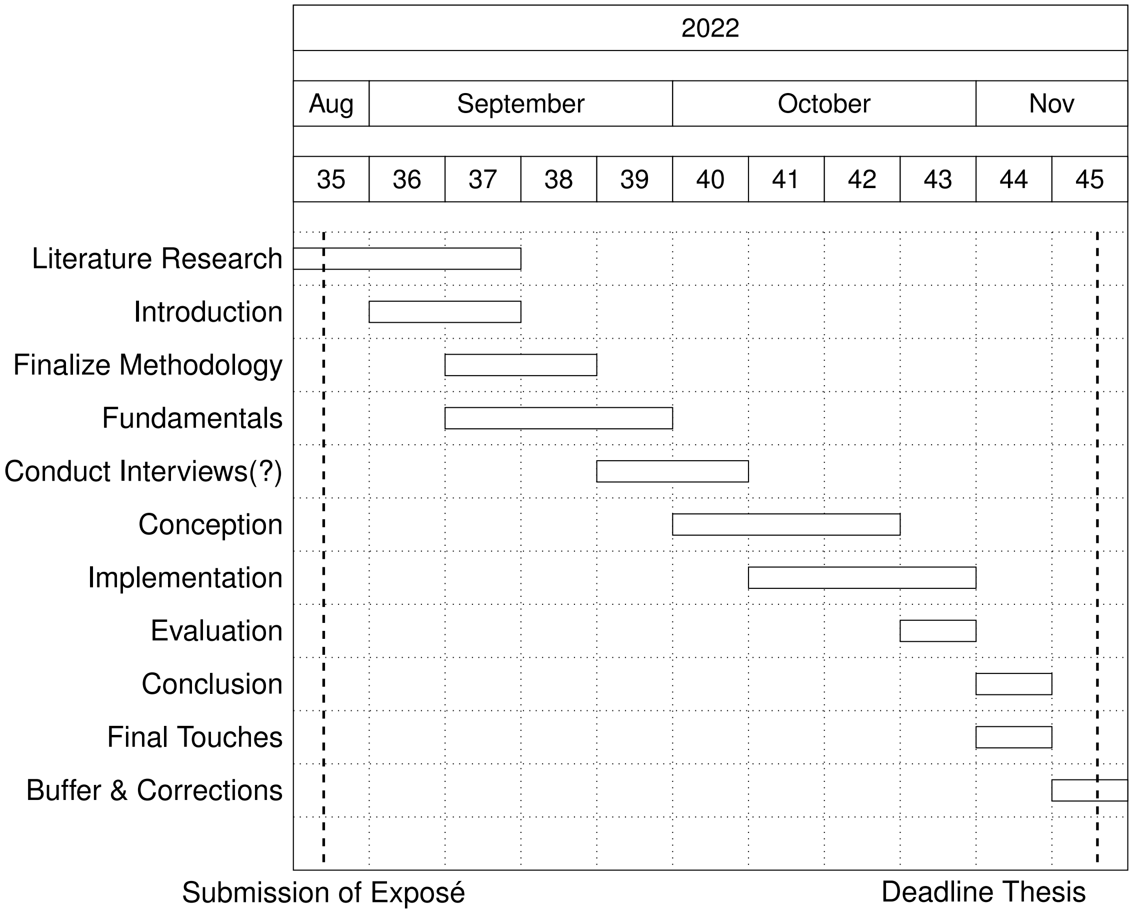
3. In addition to the specific project, the proposal should be generalizable and offer value to other research projects concerned with similar topics

4. Be able to demonstrate a working prototype

Achieving all of these goals will only be possible if there is enough high-quality existing literature available for every topic. Also, good communication with the research team is required. The timeframe is hard to assess and might be too short to create a fully working prototype implementation. In this case, the scope might have to be adjusted and only a part of the proposal might be realized as a prototype.

7 Timetable for Creation of the Thesis

The following Gantt chart shows a rough timetable for completing the thesis, broken down into calendar weeks. The chart begins in calendar week 35 of 2022, as this week contains the submission date of the exposé, which is the 31st of August. All work done prior to that, such as finding a title and writing the exposé, is not considered in this view. The deadline for submission of the thesis is the 10th of November 2022.



Bibliography

[1] S. R. Basavala, N. Kumar, and A. Agarrwal, ‘Authentication: An overview, its types and integration with web and mobile applications,’ in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, IEEE, 2012-12. DOI: 10.1109/pdgc.2012.6449853.

[2] Y. Gao, S. F. Al-Sarawi, and D. Abbott, ‘Physical unclonable functions,’ *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020-02. DOI: 10.1038/s41928-020-0372-5.

[3] G. Suh and S. Devadas, ‘Physical unclonable functions for device authentication and secret key generation,’ in *Proceedings of the 44th annual conference on Design automation - DAC ’07*, ACM Press, 2007, pp. 9–14. DOI: 10.1145/1278480.1278484.

[4] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, ‘Physical unclonable functions and applications: A tutorial,’ *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014-08. DOI: 10.1109/jproc.2014.2320516.

[5] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, ‘Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications,’ in *2008 IEEE International Conference on RFID*, IEEE, 2008-04. DOI: 10.1109/rfid.2008.4519377.

[6] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, and M. M. Prabhu, ‘Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database,’ *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424–437, 2019-05. DOI: 10.1109/tdsc.2018.2832201.

[7] Y. Yilmaz, S. R. Gunn, and B. Halak, ‘Lightweight PUF-based authentication protocol for IoT devices,’ in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, IEEE, 2018-07. DOI: 10.1109/ivsw.2018.8494884.

[8] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, ‘A design science research methodology for information systems research,’ *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007-12. DOI: 10.2753/mis0742-1222240302.