Introduction

As cybersecurity and IT progresses every day, humankind relies on the usage of the electronic devices more and more. We use these products to store valuable information while ensuring the product can keep our data secret.

An ideal product is something that withstands physical harm, defends itself from malware attacks, or survive geological catastrophes. However, for development to continue, we need to use inventions we made and ensure they are secure at least to a certain level. This level is usually determined by specific requirements that the given product has to pass, usually stated in security standards.

When an authority validates a product under a security standard, the issuing authority publishes basic information as well as detailed technical information about the product.

The information about the product is then used to represent the product's properties and its use cases, making it the main entry point for customers to choose when they need security-related information about the product.

Validated products do not have to be standalone products – a part of a product can be validated, too. Using existing products is helpful for vendors because they do not have to implement a product from scratch. They can use other validated products during development. However, creating dependencies on other products is dangerous from the perspective of cybersecurity. When a vulnerability is found in a product, all products that depend on the vulnerable product are affected. The task of finding all modules depending on the vulnerable module is not straightforward. To find them, one must search all available certificates for mentions of the one module they are looking for because the references are not bidirectional.

This thesis aims to design and implement a tool capable of creating directed graph of dependencies for Federal Information Processing Standards ("FIPS") Cryptographic Module Validation Program certificates displaying clusters of certificates referencing each other. These clusters divide the graph into small subgraphs, creating a map of references for cryptographic modules. We create the clusters by searching every cryptographic module HTML page and Security Policy PDF file to reference other certificates. The task of data extraction can be divided into three stages: HTML extraction, PDF extraction, and processing the extracted data. None of the tasks is straightforward, and sometimes advanced heuristics are needed.

One of our goals is also to extract information that might be useful in further analyses of the data. There are many types of analyses and comparisons that the extracted data offers, and some of them require knowledge of mapping certificate dependencies, making it a non-primary goal. Information needed for the rest of the analyses is also easier to extract and does not require much processing.

This thesis contains five main chapters:

- In the first chapter, **State of the Art**, we provide an overview of the most common security standards used today – Common Criteria and FIPS. We describe the certification process and documents required in Common Criteria certification and then describe FIPS 140 and the second publication of this standard, FIPS 140–2.We also attempts to parse security-related documents automatically.

- In the second chapter, we focus on **FIPS 140 Validation Programs**, namely Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program. We describe the security documents related to validation under FIPS 140 validation programs and the process of testing and validation of a product.

- In the third chapter – **Processing of certificates** – we focus on extracting data from the security documents of the FIPS 140–2 validated modules. We describe the stages of the automated process of extraction, problems encountered during each stage, and recommendations and suggestions on improving the FIPS 140–2 security standard. We provide details on the creation of the dataset containing all the extracted data. This dataset is used in further analyses.

- The fourth chapter includes analyses and comparisons performed on the dataset. We provide the results of these analyses along with a brief discussion.

The outcome of this thesis is an extension to `sec-certs` [1] – automated tool capable of extracting information from security certificates – focusing on FIPS 140–2 certificates and creating a directed graph of dependencies between them. We further analyze the extracted information and provide results.

Bibliography

1. ŠVENDA, P. *sec-certs* [online]. CRoCS, 2021 [visited on 2021-05-12]. Available from: https://github.com/crocs-muni/sec-certs.
2. STANDARDIZATION, I. O. for. *Standardization and related activities — General vocabulary* [online]. 2004. Version 8 [visited on 2021-05-01]. Available from: https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/8389141/ISO_IEC_Guide_2_2004_%28Multilingual%29_%2D_Standardization_and_related_activities_%2D%2D_General_vocabulary.pdf?nodeid=8387841&vernum=-2.
3. *Common Criteria for Information Technology Security Evaluation part 1: Introduction and general model* [online]. 2009 [visited on 2021-04-13]. Available from: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf.
4. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components* [online]. 2017 [visited on 2021-04-13]. Available from: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf.
5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Security requirements for cryptographic modules* [online]. Gaithersburg, MD, 2001 [visited on 2021-04-13]. Technical report, NIST FIPS 140-2. National Institute of Standards and Technology. Available from DOI: 10.6028/NIST.FIPS.140-2.
6. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Security requirements for cryptographic modules* [online]. Gaithersburg, MD, 1994 [visited on 2021-04-13]. Technical report, NIST FIPS 140-1. National Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Publications/fips/140/1/archive/1994-01-11/documents/fips1401.pdf.
7. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Security requirements for cryptographic modules* [online]. Gaithersburg, MD, 2019 [visited on 2021-04-13]. Technical report, NIST FIPS 140-3. National Institute of Standards and Technology. Available from DOI: 10.6028/NIST.FIPS.140-3.

8. AZOUAOUI, M.; BELLIZIA, D.; BUHAN, I.; DEBANDE, N.; DUVAL, S.; GIRAUD, C.; JAULMES, E.; KOEUNE, F.; OSWALD, E.; STANDAERT, F.-X., and WHITNALL, C. *A Systematic Appraisal of Side Channel Evaluation Strategies* [Cryptology ePrint Archive, Report 2020/1347]. 2020. Available from: `https://eprint.iacr.org/2020/1347`.

9. COMPUTER SECURITY DIVISION, I. T. L. *Validated Modules - Cryptographic Module Validation Program | CSRC | CSRC* [online]. 2016 [visited on 2021-04-13]. Available from: `https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/Search`.

10. HARKOUS, H.; FAWAZ, K.; LEBRET, R.; SCHAUB, F.; SHIN, K. G., and ABERER, K. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. *CoRR*. 2018, vol. abs/1802.02561. Available from arXiv: `1802.02561`.

11. VASSILEV, A. BowTie - A deep learning feedforward neural network for sentiment analysis. *CoRR*. 2019, vol. abs/1904.12624. Available from arXiv: `1904.12624`.

12. COMPUTER SECURITY DIVISION, I. T. L. *Validated Modules - Cryptographic Module Validation Program | CSRC | CSRC* [online]. 2016 [visited on 2021-04-13]. Available from: `https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules`.

13. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* [online]. Gaithersburg, MD, 2001 [visited on 2021-04-13]. Technical report. National Institute of Standards and Technology. Available from: `https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402DTR.pdf`.

14. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY and CANADIAN CENTRE FOR CYBERSECURITY. *FIPS 140–2 Cryptographic Module Validation Program Management Manual* [online]. Gaithersburg, MD, 2020 [visited on 2021-04-30]. Technical report. National Institute of Standards and Technology. Available from: `https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf`.

15. COMPUTER SECURITY DIVISION, I. T. L. *Cryptographic Module Validation Program: CSRC* [online]. NIST, 2021 [visited on 2021-04-13]. Available from: `https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3860`.

16. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY and COMMUNICATIONS SECURITY ESTABLISHMENT CANADA. *Cryptographic Algorithm Validation Program Management Manual* [online]. Gaithersburg, MD, 2009 [visited on 2021-04-30]. Technical report. National

Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf.

17. COMPUTER SECURITY DIVISION, I. T. L. *Cryptographic Module Validation Program: CSRC* [online]. NIST, 2021 [visited on 2021-04-13]. Available from: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2852.
18. *Licensed Laboratories : CC Portal* [online] [visited on 2021-04-25]. Available from: https://www.commoncriteriaportal.org/labs/.
19. *Touchstone: Accreditation & Assessment Management System - Customer Portal* [online] [visited on 2021-04-25]. Available from: https://www-s.nist.gov/niws/index.cfm?event=directory.search.
20. COMPUTER SECURITY DIVISION, I. T. L. *FIPS 140-3 Transition Effort | CSRC | CSRC* [online]. 2019 [visited on 2021-05-13]. Available from: https://csrc.nist.gov/projects/fips-140-3-transition-effort.