Steffen Becker, Carina Wiesen, Christof Paar, Nikol Rummel

Wie arbeiten Reverse Engineers?

Interdisziplinäre Forschung zum Verständnis technischer und kognitiver Prozesse beim Hardware-Reverse-Engineering

Im Forschungsprojekt „Lernprozesse in der IT-Sicherheit“ beschäftigen sich die Autoren mit der Frage, wie Hacking-Angriffe auf Hardware ablaufen. Gemeinsam erforschen sie die technischen und menschlichen Prozesse, die maßgeblich den Erfolg eines Hardware-Angriffs beeinflussen. Mit den Erkenntnissen zu den mentalen Vorgängen sollen optimierte Gegenmaßnahmen entwickelt werden („kognitive Obfuskation“), die zudem das Hacken durch menschliche Angreifer und Angreiferinnen besonders erschweren.

Steffen Becker

Wissenschaftlicher Mitarbeiter am Lehrstuhl für Eingebettete Sicherheit an der Ruhr-Universität Bochum und Doktorand im Forschungskolleg SecHuman. Forschungsschwerpunkte: Hardware Reverse Engineering, Trojaner und Obfuskation.
E-Mail: Steffen.Becker@rub.de

Carina Wiesen

Wissenschaftliche Mitarbeiterin am Lehrstuhl für Pädagogische Psychologie an der Ruhr-Universität Bochum und Doktorandin im Forschungskolleg SecHuman. Forschungsschwerpunkte: Lern- und Problemlöseprozesse in der IT-Sicherheit.
E-Mail: Carina.Wiesen@rub.de

Christof Paar

Sprecher des Exzellenzclusters CaSa an der Ruhr-Universität Bochum und Gründungsdirektor des Max-Planck-Institutes für Cybersicherheit und Schutz der Privatsphäre sowie Sprecher des Forschungskollegs SecHuman.
E-Mail: Christof.Paar@rub.de

Nikol Rummel

Professorin für Pädagogische Psychologie und Principal Investigator im Exzellenzcluster CaSa an der Ruhr-Universität Bochum sowie Principal Investigator im Forschungskolleg SecHuman.
E-Mail: Nikol.Rummel@rub.de

1 Einleitung

Ob Laptop oder Smartphone, ob Industrie-Roboter oder Amazons Alexa, alle vernetzten Geräte basieren auf Mikrochips, besser bekannt als ICs (integrierte Schaltkreise). Diese Mikrochips werden heutzutage in einem globalisierten Zulieferungsprozess hergestellt: Während ihr Design häufig in westlichen Industrienationen erfolgt, findet die Auftragsfertigung im Normalfall in hochmodernen Halbleiterfabriken in Ostasien statt. Die vielen verschiedenen Einzelkomponenten werden auf ihrem Weg zu den Kundinnen und Kunden üblicherweise in der Nähe des jeweiligen Absatzmarktes zum Endprodukt zusammengebaut, bevor sie als fertiges Gerät (z. B. als Smartphone, Industrie-Roboter, Herzschrittmacher uvm.) im Vertrieb landen.

Nun liegt für viele Unternehmen eines der wesentlichen Probleme darin, ihr geistiges Eigentum – und ihre damit verbundenen wirtschaftlichen Interessen – an den verschiedenen Schnittstellen des globalisierten Herstellungsprozesses vor Produktpiraterie und Manipulationen zu schützen. Eine gängige Vorgehensweise zur Offenlegung der schützenswerten Inhalte eines Mikrochips ist das Reverse Engineering. Dieses kann – wie auch andere Techniken im Kontext der IT-Sicherheit – sowohl von Angreiferinnen und Angreifern für schädliche Zwecke (z. B. Manipulationen und Produktpiraterie) als auch von Unternehmen, Forscherinnen und Forschern sowie staatlichen Stellen mit legitimen Interessen (z. B. dem Auffinden gezielter Manipulationen oder dem Nachweis von Patentverletzungen) eingesetzt werden.

Erfolgreiches Reverse Engineering von Mikrochips erfordert auf der einen Seite teures technisches Equipment und hängt auf

der anderen Seite maßgeblich von erfahrenen Expertinnen und Experten ab, die das Equipment bedienen und die Einzelschritte des Reverse Engineerings mithilfe von Programmen teilautomatisieren können.

Während die technischen Prozessschritte bereits erforscht wurden und gängige Praxis in hochspezialisierten Laboren sind, wurden die menschlichen Faktoren bisher nur unzureichend wissenschaftlich beleuchtet. In diesem Zusammenhang umfassen menschliche Faktoren sowohl angewandte Prozessschritte und Lösungsstrategien als auch kognitive Faktoren menschlicher Analysten wie beispielsweise Intelligenz. Es verwundert daher nicht, dass aktuelle Schutzmaßnahmen gegen das Reverse Engineering von Mikrochips lediglich auf ad-hoc Methoden basieren, welche durch erfahrene Angreifer häufig umgangen werden können.

Unser neuartiger Forschungsansatz zielt daher darauf ab, die Komplexität des Reverse Engineerings sowohl auf Basis moderner technischer Metriken als auch bezüglich menschlicher Faktoren zu quantifizieren [1]. Darauf aufbauend sollen neue Schutzmaßnahmen entwickelt werden, die das Hardware-Reverse-Engineering besonders komplex für menschliche Angreiferinnen und Angreifer machen. Durch diese sogenannte kognitive Obfuskation sollen Mikrochips effektiv gegen Manipulationen und den Diebstahl geistigen Eigentums geschützt werden. Dieser Beitrag skizziert die Idee des Forschungsprojektes.

2 Forschungsfragen

Vor diesem Hintergrund leitet sich die für das Projekt zentrale Forschungsfrage ab:

- **Wie lassen sich der technische und der kognitive Aufwand des Reverse Engineerings zur Extraktion der wesentlichen Informationen (z. B. besonders innovative Komponente oder kryptographischer Schlüssel) aus einem unbekannten Hardware-Design systematisch messen und erhöhen?**

Da sowohl technische als auch menschliche Aspekte den Erfolg des Hardware-Reverse-Engineerings entscheidend beeinflussen, ist es sinnvoll, die zentrale Forschungsfrage in Teil-Fragestellungen aufzuschlüsseln, die dann in interdisziplinärer Form beantwortet und perspektivisch für die Entwicklung neuartiger Schutzmaßnahmen eingesetzt werden können. Diese Fragestellungen lauten wie folgt:

- Welche sind die relevanten menschlichen Faktoren beim Hardware-Reverse-Engineering?
- Wie hoch ist der Grad der Automatisierbarkeit des Hardware-Reverse-Engineering-Prozesses in Bezug auf technische Lösungsansätze und Tools?
- Wie können diese Erkenntnisse über menschliche und technische Faktoren für die Entwicklung neuartiger Schutzmaßnahmen verwendet werden?

3 Hintergrund

Das folgende Kapitel erläutert die Forschungsidee vor dem aktuellen Stand der Wissenschaft bezüglich technischer und menschlicher Faktoren des Hardware-Reverse-Engineerings.

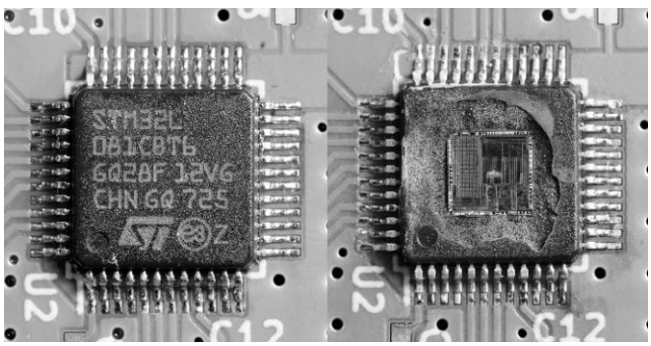
3.1 Technischer Hintergrund des Hardware-Reverse-Engineerings

Als Hardware-Reverse-Engineering wird ein mehrschrittiger Prozess bezeichnet, an dessen Ende sowohl ein genaues Verständnis aller Einzelheiten als auch eine abstrakte Beschreibung der Funktionalität des zugrundeliegenden Chips stehen [2]. Das Endresultat ist insofern vergleichbar mit einem Konzept, welches vor Beginn des Chipdesignprozesses erstellt wird. Auch aus den einzelnen Teilschritten resultierende Zwischenergebnisse können in Abhängigkeit von der jeweiligen Zielsetzung des Reverse Engineerings bereits von Interesse sein. Die Identifikation der relevanten Ergebnisse ist dabei Aufgabe des/der menschlichen Analyst/in. Ein vollständiger Reverse-Engineering-Prozess besteht aus den folgenden Schritten [3, 4]:

Ausgehend vom Mikrochip wird zunächst ein Teil des Plastik- oder Keramikgehäuses entfernt, um den Die – den eigentlichen Chip – freizulegen. Abb. 1 zeigt einen Chip vor und nach diesem Prozessschritt. Da Chips aus mehreren Schichten bestehen, welche sowohl die logischen Bausteine als auch deren Verbindungen implementieren, werden diese Schichten nach und nach freigelegt und unter einem Rasterelektronenmikroskop zu digitalen Bildern verarbeitet.

Die nächste Herausforderung besteht darin, die so entstandenen Bilder exakt aneinander auszurichten und zu einem dreidimensionalen Modell zusammenzufügen. Aus diesem Modell wird dann eine sogenannte Netzliste (Abb. 2) erstellt – eine zweidimensionale Struktur aus miteinander verbundenen logischen Grundelementen. Um auf Basis der Netzliste Rückschlüsse auf die verschiedenen Funktionen des Chips zu ziehen, werden computerbasierte Analysemethoden miteinander kombiniert. Diese machen sich die strukturellen Eigenschaften und logischen Zusammenhänge innerhalb der Netzliste zunutze, um von den millionenfach vorhandenen Grundelementen auf die Gesamtzusammenhänge zu abstrahieren.

Abbildung 1 | Mikrochip auf Leiterplatte (links), geöffneter Mikrochip mit freigelegtem Die (rechts).

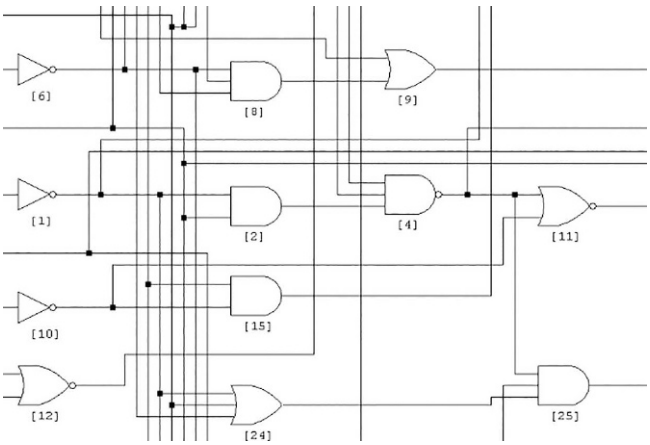


Da es keine einzelne Software gibt, die alle hier beschriebenen Schritte in sich vereint, führen Analystinnen und Analysten das Reverse Engineering oftmals mit einer Sammlung teilautomatischer Programme und Skripte aus, die sie bei ihrer jeweiligen Aufgabe unterstützen. Entscheidend ist, dass menschliche Analystinnen und Analysten die Ergebnisse der einzelnen teilautomatisierten Prozessschritte manuell kombinieren und ihnen Sinn verleihen müssen. *Damit hängt der Erfolg des Hardware-Re-*

verse-Engineerings maßgeblich von den Denk- und Analysefähigkeiten des/r Analyst/in ab.

Sollen nun Mikrochips gegen auf Reverse Engineering basierende Attacken geschützt werden, ist es essentiell, dass die manuellen Analyseschritte eines/r Angreifers/in in die Entwicklung geeigneter Schutzmaßnahmen einfließen.

Abbildung 2 | Ausschnitt einer Netzliste mit logischen Grundelementen und Verbindungen.



3.2 Menschliche Prozesse beim Hardware-Reverse-Engineering

Aktuell gibt es nur wenige wissenschaftliche Veröffentlichungen zu menschlichen Faktoren beim Reverse Engineering. Eine wichtige Vorarbeit ist die Untersuchung von menschlichen Prozessen beim Reverse Engineering von Booleschen Schaltkreisen [5]. Die Autoren untersuchten Vorgehensweisen von Studierenden, die im Rahmen von Experimenten verschiedene Boolesche Problemstellungen in Form elektrischer Schaltkreise lösen mussten. Basierend auf fünf Experimenten stellten die beiden Autoren eine Theorie zum menschlichen Vorgehen im Reverse Engineering auf und definierten Reverse Engineering als eine besondere Art des menschlichen Problemlösens. Diese Vorarbeit ist ein erster Schritt zur Untersuchung zugrundeliegender menschlicher Faktoren. Jedoch kann die Theorie von Lee und Johnson-Laird (2013) kaum auf das Feld des Hardware-Reverse-Engineerings übertragen werden: So verkörpern die Experimente zwar das Rückwärtsdenken eines/r Analysten/in, bilden aber bei weitem nicht die notwendigen Problemlöse-Kompetenzen ab, die bei der Komplexität moderner ICs, wie sie beispielsweise in Smartphones eingesetzt werden, vonnöten sind. Die in der bisherigen Forschung fehlende Übertragbarkeit der Ergebnisse auf das Feld des Hardware-Reverse-Engineerings bildet somit den Ausgangspunkt für die Entwicklung eines eigenen Forschungsdesigns mit realistischeren Problemlöseaufgaben aus dem Bereich des Hardware-Reverse-Engineerings.

4 Forschungsdesign

Um menschliche Prozesse beim Hardware-Reverse-Engineering untersuchen zu können, musste zunächst grundlegend ein methodisches Konzept entwickelt werden.

4.1 Methodische Herausforderung

Klassischerweise beziehen viele psychologische Studien in der Problemlöse-Forschung den Vergleich zwischen Expertinnen und Experten bzw. Novizinnen und Novizen mit ein [z. B. 6, 7]. Basierend auf diesem Vergleich ist es möglich, in konkreten Problemlösesituationen Rückschlüsse auf verwendete Problemlösestrategien und beteiligte Wissensarten in Abhängigkeit vom Kenntnisstand zu schließen.

Dies wäre auch ein denkbarer Forschungsansatz zur Untersuchung menschlicher Vorgehensweisen im Hardware-Reverse-Engineering. Allerdings liegt in Bezug auf die Population von Sicherheitsfachleuten mit Expertise im Hardware-Reverse-Engineering ein fundamentales methodisches Problem vor: Zum einen ist die Gesamtpopulation der Fachleute mit fortgeschrittenen Fähigkeiten im Hardware-Reverse-Engineering sehr klein. Zum anderen existieren weltweit nur wenige anerkannte Expertinnen und Experten. Erschwerend für die Erforschung menschlicher Komponenten beim Hardware-Reverse-Engineering kommt hinzu, dass die bekannten Expertinnen und Experten nicht für die oben beschriebene Forschung zur Verfügung stehen, da sie oft bei staatlichen Stellen oder Unternehmen mit hohen Geheimhaltungsanforderungen beschäftigt sind. Dieses fundamentale Problem stellte das Projekt vor die methodische Herausforderung, eine geeignete Stichprobe für die psychologische Forschung zu gewinnen und führte maßgeblich zur unten vorgestellten Forschungsmethodik.

Das Forschungsdesign bezieht Studierende relevanter Studiengänge (z. B. IT-Sicherheit oder Informatik) als Probandinnen und Probanden mit ein. Untersuchungen mit Studierenden sollen zu Ergebnissen über Invarianten im Prozess des Erwerbs von Expertise führen. Basierend auf diesen Erkenntnissen können Aussagen darüber generiert werden, welche menschlichen Prozesse und Strategien sich nicht ändern, die dann wiederum potentiell interessant für neue Obfuskationstechniken sind.

4.2 Entwicklung eines Hardware-Reverse-Engineering-Kurses

Der am Lehrstuhl für Eingebettete Sicherheit eigens entwickelte Kurs „Einführung ins Hardware-Reverse-Engineering" richtet sich an Bachelor- und Master-Studierende der Informatik, Elektrotechnik und IT-Sicherheit ab dem vierten Hochschulsemester und konnte von uns für dieses Forschungsdesign verwendet werden [8].

Eine einheitliche Vorwissensbasis der Studierenden wird grundlegend sichergestellt, indem in den ersten Semesterwochen zum einen die theoretischen Grundlagen des Hardwaredesigns gelehrt und gezielt in Hausübungen vertieft werden und zum anderen die grundlegenden Techniken des Reverse Engineerings besprochen werden (theoretische Phase). Im zweiten Veranstaltungsteil bearbeiten die Kursteilnehmerinnen und –teilnehmer fünf in ihrer Komplexität ansteigende Reverse-Engineering-Projekte, die jeweils einzelne reale Fragestellungen, mit denen ein Reverse Engineer konfrontiert ist, abbilden (praktische Phase). Durch die Aufteilung des Kurses in eine theoretische Phase, in der deklaratives Wissen erworben wird, und eine praktische Phase zum prozeduralen Wissenserwerb, werden die Studierenden optimal beim Lernen unterstützt.

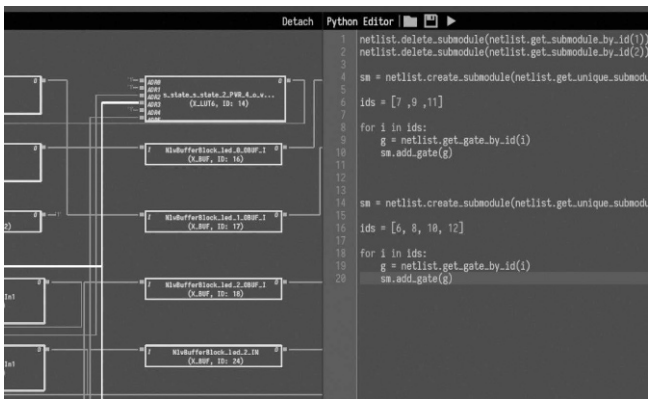
Aspektuell vertieft wird die Vorlesungsreihe durch Gastvorträge von renommierten Wissenschaftlerinnen und Wissenschaftlern und erfahrenen Praxisakteurinnen und -akteuren, die sowohl Fragestellungen zur rechtlichen Lage des Reverse Engineerings und zur Hackerethik beantworten, als auch aktuelle Einblicke in professionelle Reverse-Engineering-Labore geben.

4.3 HAL – Der Hardware Analyzer

Zentral für Lehre und Studie ist das quelloffene Reverse-Engineering-Framework HAL (https://github.com/emsec/hal). HAL ermöglicht teilautomatische und manuelle Analysen von Netzlisten. Zunächst können Analystinnen und Analysten komplexe Netzlisten mittels benutzerdefinierter Plugins partitionieren, um daraufhin die interessanten Teile mithilfe der funktionsreichen graphischen Benutzerumgebung einer detaillierten manuellen Inspektion zu unterziehen (siehe Abbildung 2 links).

Während HAL-Plugins aus Effizienzgründen in der Programmiersprache C++ geschrieben werden, können Sie mittels einer Anbindung an die hochabstrahierte Programmiersprache Python komfortabel aus einem in der Benutzeroberfläche eingebetteten Code-Editor ausgeführt werden (siehe Abbildung 2 rechts).

Abbildung 3 | Bildausschnitt der graphischen Benutzeroberfläche von HAL. Links: Graphische Darstellung der Netzliste. Rechts: Code-Editor mit Python-Skript.



HAL ermöglicht damit die strukturelle und funktionale Analyse von Netzlisten und unterstützt Analystinnen und Analysten dabei, diese passgenau durchzuführen.

Die Möglichkeit, das Verhalten von Reverse Engineers zu beobachten, ist zudem entscheidend für die Studie. Dafür protokolliert HAL das Reverse-Engineering-Vorgehen der Studienteilnehmerinnen und -teilnehmer, die der Teilnahme an der Studie im Vorhinein zugestimmt haben, in Logdateien, welche lokal gespeichert und manuell an die Forscherinnen und Forscher übermittelt werden können.

4.4 Hardware-Reverse-Engineering-Projekte

Die folgenden praktischen Hardware-Reverse-Engineering-Projekte wurden im Rahmen des Kurses durchgeführt:

- Im ersten Projekt werden die Studierenden intuitiv an das Reverse-Engineering-Framework HAL herangeführt und analysieren das Ein-/Ausgabe-Verhalten sowie einen speziellen kryptographischen Baustein einer kleinen Netzliste.
- Das zweite Projekt beschäftigt sich mit der teilautomatischen Identifikation der Kontrolllogik einer Netzliste. Die Kontrolllogik ist ein neuralgischer Punkt vieler Schaltungen, da sich Manipulationen hier besonders effektiv durchführen lassen.
- Im dritten Projekt umgehen die Studierenden eine Schutzmaßnahme der Kontrolllogik, die vor einer Überproduktion des Mikrochips durch die Halbleiterfabrik schützen soll.
- Die Netzliste des vierten Projekts implementiert die Blockchiffre AES mit einem fest eingebauten kryptographischen Schlüssel. Die Aufgabe der Studierenden besteht darin, die Netzliste so zu manipulieren, dass der Schlüssel extrahiert werden kann.
- In der Netzliste des letzten Projekts ist ein Wasserzeichen implementiert, welches bei einer Vervielfältigung durch Produktpiratinnen und –piraten erhalten bleibt und als Beweis dienen kann. Im Rahmen des Projekts detektieren und entfernen die Studierenden das Wasserzeichen.

Die hier vorgestellten Projekte decken ein breites Spektrum der Herausforderungen ab, mit denen ein Reverse Engineer in der Realität konfrontiert ist. Einschränkend ist jedoch hinzuzufügen, dass das Reverse Engineering realer Chips durch die schiere Größe der Netzliste und die Kombination verschiedener Schutzmaßnahmen ungleich komplexer sein kann.

4.5 Studiendesign

Ziel der Studie ist es, erste Erkenntnisse über Expertiseentwicklung bei Studierenden unter Einflüssen von kognitiven Faktoren (z. B. Intelligenz) und Vorerfahrungen in relevanten Wissensbereichen (z. B. Boolescher Algebra) zu gewinnen.

Die Studienteilnehmerinnen und –teilnehmer werden aus den Studierenden des Hardware-Reverse-Engineering-Kurses rekrutiert. Die Entscheidung für oder gegen die Teilnahme an der Studie wirkt sich dabei in keiner Weise auf die Bewertung des Kurses aus. Zudem ist die Studienteilnahme freiwillig und der entsprechende zeitliche Mehraufwand für die Beantwortung der psychologischen Fragebögen und Testverfahren wird monetär vergütet. Bevor die Studierenden die Einwilligungserklärung unterschreiben, werden sie über sämtliche Ziele, Methoden und mögliche Verwertungen der Ergebnisse aufgeklärt. Erst danach beginnt die Studie im praktischen Teil des Hardware-Reverse-Engineering-Kurses.

Im Rahmen der Erforschung menschlicher Vorgehensweisen beim Hardware-Reverse-Engineering fokussieren wir Veränderungen von und Einflüsse auf die folgenden Messgrößen, die zugleich die klassischen Variablen psychologischer Forschung sind: Lösungszeit (Bearbeitungszeit pro Problemlöseaufgabe), Lösungsgüte (Korrektheit pro Problemlöseaufgabe), Prozessschritte sowie Fehler beim Lösen der Problemlöseaufgaben. Basierend auf den HAL-Logfiles können Rückschlüsse über Lösungszeit, einzelne Prozessschritte sowie häufige Fehler gezogen werden.

Durch zusätzliche Fragebögen werden weitere als Kontrollvariablen einfließende Messgrößen erhoben – beispielsweise Vorwissen, Intelligenz oder Motivation.

In Tabelle 1 sind die Studienprozeduren inklusive verwendeter Erhebungsinstrumente aufgeführt. Vor jedem der fünf Projekte werden die Studienteilnehmerinnen und –teilnehmer gebeten, einen Fragebogen zur Bewertung ihres Motivationslevels in Bezug auf die aktuellen Aufgaben zu beantworten. Nach der Abgabe

des Projekts schätzen die Studierenden dessen Aufgabenschwierigkeit sowie ihre wahrgenommene mentale Belastung während der Bearbeitung des Projekts ein. Einmalig wird mit den Studienteilnehmerninnen und –teilnehmern zudem ein Intelligenztest (ca. 90-minütige Sitzung) sowie ein Kurzfragebogen zur Erfassung weiterer Variablen wie Vorwissen, Expertise-Level und Soziodemografie durchgeführt.

Tabelle 1 | Studienprozedur und Messinstrumente

Vor Bearbeitung des HRE-Problems	Nach Bearbeitung des HRE-Problems	Einmalige Abfrage
Fragebogen zur Erfassung aktueller Motivation [9]	Skala zur wahrgenommenen Aufgabenschwierigkeit [10]	Intelligenztest [12]
	Skala zur mentalen Belastung [11]	Soziodemografie (selbstentwickelter Fragebogen zu Alter, Vorwissen, Studiengang)

5 Fazit und Ausblick

Die Vertrauenswürdigkeit von Mikrochips, die sowohl in Alltagsgeräten als auch in den Systemkomponenten kritischer Infrastruktur eingebaut sind, spielt eine entscheidende Rolle für Individuen, Unternehmen und die Gesellschaft als Ganzes. Auf Reverse Engineering basierende Angriffe können z. B. durch Produktpiraterie oder durch gezielte Manipulationen schwerwiegende Folgen für die Integrität der verwendeten Mikrochips haben. Der Erfolg solcher auf Reverse Engineering basierenden Hacks wird zwar maßgeblich durch teilautomatisierte Techniken beeinflusst – diese unterstützen die Analystinnen und Analysten jedoch nur bis zu einem gewissen Punkt, ab dem sie dann dazu gezwungen sind, den Angriff manuell weiterzuführen. Dies bedeutet, dass der Erfolg des Hardware-Reverse-Engineerings weiterhin auch von menschlichen Faktoren und Prozessen abhängt.

Überraschenderweise basieren aktuelle Schutzmaßnahmen gegen das Hardware-Reverse-Engineering auf rein technisch-mathematischen Annahmen und lassen menschliche Prozesse völlig außer Acht. Das Ziel des vorgestellten Projekts besteht daher darin, sowohl die zugrundeliegenden menschlichen Prozesse als auch beeinflussende Faktoren beim Hardware-Reverse-Engineering zu untersuchen, um a) Metriken für die Schwierigkeit eines Hacks und b) Schutzmaßnahmen unter Einbezug technischer und menschlicher Faktoren – sogenannte kognitive Obfuskation – zu entwickeln. Dazu haben wir zunächst ein Studiendesign entwickelt, das sich den methodischen Herausforderungen bezüglich der geringen Gesamtpopulation solcher Analystinnen und Analysten stellt, und führen aktuell Verhaltensbeobachtungsstudien durch. Diese werden uns erste Hinweise auf bis dato wenig erforschte menschliche Prozesse liefern, welche dann perspektivisch in die Entwicklung der Metriken und Schutzmaßnahmen einfließen werden.

Literatur

[1] Wiesen, C., Albartus, N., Hoffmann, M., Becker, S., Wallat, S., Fyrbiak, M., Rummel, N., & Paar, C. (2019). *Towards cognitive obfuscation: impeding Hardware-Reverse-Engineering based on psychological insights*. In Proceedings of the 24th Asia and South Pacific Design Automation Conference (pp. 104-111). ACM.

[2] Rekoff, M. G. (1985). On reverse engineering. *IEEE Transactions on systems, man, and cybernetics, (2),* 244-252.

[3] Torrance, R., & James, D. (2009). The state-of-the-art in IC reverse engineering. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 363-381).

[4] Subramanyan, P., Tsiskaridze, N., Li, W., Gascón, A., Tan, W. Y., Tiwari, A., & Malik, S. (2013). Reverse engineering digital circuits using structural and functional analyses. *IEEE Transactions on Emerging Topics in Computing, 2*(1), 63-80.

[5] Lee, N. L., & Johnson-Laird, P. N. (2013). A theory of reverse engineering and its application to Boolean systems. *Journal of Cognitive Psychology, 25*(4), 365-389.

[6] Larkin, J., McDermott, J., Simon, D. P., & Simon, H. A. (1980). Expert and novice performance in solving physics problems. *Science, 208*(4450), 1335-1342.

[7] Boshuizen, H. P., & Schmidt, H. G. (1992). On the role of biomedical knowledge in clinical reasoning by experts, intermediates and novices. *Cognitive science, 16*(2), 153-184.

[8] Wiesen, C., Becker, S., Fyrbiak, M., Albartus, N., Elson, M., Rummel, N., & Paar, C. (2018). *Teaching Hardware-Reverse-Engineering: Educational Guidelines and Practical Insights*. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) (pp. 438-445). IEEE.

[9] Rheinberg, F., Vollmeyer, R., & Burns, B. D. (2001). FAM: Ein Fragebogen zur Erfassung aktueller Motivation in Lern-und Leistungssituationen (Langversion, 2001). *Diagnostica, 2*, 57-66.

[10] Bratfisch, O. (1972). Perceived Item-Difficulty in Three Tests of Intellectual Performance Capacity.

[11] Paas, F. G. (1992). Training strategies for attaining transfer of problem-solving skill in statistics: A cognitive-load approach. *Journal of educational psychology, 84*(4), 429.

[12] Wechsler, D. (2008). Wechsler Adult Intelligence Scale–Fourth Edition (WAIS–IV). *San Antonio, TX: NCS Pearson*, 22, 498.