Kurzfassung

Unsere moderne digitale Gesellschaft steht auf dem Fundament von digitalen Hardware Systemen, die in einer Vielzahl von verbundenen smart-X Geräten und traditionellen Computersystemen verbaut sind. Da diese Geräte und Systeme integraler Bestandteil unseres täglichen Lebens geworden sind, haben gezielte Manipulation dieser Hardware Systemen verheerende Auswirkungen für die Sicherheit und Privatheit.

In heutigen Produktionsketten sind Hardware Designs transparent für viele nicht vertrauenswürdige Stakeholder und damit zwangsläufig anfällig für Manipulation und IP Piraterie. In vielen Angriffsszenarien hat ein Angreifer allerdings nur Zugang zur low-level, potentiell obfuskierten, gate-level Netzliste und steht daher dem kosten- und zeitaufwendigem Reverse Engineering gegenüber: Zuerst müssen sicherheitsrelevante Elemente im Schaltkreis idenzifiziert werden und anschließend ein sinnvoller Hardware Trojaner eingefügt werden. Jedoch wurden diese Herausforderungen bisher nur flüchtig von der Forschungsgemeinschaft behandelt.

Zusätzlich zu destruktiven Aspekten ermöglicht Hardware Reverse Engineering verschiedene konstruktive Applikationen um Hardware Systeme abzusichern. So sind Sicherheitsingenieure dazu gezwungen nicht vertrauenswürdige Designs von Drittparteien per Reverse Engineering zu analysieren um Hardware Trojaner zu identifizieren, da der Quellcode typischerweise nicht verfügbar ist. Außerdem ermöglicht ein genaueres Verständnis von Hardware Reverse Engineering die Entwicklung solider Schutzmaßnahmen. Jedoch wurde Reverse Engineering in der Sicherheitsanalyse von verschiedenen Schutzmaßnahmen vernachlässigt, da Reverse Engineering immer noch ein undurchsichtiger und kaum verstandener Prozess ist.

Um systematisch konstruktive und destruktive Aspekte von gate-level Netlist Reverse Engineering zu erforschen, beschreiben wir zuerst das Fehlen eines Netlist Reverse Engineering- und Manipulationsframeworks in der öffentlich zugänglichen Literatur und präsentieren ein ganzheitliches Framework namens HAL. HAL unterstützt und automatisiert maßgeschneiderte Reverse Engineering Aufgaben und ermöglicht zielgerichtete Manipulation. Basierend auf der Erweiterbarkeit von HAL untersuchen wir verschiedene technische Aspekte von gate-level Netlist Reverse Engineering und wir liefern mehrere Forschungsbeiträge, z. B. den facettenreichen Arbeitsablauf der teilautomatisierten Hardware Trojaner Einfügung, Reverse Engineering Kosten basierend auf Graph Ähnlichkeitsanalysen, sowie neue Erkenntnisse bzgl. der (Un-)Sicherheit von mehreren Obfuskationsschemata basierend auf endlichen Zustandsautomaten. Außerdem untersuchen wir kognitive Aspekte beim Reverse Engineering und wir entwickeln eine Methodik basierend auf Problemlöse- und Expertiseforschung, um entscheidende menschlichen Faktoren beim Hardware Reverse Engineering zu untersuchen. Gegensätzlich zur bisherigen Meingung zeigen wir, dass die Entwicklung von automatisierten maßgeschneiderten Werkzeugen zum Reverse Engineering und zur Hardware Trojaner Einfügung nicht anspruchsvoll und zeitaufwendig sind.

Schlagworte. Gate-level Netlist Reverse Engineering, Kognitive Aspekte von Reverse Engineering, Hardware Obfuskation, Hardware Trojaner, Graph Ähnlichkeit