Kurzfassung

In den letzten drei Jahrzehnten haben sich Field Programmable Gate Arrays (FPGAs) zu fortgeschrittenen re-programmierbaren Hardwarebausteinen entwickelt und wurden zu elementaren Komponenten für zahlreiche Informations- und Kommunikationssysteme. Im Jahr 2010 wurden weltweit mehr als vier Milliarden solcher Systeme ausgeliefert. SRAM-basierte FPGAs werden weitgehend in Anwendungen wie der Luft- und Raumfahrt, dem Gesundheitswesen, dem Militärbereich, der Automobilindustrie und in Computernetzwerken sowie Datenzentren genutzt.

Viele dieser Anwendungen sind sicherheitskritisch und benötigen deshalb kryptographische Operationen beispielsweise zur Generierung von Zufallszahlen, zum Schlüsselaustausch, zur Generierung von digitalen Signaturen oder zur Verschlüsselung von Daten. Dies ermöglicht die Sicherheitsanforderungen wie Integrität, Authentizität, und Vertraulichkeit zu erfüllen. Deshalb sehen wir in der Praxis einen erhöhten Einsatz von FPGAs, die sicherheitsrelevante Aufgaben übernehmen und in Avionik Systemen wie Satelliten, der Boeing 787 (Dreamliner) oder dem Mars Rover der NASA genutzt werden.

Ein Teil der Enthüllungen durch Edward Snowden hat gezeigt, dass der US-amerikanische Geheimdienst National Security Agency (NSA) verschiedene Übertragungsgeräte während der Warensendung abfängt, um Hintertüren einzubauen. Beispielsweise führten Firmwaremanipulationen an Cisco-Routern zu einer uneingeschränkten Überwachung gezielter Datennetzwerke durch die NSA. Konkret wurde die Funktionsweise der Firmware rekonstruiert und anschließend Teile ersetzt. Während Softwaremanipulationen in weit verbreiteten Architekturen wie x86 oder ARM bereits gut erforscht sind, gab es bislang keine Dokumentationen, welche Angriffe auf kryptographische Hardwarekonfigurationen von FPGAs bzw. die zugehörige Bitstreamdatei beschreiben. Eine Bitstreamdatei, der kodierte Schaltkreis eines FPGAs, enthält eine Beschreibung der Konfiguration der internen Hardwareelemente, die beim Start geladen wird. Es kann jeden denkbaren digitalen Hardwareschaltkreis beschreiben, der eine beliebige Funktionalität ausführen kann. Angenommen ein Angreifer kommt in Besitz eines Bitstreams der einen kryptographischen Schaltkreis beschreibt, zum Beispiel durch Abhören des Konfigurationsdatenbusses oder durch Auslesen des externen nicht-flüchtigen Speichers. Dann stellt sich die Forschungsfrage, ob und speziell wie eine Manipulation dieses Bitstreams zur Schlüsselextraktion oder dem Einfügen eines Trojaners führen kann. Da das Dateiformat des Bitstreams allerdings proprietär ist und keine offiziellen Extraktionswerkzeuge zur Verfügung gestellt werden, scheint die Manipulation von kryptographischen Hardwarekonfigurationen in der Praxis auf den ersten Blick schwierig zu sein. Dies ist einer der Gründe, weshalb bisher keine praktischen Angriffe auf Hardwarekonfigurationen vorgestellt wurden.

Diese Schwierigkeit stellt sich gleichermaßen, falls eine menschenlesbare Repräsentation gegeben ist. Ein Grund hierfür ist, dass ein Angreifer komplexe Hardwarestrukturen rekonstruieren muss, welche aus hunderttausenden elektrischen Leitungen, Look-up-Tabellen und Flip-Flops bestehen können, die als unstrukturiertes Konstrukt von Gattern erscheinen.

Um sich im Allgemeinem gegen das Klonen von Bitstreams bzw. vor Manipulationen zu schützen, bieten die Marktführer Xilinx und Altera einen Verschlüsselungsmechanismus für Bitstreams an, der Vertraulichkeit und Integrität sichern soll. Ein Problem dieser Gegenmaßnahmen ist jedoch, dass der kryptographische Schlüssel beispielsweise durch Seitenkanal-Angriffe extrahiert werden kann. Die Bestimmung des geheimen Schlüssels von der Bitstreamverschlüsselung führt zum kompletten Verlust der Vertraulichkeit und Integrität. Dies ermöglicht ein Kopieren des Bitstreams und lässt bösartige Manipulationen zur realen Bedrohung werden. Insbesondere die bösartige Manipulation von Bitstreams ist ein kaum untersuchtes Forschungsfeld.

Um diese Forschungslücke zu schließen, zeigt diese Dissertation auf, dass nicht-invasive und gezielte Bitstreammanipulationen praktisch durchführbar sind und ein mächtiges Werkzeug darstellen um die Sicherheit von kryptographischen Implementierungen zu brechen. In dieser Arbeit werden somit die ersten erfolgreichen Manipulationen von Bitstreams gezeigt, welche die Sicherheitseigenschaften von Blockchiffren wirkungslos machen. Konkret beschreibt diese Arbeit Methoden zur Detektion und Manipulation, die es entweder erlauben den geheimen Schlüssel zu extrahieren oder erzwingen, dass die kryptographische Stärke der AES Blockchiffre geschwächt wird. Um die praktische Relevanz und Machbarkeit von Bitstreammanipulationsangriffen zu bestätigen, präsentieren wir den ersten injizierten FPGA Trojaner. Dazu wird das AES-Modul im Bitstream eines kommerziell verfügbaren eingebetteten Gerätes manipuliert. Dabei handelt es sich um einen FIPS-140-2 Level 2 zertifizierten Hochsicherheits-USB-Stick der Firma Kingston.

Gezielte Bitstreammanipulationen, insbesondere diejenigen, welche eine vorherige Detektion von relevanten kryptographischen Primitiven erfordern, weisen eine bereits sehr gute Erfolgsquote auf, haben bei speziellen AES Implementierungen allerdings keine Erfolgsgarantie. Um eine weitere generische Methode zur Schlüsselextraktion bzgl. AES aufzuzeigen, präsentieren wir eine neuartige und effiziente Vorgehensweise, die erfolgreich Fehlerinjektionsangriffe – auch auf verschlüsselte Bitstreams – durchführt. Diese Technik führt zu einer noch höheren Erfolgsrate bzgl. der Schlüsselextraktion diverser AES Implementierungen, unabhängig einer vorherigen Lokalisation des AES im Bitstream. Der Angriff funktioniert zudem völlig unabhängig von der zugrunde liegenden Hardwarearchitektur. Folglich kann der Gebrauch von teuren Laserequipments oder der Rekonstruktionsprozess bezüglich der zugrunde liegenden Hardware-Konfiguration vermieden werden, welche ähnlich komplex wie die Rekonstruktion eines Application Specific Integrated Circuits (ASICs) sein kann.

Zusammenfassend kann gesagt werden, dass diese Arbeit auswertet zu welchem Grad nicht-invasive Bitstreammanipulationen die Systemsicherheit von SRAM-basierten FPGAs aushebeln können.