Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Abschlussarbeit (Bachelor/Master) in Kooperation mit Fraunhofer AISEC, Garching

Konzipierung verdeckter Kommunikationskanäle

Motivation und Aufgabenstellung

In vielen Bereichen werden Aufgaben und Funktionen durch eingebettete Systeme erbracht. Diese haben dadurch u. U. auch Zugriff auf sensible Informationen über ihre Anwender oder Betreiber. Dennoch nehmen manche Hersteller die daraus erwachsende Verantwortung zum Schutz ihrer Kunden noch nicht richtig wahr. Proprietäre Software oder veraltete Softwarekomponenten mit bekannten Sicherheitslücken können bereits beim Marktstart von Geräten deren Anwender gefährden. Weiterhin stellen teils undokumentierte Funktionen und Kommunikationskanäle bei einigen Geräten für unbedarfte Betreiber ein unkalkulierbares Sicherheitsrisiko dar.

In dieser Abschlussarbeit soll exemplarisch an Druckern recherchiert werden, über welche Möglichkeiten (bspw. Modifikationen im Druckbild) verdeckte Kommunikationskanäle realisiert werden könnten. Dazu können die als Wasserzeichen aufgedruckten Informationen (Machine Identification Code (MIC)) ebenso wie Grauabstufungen im Schriftbild (Printer bzw. Scanner Forensic) als Ideengeber verwendet werden.

Um geeignete Abwehrmaßnahmen entwickeln zu können soll zunächst die Domäne untersucht werden. Die gewonnen Erkenntnisse aus der Analyse der oben genannten Ansätze sollen in ein Konzept überführt werden, wie ein solcher verdeckter Kommunikationskanal für einen Datentransfer ausgenutzt werden kann. Zu berücksichtigende Aspekte wären dabei mögliche Datenraten und wie ein solcher Kanal durch eine gezielte Manipulation der Firmware etabliert werden könnte. Ein geeigentes Szenario ist zu skizzieren, in welchem relevante Daten durch diesen Kanal übertragen werden können. Abschließend sollen die Erkenntnisse in einem geeigneten Aufbau praktisch umgesetzt und bewertet werden.

Anforderungen

- Gute Kenntnisse und Erfahrung mit Analyse von Firmware
- Gute Grundkenntnisse in IT Sicherheit sowie kreatives, eigenmotiviertes Arbeiten
- Interesse und Kenntnisse in Steganographie und Kryptographie vorteilhaft

Kontakt

Norbert Wiedermann
Telefon: +49 89 322-9986-141
E-Mail: norbert.wiedermann@aisec.fraunhofer.de

Sven Plaga
Telefon: +49 89 322-9986-134
E-Mail: sven.plaga@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Department Product Protection and Industrial Security
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de