Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

1 *Anzeige auf Drucker-Display*
2 *Darstellung der GUI*

FACT – FIRMWARE ANALYSIS AND COMPARISON TOOL

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Zanderstraße 5
53177 Bonn-Bad Godesberg

ANSPRECHPARTNER
Johannes vom Dorp
Telefon +49 228 50212-570
johannes.vom.dorp@fkie.fraunhofer.de

Raphael Ernst
Telefon +49 228 50212-562
raphael.ernst@fkie.fraunhofer.de

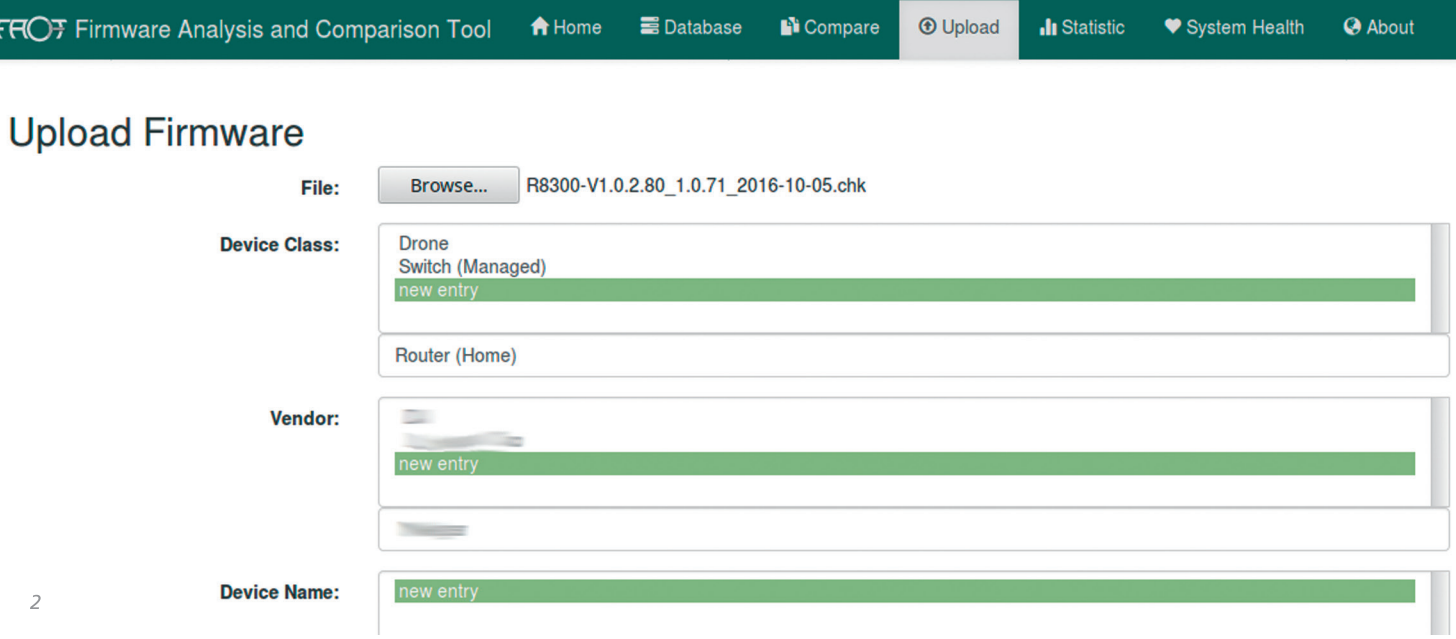
www.fkie.fraunhofer.de/cad

AUSGANGSSITUATION

In den meisten IT-Sicherheitskonzepten werden Embedded Devices, wie z. B. Router, Firewalls, IP-Telefone oder auch eine Motorsteuerung in einem Fahrzeug, nicht als Bedrohung angesehen. Dabei steigt ihre Verbreitung insbesondere durch den »Internet-of-Things«-Boom stetig und tangiert immer mehr Bereiche des täglichen Lebens. Zudem sind sie längst auch in kritischen Bereichen wie dem Gesundheitswesen sowie in Überwachungs- und Zugangssystemen im Einsatz.
Studien, Analysen von Experten und auch die zunehmende Veröffentlichung immer neuer Sicherheitslücken belegen die leichte Kompromittierbarkeit der Geräte. Bereits 2013 zeigten die Snowden Leaks, dass Geheimdienste seit langem Router manipulieren, um fremde Netzwerke zu infiltrieren. Ferner zeigen Botnetze wie »Mirai«, dass auch Kriminelle das Potenzial längst erkannt haben. Die Sicherheit von Embedded Devices muss daher unbedingt deutlich erhöht werden. Als Beitrag zur Sicherheit hat das Fraunhofer FKIE das »Firmware Analysis and Comparison Tool« (FACT) entwickelt, das die Firmware solcher Geräte automatisierten Sicherheitsanalysen unterzieht. Dies ermöglicht eine Einschätzung, wie sicher das Gerät ist. Zudem erhält man Anhaltspunkte für proaktive angemessene Sicherheitsmaßnahmen, um das Risiko einer Manipulation des Gerätes zu reduzieren. Ferner kann FACT Firmware-Images vergleichen, wodurch z. B. die Umsetzung und Wirksamkeit von Sicherheits-Patches leichter überprüft werden kann.

FALLBEISPIEL PRINTER RANSOMWARE

Netzwerkdrucker sind in nahezu allen Unternehmen und Behörden anzutreffen. Oft sind sie leicht angreifbar, was zu schwerwiegenden Folgen für die Sicherheit des ganzen Netzwerks führt. Um dies zu verdeutlichen, hat Fraunhofer FKIE einen Awareness-Demonstrator gebaut, der auf Druckern eines namhaften Herstellers mit originaler Firmware funktioniert. Die genutzten Sicherheitslücken wurden dabei mit der Unterstützung von



FACT innerhalb kürzester Zeit gefunden. Der Demonstrator nutzt ein manipuliertes Dokument, das beim Drucken die Firmware des Druckers verändert, den Drucker unbrauchbar macht und sich anschließend selbstständig auf alle Drucker im selben Netzwerk ausbreitet.

HERAUSFORDERUNG FIRMWARE-ANALYSE

Wenn man nach Sicherheitslücken in Firmware sucht, stößt man auf einige Herausforderungen. Zunächst muss die Firmware entpackt werden, um an die einzelnen Module und Programmteile zu gelangen. Das Problem dabei ist, dass die meisten Hersteller ihre Firmware in eigenen, nicht dokumentierten, proprietären Containern ausliefern. Zudem sind einige wenige Hersteller dazu übergegangen, ihre Firmware zu verschlüsseln, was das Entpacken zusätzlich erschwert.

Die nächste Herausforderung ist, sich einen Überblick zu verschaffen: Wie ist die Firmware aufgebaut? Welche Software wird benutzt? Wie sind Authentifizierung und Transportverschlüsselung implementiert? Oft finden sich hier bereits die ersten Sicherheitsprobleme wie z. B. veraltete Software mit bekannten Sicherheitslücken oder privates Schlüsselmaterial, das auf allen Geräten gleich ist und viele Sicherheitskonzepte ad absurdum führt.

Die nächste Herausforderung ist die Suche nach interessanten Stellen für weitere detailliertere Analysen. Diese Fokussierung ist nötig, da Firmware ähnlich komplex geworden ist wie auch andere Computersysteme. Würde man versuchen die gesamte Firmware händisch zu analysieren, würde man mehrere Jahre für eine Firmware-Version eines einzelnen Gerätes benötigen. Eine umfassende, komplett manuelle Analyse von mehreren Geräten lässt sich dementsprechend gar nicht bewerkstelligen.

AUTOMATISIERUNG

Um dennoch eine differenzierte Untersuchung möglichst vieler Geräte in kurzer Zeit durchführen zu können, ist ein hoher Automatisierungsgrad unabdingbar. Zu diesem Zweck wurde FACT entwickelt, das das Entpacken, die Übersichtsgewinnung und bereits einige automatisierte Sicherheitsanalysen liefert. Dabei ist FACT über eine Web-GUI einfach bedienbar und gleichzeitig durch eine REST-Schnittstelle gut integrierbar. Um auf die Vielzahl von unterschiedlichen Containern und Betriebssystemen sowie die Diversität der Arten von Sicherheitslücken eingehen zu können, basiert FACT auf einem komplett Plug-In basierten Ansatz, der eine unkomplizierte Erweiterbarkeit garantiert.

VERGLEICHE

In vielen Fällen ist das Ziel nicht nur, Sicherheitslücken in einer Firmware zu finden, sondern auch zu prüfen, wie ein Hersteller ein Problem beseitigt hat. In anderen Fällen gilt es herauszufinden, an welchen Stellen sich eine manipulierte von der originalen Firmware unterscheidet. Aus diesen Gründen ermöglicht FACT den direkten Vergleich von mehreren Firmware-Images basierend auf verschiedenen Aspekten wie beispielsweise ausgetauschten/zusätzlichen Dateien oder Software.

VERFÜGBARKEIT, UNTERSTÜTZUNG UND WEITERENTWICKLUNG

Die Basisversion »FACT_core« steht unter GPLv3 kostenlos für den Privatgebrauch, die Forschung oder die kommerzielle Nutzung zur Verfügung. Ferner gibt es verschiedene Möglichkeiten, wie z. B. durch die Entwicklung und Veröffentlichung von weiteren Entpack-, Analyse- oder Vergleichs-Plug-Ins, das Projekt zu unterstützen.

Zudem können Sie Fraunhofer FKIE beauftragen, weitere auf Ihre Bedürfnisse zugeschnittene Analysemethoden und Funktionalitäten zu erforschen und zu entwickeln. Sprechen Sie uns gerne an.

DANKSAGUNG

Die Entwicklung von FACT wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) finanziell gefördert.

https://fkie-cad.github.io/FACT_core/