Gemischte Hacks

Hacker zeigen Sicherheitslücken und Open-Source-Projekte auf dem CCC-Kongress 34C3

Experten aus dem Umfeld des Chaos Computer Club bewiesen auf der Leipziger Hacker-Konferenz, wie verwundbar die vernetzte Digitalwelt ist. 2017 hatten sie E-Zapfsäulen, Banking-Apps, Staubsauger-Roboter und 4G-Mobilfunk im Visier. Sie schafften aber auch Neues, wie einen Open-Source-Satelliten, der in Rekordzeit entstand.

Von Stefan Krempl

Auf dem 34. Chaos Communication Congress (34C3) konnte man sich des Eindrucks nicht erwehren, dass es schlecht bestellt ist um die IT-Sicherheit. Oft mangelt es bei neuen Produkten an Basisvorkehrungen, die den Nutzer vor Überwachung sowie Daten- und Geldklau schützen könnten. Und wo Schutzmaßnahmen getroffen werden, reichen Hackern teils einfachste Mittel, um sie auszuhebeln.

Die wachsende Infrastruktur öffentlicher Stromtankstellen war bereits vor zwei Jahren ins Visier des Chaos Computer Club (CCC) geraten. Vieles sei „schon kaputt“, hatte es damals geheißen. Sicherheitsforscher und CCC-Mitglied Mathias Dalheimer meldete nun Vollzug: „Die Anbieter haben grundlegende Sicherheitsmechanismen nicht umgesetzt“, erklärte das CCC-Mitglied. Wären die Lücken an der Kasse im Supermarkt genauso groß, könnte man dort „mit der Fotokopie einer Girokarte“ bezahlen.

Tank-Tricks

Hauptproblem sind unzureichende Authentisierungsverfahren. Während etwa beim Online-Banking außer einer PIN in der Regel zumindest eine TAN als zusätzlicher Faktor erforderlich ist, reicht bei Ladesäulen eine einzelne, einfach in die Finger zu bekommende Variable. In einem Video führte Dalheimer vor, dass sich über seine selbst gebaute „Testbox“ in Form eines Auto-Lade-Adapters auch zum Beispiel ein Waffeleisen an den hierzulande vorherrschenden 230-V-Wechselstrom-Zapfsystemen anschließen lässt.

Als Abrechnungslösung kommt an den über 11.000 hiesigen öffentlichen E-Zapfsäulen in der Regel das Open Charge Point Protocol (OCPP) in Version 1.5 von 2012 zum Einsatz. Er habe die Spezifikation gelesen und nach 20 Minuten kapiert, woran es hapere, berichtete der Fraunhofer-Wissenschaftler. Ein Token von 20 Zeichen reiche aus, um mit dem Zentralsystem im Backend des Betreibers kommunizieren zu können und Strom zu beziehen.

Die Ladekarten, auf denen die erforderlichen Token gespeichert seien, könne man mit Lesegeräten inspizieren, sagte Dalheimer. Dabei habe er festgestellt, dass in der Regel Nahfunk-Karten mit „Mifare Classic“-Chips genutzt würden, obwohl deren Krypto-Implementierung bekanntermaßen löchrig sei. Die Smart Cards könnten auf triviale Weise ausgelesen, über Zusatzwerkzeuge wie Chameleon Mini simuliert oder ganz einfach kopiert werden. Eine billige Blankokarte aus China reiche dann aus, um auf fremde Rechnung Strom zu tanken. Ein betrogener Nutzer bekomme das im Zweifelsfall erst einen Monat später im Rahmen seiner Abrechnung mit. Die Schwäche betreffe alle ihm bekannten Ladekartensysteme, betonte Dalheimer.

USB-Ports für die Wartung der Geräte eröffnen weitere „Spielwiesen“. Dalheimer zeigte, dass er zu einem der Lademodule Root-Zugang hatte und darüber signalisierte: „Heute gratis laden.“ Auch Kartennummern vorangegangener Fahrer könnten so extrahiert und missbraucht werden.

Konten-Klau

Der Sicherheitsforscher Vincent Haupert enthüllte Details, wie er zusammen mit einem Kollegen schwere Lücken in 31 Banking-Apps ausnutzen und etwa Überweisungen durch untergeschobene IBANs und geänderte Zahlbeträge manipulieren konnte. Bekannt war bereits, dass auf das „appTAN“-Verfahren setzende Anwen-

Karten für E-Tankstellen kann man fälschen, um Strom auf fremde Rechnung zu zapfen.

Bild: CC by 4.0 34C3 media.ccc.de

dungen, beispielsweise von Comdirect, der Commerzbank und der Fidor-Bank, betroffen sein sollten (siehe c't 26/2017, S. 14). Haupert setzte nun unter anderem die BB-Bank, die Citibank, Wüstenrot und die Volks- und Raiffeisenbanken mit auf die Liste. Den Apps gemeinsam war, dass sie die Komponente „Shield" des norwegischen Unternehmens Promon verwenden. Das habe auf den Sicherheitshinweis reagiert und eine neue Shield-Version entwickelt. Das Hauptproblem bleibe aber bestehen: Für eine echte 2-Faktor-Authentifizierung wären zwei separate Endgeräte nötig – eins fürs Banking und eins, um die TAN zu erhalten oder zu generieren.

Andere Hacker erläuterten auf dem 34C3, wie sie das Verschlüsselungssystem des Staubsaugers „Mi Robot Vacuum" von Xiaomi unter anderem mit etwas Alu-Folie knackten und das Gerät aus der Cloud der Chinesen „befreiten". Die Sicherheitsforscherin Silke Holtmanns warnte vor Abhörmöglichkeiten der Handy-Kommunikation, da vor allem wegen des Kostendrucks im Mobilfunkmarkt das mit 4G verknüpfte Authentifizierungs- und Abrechnungsprotokoll Diameter nicht immer sachgerecht eingesetzt werde.

Bereits im Sommer hatte der CCC massive Schwachstellen in der Auswertungssoftware PC-Wahl aufgedeckt, die in vielen Bundesländern eingesetzt wird. In Leipzig hat die Hackervereinigung die Konsequenz daraus formuliert: Zur Auswertung von Wahlergebnissen dürfe künftig nur noch Open Source verwendet werden. Thorsten Schröder erklärte dazu: „Oldtimer-Software" wie PC-Wahl müsse „in modernen, sicheren Programmiersprachen mit zeitgemäßen Konzepten neu geschrieben und auditiert werden." Auch die Ergebnisse begleitender Prüfungen sollten „parallel mit Quellcode publiziert werden".

Satelliten-Spiele

Pierros Papadeas berichtete in Leipzig davon, wie in nur sechs Monaten ein Open-Source-Satellit namens Upsat entstand, der die Plasmakonzentration in der Thermosphäre misst. Den Auftrag erhielt die von Papadeas gegründete Libre Space Foundation von der Universität Patras. An der Ausführung war der Hackerspace Athen maßgeblich beteiligt.

Rund um die wissenschaftliche Nutzlast bauten die Tüftler dort einen Steuercomputer, einen „Positionsfinder" in Form einer Kamera und eine GPS-Antenne. Letztere stelle einen der verbliebenen „schwarzen Flecken" im Open-Source-Bereich dar, da es dafür nur reguläre Lizenzen für einige tausend Euro gebe, beklagte Papadeas. Parallel habe das Team die elektronische Seite für die Kommunikation zwischen den einzelnen Bauteilen beackert. Vorgefunden habe es teils 30 bis 40 Jahre alten Code für Mikrocontroller, den sie durch Open Source ersetzten. Nach weniger als einem Monat habe ein Modell für das „Communication Board" auf dem Tisch gelegen. Drum herum mussten noch eine Box und eine Stromversorgung mit Solarzellen und Akkus gebaut werden.

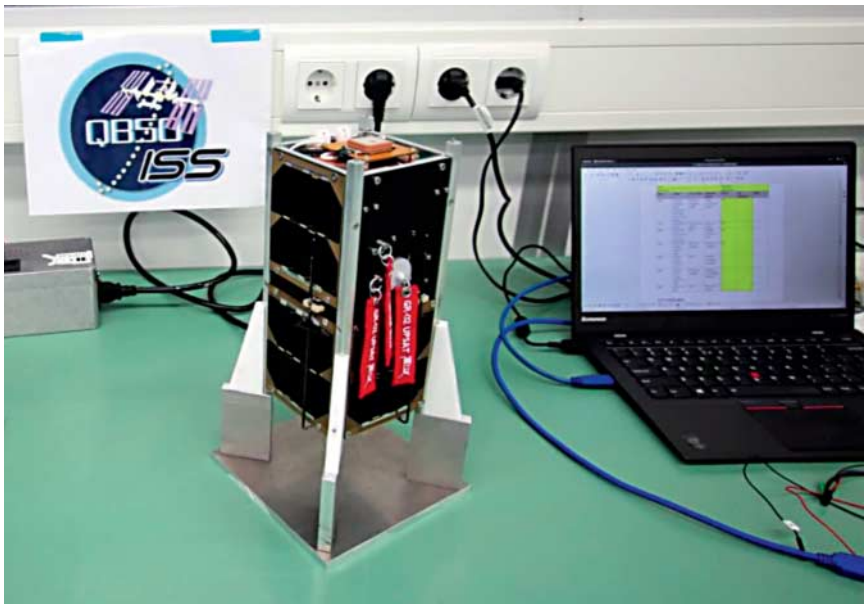

Bild: CC by 4.0 34C3 media.ccc.de

Der Open-Source-Satellit Upsat misst die Plasmakonzentration in der Thermosphäre und sendet die Daten zur Erde.

Um die Komponenten zusammenzufügen, benötigten die Macher eine „Clean Box", wie sie etwa auch bei der Halbleiterproduktion im Einsatz ist. Diese entwarfen sie selbst, ebenso wie die Vakuumkammer, in denen die Programmierer die thermischen Eigenschaften des Komplexes unter simulierten Weltraumbedingungen testen konnten. Schließlich mussten die Entwickler den Satelliten noch auf seine elektromagnetische Verträglichkeit prüfen. Da dies im Hackerspace nicht möglich war, wichen sie auf ein früheres Militärlabor aus.

Für die Bodenstationen hatte die Libre Space Foundation schon früher ein Open-Source-Kit entwickelt, das aus einer Dreheinrichtung, einer rund 300 Euro teuren Antenne, einem eigenen Controller auf Basis des Raspberry Pi 3, GNU Radio und einer Client-Software besteht, die unter anderem Logs aufzeichnet. Dazu gekommen ist inzwischen eine Datenbank, die dem Crowd-Sourcing von Satellitendaten dient und für das Archivieren von Audiodateien mit dem Internet Archive kooperiert. Es gibt auch eine öffentliche Programmierschnittstelle (API), über die Apps von Dritten eingebunden werden können.

Am 17. Mai 2017 brachte eine Trägerrakete aus den USA den Upsat zur Internationalen Raumstation ISS, von der aus er einen guten Monat später in den Weltraum „ausgespuckt" wurde. Nach der vorgeschriebenen Wartezeit von 30 Minuten sei der weltweit erste Open-Source-Satellit in den Operationsbetrieb gegangen, freute sich Papadeas. Wenig später habe er die ersten Daten an Bloomington im US-Bundesstaat Indiana gefunkt.

Vom Boden wurden dann Prozesse wie der Ladezyklus des Flugkörpers überwacht. Doch es lief nicht alles einwandfrei: Das Heiz- und Kühlaggregat für den Akku verbraucht zu viel Strom, weshalb sich Upsat häufig in den Ruhezustand versetzt und nur während vergleichsweise kurzer Zyklen Daten sendet. Dennoch bezeichnete Papadeas das Projekt als geglückt, da die Tüftler den Großteil der Technik richtig konstruiert hätten und Nachahmer nun auf den Ergebnissen aufbauen könnten. Es sei „keine höhere Mathematik", eigene Flugobjekte fürs All zu fertigen. Die Gesamtkosten hätten sich mit 120.000 US-Dollar im unteren Rahmen bewegt. *(ad@ct.de)* c't