kiss/shutterstock.com

Wer vertraut dem Blauzahn?

von Matthias Deeg, Gerhard Klostermeier & Sebastian Schreiber

Harald I. „Blauzahn“ Gormsson war ein Kommunikationstalent. Ganze Völker hat er vereint. Das ist zwar Jahrhunderte her, war aber dennoch Grund genug dafür, den dänischen Wikingerkönig als Namensgeber für das in den 1990ern entwickelte Funkverfahren „Bluetooth“ heranzuziehen. Bluetooth befreite zunächst das Mobiltelefon vom lästigen Kabel und sorgte auf seinem weiteren Siegeszug dafür, dass heute zahllose Geräte drahtlos miteinander kommunizieren. Tastaturen und Mäuse sprechen mit dem PC, Mobiltelefone mit Kopfhörern – wie von Geisterhand. Das ist bequem. Einst entwickelt für den Consumer-Bereich, halten die Fähigkeiten des Funkprotokolls aber auch zunehmend Einzug in die Industrie, etwa in der Gebäude- und Fabrikautomation. Die auf Bluetooth basierende Vernetzung verspricht viel. Zuverlässigkeit: Der Ausfall einer Komponente beeinträchtigt das Gesamtnetz kaum. Skalierbarkeit: Mehrere Tausend Geräte im Verbund sind möglich. Sicherheit: Hoher Schutz gegen Angriffe von außen. Ist der Blauzahn der Gegenwart also tatsächlich bequem und sicher?

Grundlagen der Bluetooth-Sicherheit

Die drahtlose Funktechnologie Bluetooth – derzeit in verschiedenen Versionen von 1.0 bis 5.0. verbreitet – dient dem Austausch von Daten über kurze Entfernungen. Bluetooth wird von der Bluetooth Special Interest Group (SIG) betrieben und ist in Dokumenten wie „Bluetooth Core Specification Version 5.0“ definiert. Das Bluetooth-Sicherheitsmodell beinhaltet fünf Elemente:

1. Kopplung („Pairing“): Prozess der erstmaligen Verbindungsaufnahme zur Erzeugung eines oder mehrerer gemeinsamen/r Sicherheitsschlüssel/s
2. Bindung („Bonding“): Vorgang der Speicherung der erzeugten Schlüssel, um ein vertrauenswürdiges Gerätepaar für nachfolgende Verbindungen zu bilden
3. Geräteauthentifizierung („Device Authentication“): Überprüfung, dass die beiden Geräte dieselben Schlüssel nutzen
4. Verschlüsselung („Encryption“): Sicherstellung der Nachrichtenvertraulichkeit
5. Integrität („Intregrity“): Schutz vor Nachrichtenfälschungen

Um miteinander zu kommunizieren, müssen die Geräte ein „Geheimnis“ teilen. Dieses Geheimnis, ein kryptografischer Schlüssel, wird während des Kopplungsprozesses erstellt. Jedes gekoppelte („bonded“) Bluetooth-Gerät speichert einen oder mehrere gemeinsame Sicherheitsschlüssel für vertrauensvolle, nachfolgende Verbindungen lokal ab. Neben diesem kryptografischen Schlüsselmaterial speichert jedes gekoppelte Gerät darüber hinaus die Bluetooth-Adresse (BD_ADDR) der Geräte, mit denen das Geheimnis geteilt wird.

Die Angriffsvorbereitungen

Bei einem Forschungsprojekt machte die SySS GmbH zwei Beobachtungen, aus denen sich in Kombination eine interessante Angriffsmöglichkeit auf das Vertrauensverhältnis bei Bluetooth-Verbindungen ergibt:

1. Das kryptografische Schlüsselmaterial gekoppelter Bluetooth-Geräte kann von einem Angreifer mit physischem Zugang ohne größere Probleme extrahiert werden.
2. Die meisten Bluetooth Stacks moderner Betriebssysteme – das sind Protokolle in einer hierarchischen Ordnung, die die Nutzung mobiler Funkverbindungen ermöglichen – verknüpfen die spezifischen Eigenschaften eines gekoppelten Bluetooth-Gerätes nicht mit den Verbindungsinformationen.

Bei einem Test mit Bluetooth-Tastaturen stellte sich heraus, dass die meisten Bluetooth-Stacks nicht darauf reagieren, wenn gekoppelte Geräte ihre Eigenschaften verändern. Mit einem eigens entwickelten Softwaretool, dem „Bluetooth Keyboard Emulator“, ließ sich z. B. der Name, die Hersteller-ID oder die Seriennummer eines Geräts beliebig anpassen, ohne dass der gekoppelte Host dies beanstandete. Einzig die Bluetooth-Adresse und der Link Key mussten identisch bleiben.

Was jedoch noch interessanter war: Manche Bluetooth-Stacks reklamierten nicht einmal veränderte Geräteklassen oder Funktionen. Was aber, wenn aus dem einmal gekoppelten und damit als vertrauensvoll eingestuften Gerät plötzlich ein ganz anderes wird?

Das Angriffsszenario

Nehmen wir also folgendes Szenario für einen möglichen Hacker-Angriff an:

Matthias Deeg, Expert IT Security Consultant und Head of Research & Development bei der SySS

Gerhard Klostermeier, Senior IT Security Consultant bei der SySS

Sebastian Schreiber, Diplom-Informatiker und SySS-Geschäftsführer

Bilder (3): SySS GmbH

1. Das potenzielle Opfer kauft Bluetooth-Kopfhörer und koppelt diese mit seinem Computer oder Smartphone.
2. Der Angreifer erhält Zugriff auf den Kopfhörer, etwa durch Verlust, Entsorgung, Verkauf oder ganz gezielt durch Diebstahl. Einige Minuten physischer Zugang zum Gerät sind ausreichend.
3. Der Angreifer extrahiert die Verbindungsinformationen aus den Kopfhörern. Mit entsprechenden Adaptern lässt sich der SPI Serial Flash-Chip, auf dem Bluetooth-Geräteadresse und Link Key gespeichert sind, auslesen (In-Circuit Reading).
4. Der Angreifer nutzt die extrahierten Verbindungsinformationen, um eine gültige Verbindung zum Computer oder Smartphone des Opfers mit einem emulierten Gerät herzustellen.
5. Abhängig vom Bluetooth-Stack des Opfergeräts kann das emulierte Gerät des Angreifers als ein völlig anderes fungieren, z. B. als Tastatur anstelle von Kopfhörern. Dies ermöglicht es dem Angreifer, bösartige Handlungen auf dem Opfergerät durchzuführen, um beispielsweise Zugang zu schützenswerten Daten zu erlangen.

Der Testlauf

Getestet wurde der Angriff mit einem handelsüblichen Bluetooth-Kopfhörer, der an verschiedene Clientsysteme mit unterschiedlichen Betriebssystemen gekoppelt wurde. In drei von fünf Testfällen war der Angriff mit dem emulierten Bluetooth-Gerät erfolgreich. Das Clientsystem akzeptierte die Verbindung mit der „nachgebildeten“ Bluetooth-Tastatur, die den extrahierten kryptografischen Schlüssel der Kopfhörer nutzte. Obwohl das ursprünglich verbundene Gerät ein Kopfhörer war, berücksichtigten die getesteten Android-, iOS- und Mac OS X-Clientsysteme keineswegs, dass die Vertrauensstellung zu einem Kopfhörer nun plötzlich eine Vertrauensstellung zu einer Tastatur darstellte, die tadellos funktionierte. Der Angriff funktionierte nicht bei Windows 10- und Arch Linux-Testsystemen. Die Gründe hierfür sind noch unklar und bieten Gegenstand für weitere Untersuchungen.

Die Testergebnisse zeigen, dass mit dem eigens entwickelten Bluetooth Key Emulator Profiländerungen gekoppelter Bluetooth-Geräte weiterhin möglich sind und von Angreifern ausgenutzt werden können. Dabei zeigen nicht nur iOS-Geräte diese Anfälligkeit, sondern auch Android- und Apple OS X-Geräte.

Ist dem Blauzahn noch zu trauen?

Das hier vorgestellte Angriffsszenario zeigt deutlich: Auch Bluetooth-Geräte wie z. B. Kopfhörer, die auf den ersten Blick als weniger schützenswert angesehen werden, lassen sich für Angriffe auf „interessantere“ Bluetooth-Geräte – etwa ein geschäftlich genutztes Smartphone – missbrauchen. Daher sollte die ursprünglich etablierte Vertrauensstellung zwischen Bluetooth-Geräten von Zeit zu Zeit überprüft werden.

Bluetooth – bequem und sicher also? Insbesondere bei Zusatzgeräten, denen in puncto Sicherheit weniger Aufmerksamkeit geschenkt wird, lohnt sich ein Funken mehr Sicherheitsbewusstsein. Damit der „harmlose“ Kopfhörer nicht zur bösen Tastatur mutiert.

Continuous Attack and Threat-Simulation (CAT-Simulation)

Cyberbedrohungen stets im Blick

von Jürgen Bruder

Im Zuge der fortschreitenden Digitalisierung werden IT-Infrastrukturen immer komplexer. Damit vergrößert sich gleichzeitig die Angriffsfläche. Mit Ransomware, spezifischer Malware oder Phishingattacken haben Cyberkriminelle in den vergangenen Jahren für enorme Schäden gesorgt. Und das Bedrohungspotenzial steigt. Derzeit setzen Hacker häufig Programme ein, die Sicherheitslücken in der Software gezielt ausnutzen. Um solchen Attacken wirkungsvoll zu begegnen, sind Technologien der nächsten Generation gefragt.

Jürgen Bruder, Bereich Cyber- und Informationssicherheit, TÜV Hessen

Unbekannte Schwachstellen werden häufig erst nach erfolgreichen Angriffen entdeckt. Diese Latenz nutzen Hacker zielstrebig und effizient aus. Doch bisher wird die Sicherheit von IT-Systemen oftmals nur mit klassischen Verfahren, wie Penetrationstests, geprüft. Aber dabei handelt es sich – methodisch bedingt – nur um Momentaufnahmen. Schon kleinste Veränderungen in der Infrastruktur nehmen dem Ergebnis seine Aussagekraft. Punktuelle Analysen einzelner Objekte sind ebenfalls nicht erfolgversprechend, denn nur die Summe aller Untersuchungen zeigt den realen Sicherheitsstatus.

Die nächste Stufe

Um den Schutz der IT-Infrastrukturen dauerhaft zu gewährleisten, ist deshalb eine kontinuierliche Prüfung notwendig, die auch aktuelle Angriffsvektoren berücksichtigt. Die Continuous Attack and Threat-Simulation (CAT-Simulation) von TÜV Hessen simuliert deshalb real existierende Cyberangriffe rund um die Uhr. Dafür setzt der Managed Service verschiedene Methoden zur Angriffssimulation unterschiedlicher Vektoren ein, wie E-Mail-, Netzwerk-, und Firewall-Attacken. Zudem wird auch die Infrastruktur und die Endgerätesicherheit geprüft. Die Grundlage für die CAT-Simulation ist die LION-Plattform (Learning I/O-Network), ein lernendes Netzwerk, das permanent neue Vektoren in seine Simulation integriert und auch komplexe Angriffsmöglichkeiten kombiniert.

Wie effizient die installierten Sicherheitstechnologien arbeiten, zeigen die Ergebnisse der kontinuierlich simulierten Angriffe übersichtlich auf einem Dashboard. Eine Auswertung bietet die Chance, die Wirkung der eingesetzten Lösungen weiter zu steigern. Die CAT-Simulation macht Cybersicherheit damit erstmals kontinuierlich messbar – und zertifizierbar.

juergen.bruder@tuevhessen.de
www.tuev-hessen.de