

Mobiler Funk-Hacker

Portables Software Defined Radio im Test

Um die Sicherheit von Funkverbindungen zu untersuchen, nutzen Hacker ein Software Defined Radio wie das HackRF One. Die Erweiterung Portapack macht dieses zu einem portablen Gerät für den mobilen Einsatz, das auch ohne Rechner funktioniert.

Von Tobias Scheible

Funkverbindungen sind ein unsichtbares und häufig unterschätztes Sicherheitsrisiko. Nicht selten kommen noch Jahrzehnte alte Funkprotokolle zum Einsatz, die heutigen Ansprüchen an die Sicherheit nicht gerecht werden können. Ein prominentes Beispiel ist die anfällige Grünphasen-Steuerung unzähliger Verkehrsampeln in ganz Deutschland [1], aber auch zu Hause funken etwa Fernbedienungen von Zentralverriegelungen und Garagentoren, Komponenten von Smart-Home-Systemen und weitere Geräte oft noch mit unsicheren Protokollen.

Um die Sicherheit solcher Funkverbindungen zu überprüfen, eignen sich sogenannte Software Defined Radios (SDRs) besonders gut. SDRs nutzen Chips, die Phase und Amplitude von Funkwellen roh digitalisieren können, um diese Daten an einen Computer weiterzureichen. Diese Rohdaten erlauben es, Mischer, Filter und Demodulatoren in Software umzusetzen, was SDRs sehr flexibel macht. Sie beherrschen praktisch jede Modulationsart (FM, AM, QAM etc.), solange die Bandbreite der Aus-

tet. Besitzt das SDR Sendehardware, klappt das auch in die andere Richtung. Das abgedeckte Frequenzspektrum und die unterstützte Bandbreite variieren von SDR zu SDR.

HackRF One

Ein typischer Vertreter dieser Geräteklasse ist das HackRF One. Es wird zum Testen und Entwickeln von Funktechnologien eingesetzt, aber auch von Hackern. Entwickelt hat es Michael Ossmann von Great Scott Gadgets, die Finanzierung lief bereits 2014 über Kickstarter.

Das HackRF One war das erste SDR mit Sendefunktion, das zu einem verhältnismäßig günstigen Preis angeboten wurde. Hard- und Software sind Open Source (GPLv2), wodurch sich eine große Community gebildet hat. Ein weiterer großer Vorteil ist, dass viele SDR-Anwendungen das HackRF unterstützen. Durch diese Faktoren gilt das HackRF One heute als wichtigstes Werkzeug für Penetrationstester, Hacker und Entwickler von Funktechnik.

Das vielseitige SDR empfängt und sendet Signale im Bereich von 1 MHz bis 6 GHz. Die Hardware hat theoretisch genug Leistung, um auch breitbandige Signale wie WLAN zu untersuchen. Die Firmware des HackRF One ist aktualisierbar, zudem kann man auf Alternativ-Firmware aus der Community zurückgreifen. Auf der Platine befinden sich Erweiterungsschnittstellen in Form von Pfostenleisten, über die man zusätzliche Komponenten anschließt. Zudem ist es darüber steuerbar.

Portapack

Um das HackRF One zum Leben zu erwecken, ist normalerweise ein Rechner



Bild: Tobias Scheible

geschlossen wird – zum Beispiel ein Notebook oder ein Raspberry Pi. Eleganter klappt das mit dem Portapack, einer Zusatzplatine, die man auf die Pfostenleisten des HackRF-Boards steckt. Es verwandelt das HackRF One in ein portables Standalone-Gerät. Damit gehen etwa das Aufzeichnen und Senden von Signalen sowie das Scannen nach Übertragungen auch unterwegs leicht von der Hand. So testet man Funkverbindungen sehr schnell, ohne sich in komplizierte SDR-Software einarbeiten zu müssen.

Das Portapack bringt Farbdisplay und Bedientasten mit und ergänzt außerdem einen MicroSD-Steckplatz und einen Audioanschluss. Je nach Modell sind auch noch ein Lautsprecher und ein JST-Anschluss für Lithium-Ionen-Akkus an Bord. Die beste Ausstattung bietet das aktuelle H2-Modell. In jedem Fall ist vor dem Bestellen ein prüfender Blick in die Produktbeschreibung gefragt, denn das Portapack steht ebenfalls unter GPLv2-Lizenz, es gibt deshalb viele Hersteller und subtile Unterschiede. Mitunter zählt sogar ein Touchscreen zur Ausstattung.

Um das Hardware-Add-on zu nutzen, muss man eine Portapack-Firmware auf dem HackRF installieren. Sie liefert die grafische Bedienoberfläche auf das Farbdisplay und die erforderliche Signalverarbeitung, die sonst auf dem Computer statt-

derzeit Mayhem. Dieser wird aktiv gepflegt, verwaltet Aufzeichnungen und wertet unter anderem ADS-B-Nachrichten (Informationen von Flugzeugen) aus. In der Produktbeschreibung sollte man darauf achten, dass das angebotene Portapack mit der Mayhem-Firmware kompatibel ist.

Das Originalgehäuse des HackRF passt nicht mehr, wenn die Portapack-Platine aufgesteckt ist. Es stehen aber diverse angepasste Gehäuse zur Auswahl. Wer Zugriff auf einen 3D-Drucker hat, druckt sich einfach selbst eines aus. Das Portapack ist sowohl für etwa 100 Euro separat erhältlich, also auch in Komplettsätzen mit SDR, Gehäuse und Akku. Mit etwas Glück kann man so ein Set auf einschlägigen Shoppingportalen wie AliExpress schon für rund 300 Euro bekommen.

Probehack

Um das Zusammenspiel von HackRF One und Portapack zu testen, haben wir einen Mini-Pentest durchgeführt: Ein klassischer Replay-Angriff sollte zeigen, wie es um die Sicherheit einer vernetzten Alarmanlage bestellt ist. Bei einem Replay-Angriff wird eine Übertragung aufgezeichnet und zu einem späteren Zeitpunkt erneut gesendet – in der Hoffnung, dass der Empfänger beispielsweise einen Schaltbefehl erneut ausführt. Dabei muss die Struktur der Nachricht nicht bekannt sein und es kann sogar eine Verschlüsselung zum Einsatz kommen, sofern die verschlüsselten Funkpakete nicht variieren.

Übertragungen, die mit Einmalcodes (Nonce) gesichert sind, oder kontinuierliche Datenübertragungen, die eine Sequenznummer oder Message Authentica-

tion Codes (MAC) verwenden, sind nicht anfällig für solch einen Angriff. Das ist eigentlich seit Jahren Stand der Technik, allerdings werden immer noch Geräte verkauft, die nicht gegen Replay-Angriffe geschützt sind.

Aber Vorsicht: Fremde Systeme zu stören oder anzugreifen ist strafbar, solange deren Besitzer nicht ausdrücklich zugestimmt haben, etwa im Rahmen eines Pentests [2]. Zudem ist die Nutzung von Funkfrequenzen durch die Bundesnetzagentur streng reguliert [3].

Für den kleinen Pentest haben wir HackRF One und Portapack mit der Teleskopantenne ANT500 von Great Scott Gadgets eingesetzt, die wir an die SMA-Buchse des SDR geschraubt haben. Als Zielobjekt musste eine kleine Funkalarmanlage herhalten. Das Alarmsystem besteht aus Fenstersensoren, einer Fernbedienung zum Scharfschalten des Alarms sowie einer Basisstation mit Sirene und optischem Alarmgeber. Alles ist über Funk miteinander vernetzt. Ziel des Tests war es, das Signal zur Deaktivierung der Alarmanlage mit dem SDR aufzuzeichnen und die Anlage damit zu einem späteren Zeitpunkt zu entschärfen.

Um die Funkübertragung aufzuzeichnen, wählten wir im Hauptmenü des Portapack den Eintrag „Capture“ aus. Anschließend mussten wir noch die gewünschte Frequenz einstellen. Da die Alarmanlage laut Datenblatt auf dem Frequenzband 433 MHz arbeitet, stellten wir die typischerweise genutzte Frequenz ein (433,9 MHz). Ist ein funkendes Gerät nicht mit WLAN, Bluetooth oder Mobilfunk ausgestattet, findet man im Datenblatt meist 433 oder 868 MHz als Frequenzangabe.

Danach starteten wir die Aufzeichnung mit „REC“. Als wir auf der Fernbedienung der Alarmanlage die Taste zum Entschärfen drückten, wurde die Übertragung als helle Linie im Display des Portapack sichtbar und wir stoppten die Aufzeichnung. Das Ergebnis landete in einer Datei auf der Speicherkarte. Anschließend schalteten wir die Alarmanlage mit ihrer Fernbedienung wieder scharf.

Zeit für das große Finale: Wir sendeten das zuvor aufgezeichnete Entschärfungssignal mit dem SDR aus, indem wir das Wiedergabesymbol (Dreieck nach rechts) auf dem Display aktivierten. Die Alarmanlage bemerkte den Schwindel nicht und quittierte das Entschärfen mit einem Blinken. Wir machten die Probe auf Exempel und öffneten einen Fenstersensor, der mit der Anlage gekoppelt war.

Wäre die Alarmanlage noch scharf gewesen, wäre ein lautstarker Alarm losgetönt – es passierte jedoch nichts, die Alarmanlage blieb stumm. Damit war der Replay-Angriff erfolgreich.

Fazit

Das HackRF One und die Erweiterung Portapack sind ein starkes Team. Mit dem Set kann man viele Tests und Untersuchungen von Funksignalen auch unterwegs schnell und einfach durchführen. Durch die große Community und die gute Unterstützung durch viele Anwendungen ist der Einstieg leicht.

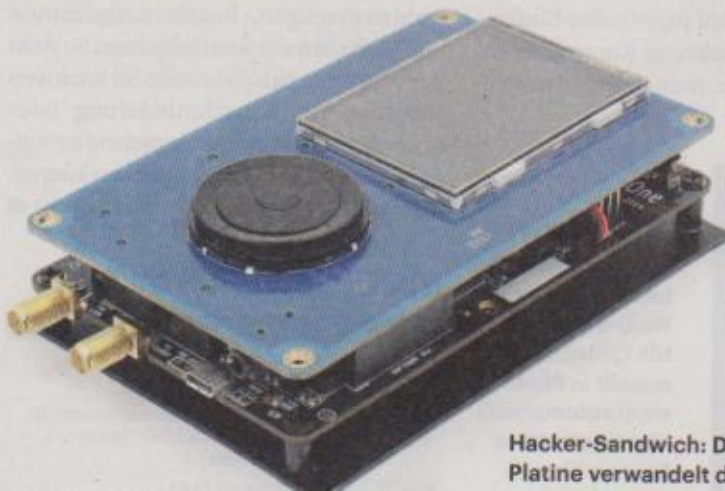
Die gebotenen Funktionen laden zum Experimentieren ein und eröffnen völlig neue Perspektiven zum Verständnis von Funkverbindungen. Wichtig ist jedoch, vor dem Loslegen die rechtliche Lage zu studieren, um nicht ungewollt gegen geltende Gesetze zu verstoßen. (rei@ct.de) 

Literatur

- [1] Ronald Eikenberg, David Wischnjak, Grüne Welle, Viele Ampeln sind per Funk einfach manipulierbar, c't 1/2023, S. 120
- [2] Verena Ehrl, Elektronische Übeltäter, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c't 18/2017, S. 78
- [3] Jonathan Laux, Ampel, werde grün!, Eingriffe in funkgesteuerte Verkehrsleitmatrie aus rechtlicher Sicht, c't 1/2023, S. 130

HackRF One mit Portapack

Mobiles Software Defined Radio	
Hersteller	diverse (Open Source)
Stromversorgung	Micro-USB oder Akku



Hacker-Sandwich: Die Portapack-Platine verwandelt das HackRF in