Textfänger

Raspberry Pi: Lauschangriff auf GSM-SMS

Vom Bastelcomputer zum Spionagegerät: Brisante Entdeckungen in Broadcoms ARM-SoCs für den Raspberry Pi zeigen, dass die Chips auch für das Mitschneiden und beschleunigte Entschlüsseln von 2G-Mobilfunk gerüstet sind – und das ohne Zusatzhardware.

Von Andrijan Möcker

Regierungen geben jedes Jahr Millionen aus, um Polizei, Militär, Geheimdienste und weitere Behörden mit Überwachungstechnik auszustatten. Regelmäßige Messen bringen Käufer und Hersteller zusammen – wer sich behauptet, kann auf hochpreisige Aufträge hoffen.

Sicherheitsforscher haben nun entdeckt, dass auch Broadcom ein Stück des Kuchens abhaben möchte: Die US-amerikanische Firma stellt von LEDs über WLAN-Modems bis hin zum System-on-Chip eine Vielzahl von Elektronikkomponenten her, die weltweit zum Einsatz kommen – auch im Raspberry Pi. In den Chips der Versionen 3 (BCM2837) und 4 (BCM2711) fand das niederländische IT-Security-Team undokumentierte Hardwarebeschleuniger für GSM-Kryptografie. In Kombination mit den ebenfalls von Broadcom hergestellten Chips für WLAN und Bluetooth kann der Raspberry Pi in ein gefährliches Spionagewerkzeug für Mobilfunk verwandelt werden. Die Forscher wandten sich im Januar anonym an c't und übermittelten ein Programm, das die Funktionen in Aktion zeigt.

Projekt Kviten

Das Team wollte ursprünglich die Firmware des beim Raspberry Pi 4 verwendeten Broadcom-Chips BCM2711 analysieren und auf undokumentierte Funktionen abklopfen, die für Bastler sinnvoll sein könnten. Broadcom hält sich seit Jahren größtenteils sehr bedeckt, wenn es um den Quellcode und ausführliche Datenblätter zu seinen Produkten geht. Veröffentlichungen versucht die Firma zu unterbinden. Das führte bereits öfter zu Schwierigkeiten beim Bau von Open-Source-Produkten wie dem Raspberry Pi. Aktuell ist zwar dessen Software größtenteils quelloffen, die Hardware jedoch nicht.

Die mutmaßliche Spionagefunktion entdeckte ein Forscher des Teams zufällig, als er aus Versehen die falsche Binärdatei auf eine bestimmte Bytesequenz durchsuchte und Kommentare entdeckte, die auf einen „Accelerator for cellular network cryptography" (ACNC) und ein „Projekt Kviten" hindeuten. Dem Informatikstudent fiel die Besonderheit sofort auf, denn der BCM2711 war nie für den Einsatz in Smartphones gedacht.

Eine genauere Untersuchung des Maschinencodes in der Datei ergab, dass der BCM2711 umfangreiche Funktionen besitzt, um Berechnungen mit dem beim Mobilfunkstandard GSM (2G) eingesetzten Verschlüsselungsalgorithmus A5 in Hardware zu beschleunigen. Trotz der Brisanz hatten Broadcoms Entwickler den Großteil des Codes umfangreich kommentiert, sodass das Team keine Schwierigkeiten hatte, den Programmcode und die damit verbundenen Funktionen zu rekonstruieren. „Wir vermuten, dass die Zeilen durch eine Unachtsamkeit in das Binary gelangt sind", sagte ein Mitglied des Teams im Gespräch mit c't. Im späteren Verlauf stellte das Team fest, dass auch der BCM2837 in den Raspberry-Pi-3-Versionen die Funktionen besitzt.

Konkret können die Prozessoren mithilfe einer zusätzlichen, in den RAM geladenen Indexdatei deutlich schneller als andere Prozessoren auf die seit 2009 zur Verfügung stehenden A5-Rainbow-Tables zugreifen und so die GSM-Verschlüsselung in wenigen Sekunden brechen. Um Telefongespräche zu entschlüsseln, müsste man allerdings die zwei Terabyte großen Tabellen auf den Raspberry laden.

Verschlüsselte Nachrichten auf GSM-Steuerungskanälen kann der Hardwarebeschleuniger jedoch ohne Rainbow-Tables brechen: Viele Netzbetreiber verwenden hier noch immer eine reduzierte Schlüssellänge von 24 Bit – eine Maßnahme aus der Entwicklung der GSM-Spezifikation in den 1980er Jahren, um die Standby-Zeit der Geräte zu verlängern. Über die GSM-Steuerungskanäle laufen aber nicht nur Betriebsparameter wie Frequenzkorrektur und Synchronisation, sondern auch SMS.

Erste Versuche mit einem externen Software Defined Radio (SDR) zeigten, dass 100 bis 160 Zeichen lange Kurznachrichten in 30 bis 120 Sekunden geknackt werden können – vorausgesetzt der Netzbetreiber hat nicht das gesamte Netz auf

Test Mode Support

The BCM43455 fully supports Bluetooth Test mode as described in Part I:1 of the *Specification of the Bluetooth System Version 3.0*. This includes the transmitter tests, normal and delayed loopback tests, and reduced hopping sequence.

In addition to the standard Bluetooth Test Mode, the BCM43455 also supports enhanced testing features to simplify RF debugging and qualification and type-approval testing. These features include:

- Fixed frequency carrier wave (unmodulated) transmission
  - Simplifies some type-approval measurements (Japan)
  - Aids in transmitter performance analysis
- Fixed frequency constant receiver mode
  - Receiver output directed to I/O pin
  - Allows for direct BER measurements using standard RF test equipment
  - Facilitates spurious emissions testing for receive mode
- Fixed frequency constant transmission
  - 8-bit fixed pattern or PRBS-9
  - Enables modulated signal measurements with standard RF test equipment

Der im Datenblatt des BCM43455 erwähnte Testmodus ist laut des Forscherteams der Schlüssel zur der breitbandigen Lauschfunktion des Chips. Dazu wird das Modem in den beschriebenen „Fixed frequency constant receiver mode" versetzt.

Das Kombimodem eines Raspberry Pis mit Anpassungskomponenten und Bandpass-Filter (weiß). Letzterer lässt sich nur sehr schwer entfernen – meist zerstört man das Modem beim Versuch.

die verbesserte Algorithmusvariante A5/3 umgestellt.

Getarnter Breitbandempfänger

Das Forscherteam vermutete zunächst, dass Broadcom die Entschlüsselungsfunktion mit einem externen Software Defined Radio in Form eines unscheinbaren USB-Sticks verkaufen würde, doch entdeckten wesentlich Gewiefteres: Der Code nutzt einen Testmodus der auf den Raspberrys verbauten Kombichips (WLAN+Bluetooth) der BCM43-Reihe. Dieser ermöglicht es, den Bluetooth-Chipsatz frei von 780 MHz bis 2,6 GHz arbeiten zu lassen. GSM wird in den meisten Ländern zwischen 800 MHz und 2 GHz betrieben. Weitere Befehle, die über die serielle Schnittstelle gesendet werden, ändern unter anderem die Bandwidth-Time des GMSK-Demodulators auf den für GSM passenden Wert 0,5. Weitere Änderungen sind nicht nötig, denn auch Bluetooth verwendet die GMSK-Modulation. Mit den passenden Einstellungen liefert der Chip einen rohen Bitstream der empfangenen Daten sowie weitere Informationen zur Signalstärke, der Frequenz und dem Störabstand.

In den Versuchen der Forscher erwies sich der Empfänger in den entsprechenden Frequenzbereichen jedoch als relativ taub. Eine Analyse in einem Labor für Hochfrequenztechnik ergab, dass die Raspberry Pis 3 und 4 einen Bandpassfilter für 2,4 und 5 GHz haben. Ob es hier Varianten ohne Bandpassfilter oder sogar mit einer weiteren Antenne gibt, ist noch ungeklärt: „Wir haben Befehle im Code entdeckt, die eigentlich unbelegte GPIOs am Modem ansprechen. Das könnte auf einen HF-Umschalter für eine zweite Antenne hindeuten."

Praxisversuch

Trotz der umfangreichen Gespräche, Screenshots und Screencasts erhielt c't lange keine Chance, den Fund selber zu testen – zu groß war die Sorge der Forscher, dass die Software in den falschen Händen großen Schaden anrichtet. Letztendlich erklärte sich das Team bereit, c't die erste rohe Version eines SMS-Decoders ohne Rufnummernanzeige bereitzustellen, das Rufnummern automatisch anonymisiert. Sie ist aufgrund der schlecht eingestellten Trennschärfe unbrauchbar für gezielte Spionage.

Der SMS-Empfang klappt so nur, wenn kein anderes WLAN- oder Bluetooth-Gerät in der Nähe funkt. Wir begaben uns mit einem Raspi 4 inklusive Display und Powerbank aufs Land, versetzten alle Handys in den Flugmodus und aktivierten das Beispielprogramm. Nach etwa fünf Minuten tauchte die erste SMS auf dem Display auf, die nächste erste nach 15. Keinen Erfolg hatten wir in der Nähe von Windrädern. Offenbar störte hier der rege Austausch über Funk, den die Windkraftwerke pflegen, den Empfang.

Eigene SMS zu empfangen erwies sich indes als schwierig: Sobald wir den Flugmodus unseres Handys deaktivierten, meldete das Programm zu hohe Signalpegel für eine Dekodierung. Eine in etwa 250 Metern Entfernung abgeschickte SMS bereitete dem Chip aber keine Probleme mehr und unser Text erschien auf dem Display.

Wenn Sie das Experiment selbst nachvollziehen wollen, finden Sie das Kommandozeilenprogramm mit dem Namen „huhtikuu" über ct.de/y3us. Laden Sie das Archiv auf einen Raspberry Pi (ab Version 3) mit einem aktuellen Raspbian und entpacken Sie es.

Öffnen Sie dann eine Kommandozeile und navigieren Sie in den Ordner, in dem das Programm liegt. Mit folgendem Befehl starten Sie die Einrichtungsroutine:

```
./huhtikuu prepare
```

War das erfolgreich, versorgen Sie den Raspberry per Powerbank (oder Adapter für den Zigarettenanzünder im Auto) mit Strom und verlassen Sie die Stadt. Sie sollten einen Standort wählen, der zwar abgelegen, dennoch einigermaßen mit Mobilfunk abgedeckt ist. Mit folgendem Befehl beginnt der Scan:

```
./huhtikuu scan
```

Haben Sie etwas Geduld. Sofern keine Störquellen erkannt wurden, sollten Sie nach etwa fünf bis zehn Minuten eine erste Nachricht sehen. Starke Störungen lassen den Scan abbrechen. Überprüfen Sie noch einmal, ob alle mitgeführten Geräte in den Flugmodus versetzt wurden. Hat alles funktioniert, sieht das Ergebnis so aus:

```
Message: **** ist Ihr Sicherheitscode
Timestamp:
Frequency: 929,5 MHz
Channel: SDCCH
Cipher: A5
```

Warnung

Verzichten Sie auf den Versuch, den Bandpass-Filter zu entfernen, um bessere Ergebnisse zu erzielen: Theoretisch kann der Bandpass-Filter, sofern korrekt identifiziert, vom Board des Raspberry Pis entfernt und die entsprechende Stelle überbrückt werden. In der Praxis ist dies aber selbst mit professionellem Werkzeug extrem schwierig. Das Forscherteam zerstörte nach eigener Aussage mehrere Raspberrys bei dem Versuch und kam nicht zum Erfolg.

SpyPi

Eine bei Broadcom angefragte Stellungnahme blieb bislang unbeantwortet. Doch das Projekt Kviten beweist, dass Broadcom weit mehr als einen SoC für Raspberry Pis im Sinn hatte, als es den BCM2711 und den BCM2837 für den Raspberry Pi 3 und den Raspberry Pi 4 entwickelte. Die beiden Versionen können so, wenn entsprechend angepasst, als harmlose Bastelplatine getarnt leicht durch jede Flughafen- oder Grenzkontrolle schlüpfen. Ob und wie der Raspberry Pi als Spionagewerkzeug zum Einsatz kam, wird sich wohl nie beantworten lassen. *(amo@ct.de)* c't

huhtikuu Download: ct.de/y3us