Schnelltipper

USB Rubber Ducky

Der USB Rubber Ducky ist nicht so harmlos, wie er aussieht. Am Rechner meldet er sich als USB-Tastatur an und übernimmt ungefragt das Ruder.

Von David Wischnjak

Der USB Rubber Ducky sieht absolut unverdächtig aus: Das Hacking-Gadget steckt in einem schwarzen Standardgehäuse für USB-Sticks und ist damit äußerlich nicht von einem gewöhnlichen Speicherstick zu unterscheiden. Seine wahren Absichten offenbart das Gerät erst, wenn es mit einem Rechner verbunden wird. Dann gibt es sich nicht etwa als Massenspeicher aus, sondern als USB-Tastatur (HID). Wer das Gerät etwa auf dem Firmenparkplatz findet und leichtfertig in den Rechner steckt, erlebt sein blaues Wunder: Der Rubber Ducky tippt in Windeseile vom Angreifer zuvor einprogrammierte Tastenbefehle runter – und das kann fatale Folgen haben.

So kann das Gerät etwa per Tastaturbefehl die mächtige Kommandozeile öffnen und dort alle Befehle ausführen, die auch der angemeldete Nutzer ausführen darf. Der Rechner kann so zum Beispiel mit Schadsoftware infiziert werden. Es gelang uns, den Rubber Ducky so zu konfigurieren, dass er vollautomatisch alle gespeicherten WLAN-Zugangsdaten einsammelt und per Mail verschickt. Aber auch harmlosere Aktionen sind möglich: Ein Pentester könnte zu Demonstrationszwecken etwa das Windows-Hintergrundbild ändern oder die Maustasten vertauschen. Prinzipiell eignet sich der Rubber Ducky auch, um wiederkehrende Admin-Aufgaben zu automatisieren.

Programmiert wird der Stick in einer simplen Skriptsprache namens Ducky-Script, mit der eine Abfolge von Tastatureingaben beschrieben wird. Im offiziellen Git-Repository (ct.de/y8mu) findet man viele fertige Skripte, die man nur noch auf die microSD-Karte im Bauch des Geräts kopieren muss. *(rei@ct.de)*

USB Rubber Ducky
Hersteller: Hak5
Preis: 45 US-$
Aufwand:
Gefahr:

Wolf im Hasenkostüm

Bash Bunny

Der Bash Bunny beherrscht nahezu jeden USB-Angriff. Mit diesem vielseitigen USB-Stick können Pentester im Vorbeigehen etwa Rechner übernehmen und Daten stehlen.

Von David Wischnjak

Etwas größer als ein Rubber Ducky (siehe oben) und damit nicht ganz so unverfänglich ist der Bash Bunny, dafür steckt darin ein leistungsfähiger Embedded-PC mit Quad-Core-ARM-CPU, 512 MByte RAM und einem angepassten Debian-Linux. Er führt alle Rubber-Ducky-Skripte und zudem auch Linux-Binaries aus. Außerdem hat er einen Schieberegler mit drei Positionen, zwei davon für verschiedene Angriffe und einen für das Beladen und Programmieren („Arming-Mode“). Im Unterschied zum Rubber Ducky verfügt der Bash Bunny über einen schnelleren internen Speicher. Ferner kann er sich auch als Netzwerkkarte oder serielle Schnittstelle am Rechner melden. Über Letztere greift man auf die Linux-Shell des Bash Bunny zu.

Pentester lassen einen Bash Bunny nicht irgendwo liegen – dafür ist er zu auffällig und auch etwas zu teuer –, vielmehr dient er ihnen als Werkzeug, um PCs im Vorbeigehen zu übernehmen. Das geht auch spurlos. So genügen einige wenige Befehle, um beispielsweise Daten wie alle im Rechner gespeicherten Passwörter direkt auf den Stick zu kopieren. Eine LED signalisiert dabei, wann das Gerät wieder herausgezogen werden kann. Der Bash Bunny kann als USB-Netzwerkkarte im Klartext übertragene Zugangsdaten aus dem Datenverkehr des Systems abgreifen – selbst dann, wenn der Rechner gesperrt ist (Details siehe S. 75). *(rei@ct.de)*

Bash Bunny
Hersteller: Hak5
Preis: 100 US-$
Aufwand:
Gefahr:

Buchstabenspion

KeyGrabber Wi-Fi Premium

Der KeyGrabber sieht aus wie ein harmloser Adapter, zeichnet aber sämtliche Tastatureingaben auf und verschickt sie per WLAN.

Von Ronald Eikenberg

Der optisch unauffällige KeyGrabber Wi-Fi Premium ist im Grunde ein in Hardware gegossener Trojaner: Das winzige Gerät wird einfach zwischen USB-Tastatur und Rechner gesteckt und zeichnet fortan sämtliche Tastatureingaben auf. Das Gerät arbeitet transparent; eine Verzögerung beim Tippen spürt man nicht. Sein wahres Gesicht offenbart es erst, wenn man eine zuvor festgelegte Tastenkombination auf der angeschlossenen Tastatur drückt – standardmäßig die Tasten „K“, „B“ und „S“ gleichzeitig. Dann meldet sich der Keylogger als Massenspeichergerät am Rechner an und gewährt Zugriff auf die Tastaturmitschnitte. Für diese ist im vier GByte fassenden internen Speicher ordentlich Platz. Dort findet man auch diverse Konfigurationsdateien, mit denen sich der Keylogger umfassend konfigurieren lässt. Alternativ kann man die Konfiguration auch über die Windows-Software „KL Tools“ durchführen.

Die von uns ausprobierte Premium-Version verband sich sogar über WLAN mit einem Accesspoint und verschickte darüber die Aufzeichnungen per Mail an die von uns vorgegebene Adresse. Zudem kann man die Mitschnitte jederzeit über die KL Tools abholen, wenn man sich im gleichen Netz befindet und das Passwort kennt. Auch wenn das Missbrauchspotenzial des USB-Keyloggers groß ist, so gibt es auch legitime Einsatzzwecke: etwa als autarker Backup-Speicher für Geschriebenes, dem auch ein PC-Crash nichts anhaben kann. *(rei@ct.de)*

KeyGrabber Wi-Fi Premium
Hersteller: KeeLog
Preis: 150 €
Aufwand:
Gefahr:

Datenverteiler

Throwing Star LAN Tap Pro

Mit dem LAN Tap Pro ist das Belauschen verkabelter Netzwerkverbindungen so einfach, wie es nur sein kann.

Von Ronald Eikenberg

So einfach wie genial ist der Throwing Star LAN Tap Pro: Man hängt ihn zwischen Netzwerk-Client und Netzwerk und kann fortan sämtliche übertragene Daten passiv mitlesen. Das schwarze Kästchen hat an vier Seiten RJ45-Buchsen: Links und rechts schließt man den Client und das Netzwerk an, vorne und hinten kommen die durchgeleiteten Daten raus. Dazu werden die Sendeleitungen der beiden überwachten Ports einfach elektrisch zu den Analyse-Ports geführt. Einen dieser beiden Analyse-Ports verbindet man mit einem Rechner, auf dem ein Packet Sniffer wie Wireshark oder tcpdump läuft. Im Sniffer erscheint anschließend alles, was die LAN Tap Pro passiert.

An den Analyse-Ports sind lediglich die Empfangsleitungen verbunden. Selbst wenn der Auswertungs-Rechner etwas sendet, werden diese Daten nicht verschickt. So kann man den Netzwerkverkehr verkabelter Geräte untersuchen, ohne dass Client oder Netz etwas davon mitbekommen können.

Der Throwing Star LAN Tap Pro kommt ohne Stromversorgung aus. Er leitet Netzwerkverbindungen mit maximal 100 MBit/s durch, Gigabit-Verbindungen stuft er auf diese Geschwindigkeit herab. Die von uns getestete Pro-Variante steckt komplett zusammengebaut in einem robusten Plastikgehäuse. Wir konnten auf Anhieb etwa Gespräche mitschneiden, die wir zu Testzwecken mit einem VoIP-Telefon führten. Wer möchte, kann sich für 15 US-Dollar einen Bausatz ordern, bei dem man noch die RJ45-Buchsen sowie zwei Kondensatoren aufs wurfsternförmige Board löten muss.

(rei@ct.de) c't

Throwing Star LAN Tap Pro
Hersteller: Great Scott Gadgets
Preis: 40 US-$
Aufwand:
Gefahr:

Schnüffel-Interface

LAN Turtle

Die LAN Turtle hat es aufs Netzwerk abgesehen: Pentester demonstrieren mit ihr Angriffe auf das lokale Netz und installieren etwa im Vorbeigehen eine aus dem Internet erreichbare Backdoor ins Firmennetz. Aber auch als smarte Netzwerkkarte kann das vielseitige Gerät dienen.

Von Ronald Eikenberg

Von außen betrachtet ist die LAN Turtle eine schnöde USB-Netzwerkkarte: Auf der einen Seite hat sie einen USB-Anschluss, auf der anderen eine RJ45-Netzwerkbuchse. In dem unspektakulären Gehäuse steckt ein Embedded-Rechner, der die volle Kontrolle über den durchgeleiteten Datenverkehr hat. Auf der LAN Turtle läuft die aus der Router-Welt bekannte Linux-Distribution OpenWRT, welche mit einem Arsenal an Angriffswerkzeugen vorbestückt ist. Damit kann man der Sicherheit von Netzwerken und Clients auf den Zahn fühlen.

Die LAN Turtle arbeitet unkonfiguriert wie eine USB-Netzwerkkarte und schleift den Datenverkehr unverändert an den angeschlossenen Rechner. Alternativ kann man das Gerät auch autark betreiben, dann wird sie über USB lediglich mit Strom versorgt und auf der anderen Seite mit dem Zielnetzwerk verbunden. Auf diese Weise hat ein Pentester einen optisch unauffälligen Client im Netz seiner Wahl, der unter seiner Kontrolle steht.

Um die LAN Turtle scharfzuschalten, verbindet man sich über USB mit ihr, woraufhin das Betriebssystem die Standardtreiber für USB-Netzwerk-Interfaces installiert. Auf der Turtle läuft ein DHCP-Server, welcher dem Rechner eine Netzwerkkonfiguration zuweist. Fortan ist man mit dem internen Netz des Hacking-Gadgets verbunden und kann via SSH als root zugreifen. Auf der Shell präsentiert sich ein Menü, mit dessen Hilfe die Einrichtung der Pentesting-Tools leicht von der Hand geht.

Zu den Tools zählt AutoSSH, das man dazu nutzen kann, um eine aus dem Internet erreichbare Backdoor ins Netzwerk einzurichten. Es baut einen sogenannten Reverse SSH Tunnel auf (siehe S. 77). Dabei wird eine ausgehende Verbindung zu einem System im Internet hergestellt. Der Pentester verbindet sich ebenfalls mit diesem System und kann darüber anschließend via SSH auf die LAN Turtle zugreifen. Das hat den Vorteil, dass der SSH-Server des Geräts nicht direkt aus dem Internet erreichbar sein muss. Wir konnten mit der Turtle erfolgreich einen solchen Tunnel bauen. Als Zwischenstation diente eine virtuelle Linux-Maschine in Microsofts Azure-Cloud. Durch den Tunnel hatten wir aus der Ferne vollen Zugriff auf das Netz, das mit dem LAN-Port der Turtle verbunden war.

Weiterhin ist unter anderem der Netzwerk-Scanner nmap vorinstalliert, der detaillierte Informationen über die Clients und Server im Netz liefert und deren Schwachstellen auskundschaftet. Möchte der Pentester das Abgreifen von Zugangsdaten demonstrieren (siehe Seite 75), nutzt er das QuickCreds-Modul der LAN Turtle. Dieses extrahiert Klartext-Passwörter und NTLM-Hashes aus dem durchgeleiteten Datenverkehr. In dieser Position des Man-in-the-Middle kann die Turtle zudem mit dsniff die aufgerufenen HTTP-Seiten protokollieren oder die Anfragen umleiten.

Auch als Admin hat man an den portablen Mini-Rechnern wahrscheinlich seine Freude. Wer gerne Herr über seine Daten ist, erhält einen smarten Netzwerkadapter, der den durchgeleiteten Traffic frei verändern kann – oder durch das Tor-Netz schleust. Limitiert ist das Gerät lediglich durch seine Hardware-Ausstattung: Es wird von einer 400 MHz schnellen MIPS-CPU angetrieben, der 64 MByte Arbeitsspeicher sowie 16 MByte persistentes Flash zur Seite stehen. *(rei@ct.de)*

LAN Turtle
Hersteller: Hak5
Preis: 50 US-$
Aufwand: ■■■■■□
Gefahr: ■■■■■■

USB-Zerstörer

USB Killer 3.0 „Anonymous“

Der USB Killer sieht aus wie ein harmloser USB-Stick, dient aber zur Beschädigung von Geräten mit USB-Buchsen wie PCs, Notebooks, Server, Smartphones, TV- und Audio-Elektronik, Autoradios oder Messtechnik.

Von Christof Windeck

Den USB Killer 3.0 liefert der Hersteller aus Hongkong ab 55 Euro direkt nach Deutschland. Die schwarze „Anonymous“-Version gleicht äußerlich einem USB-Speicherstift, beschädigt beim Einstecken jedoch viele Geräte mit USB-Buchsen irreversibel. Der Vorgang dauert nur wenige Sekunden und hinterlässt meistens keine äußerlichen Spuren. Für die Micro-USB-, USB-C- und Apple-Lightning-Buchsen von Smartphones, Tablets und Digicams liefert USB Kill gegen Aufpreis Adapter.

Der USB Killer lädt mit Energie aus der jeweiligen USB-Buchse einen Kondensator auf und erzeugt damit pro Sekunde acht Spannungspulse mit –220 Volt zwischen den beiden USB-2.0-Datenleitungen und der Masse der 5-Volt-Versorgung. Das ist für einige Geräte zu viel: Unser Test-Notebook ist nach nur wenigen Sekunden den Hardware-Tod gestorben (Video siehe ct.de/y5ny). Einem Smartphone machten die Stromstöße hingegen nichts aus.

Ob ein Gerät dem Sabotage-Stick standhält, lässt sich kaum beurteilen. Normgerechte USB-Geräte müssen zwar gegen elektrostatische Entladungen geschützt sein, doch dieser ESD-Schutz hilft nicht gegen alle Impulse und fehlt manchmal ganz. Unempfindlich sind nur Ladegeräte, die keine Datenleitungen nutzen; manche tun das aber, etwa für Schnellladung per QuickCharge. Dann kann sie der USB Killer ebenfalls beschädigen. Selbst wenn nur der USB-Controller über den Jordan geht, drohen bei vielen Geräten mit USB-Ports teure Reparaturen. Zum Schutz kann man nur raten, keine unbekannten USB-Geräte auszuprobieren. *(rei@ct.de)*

USB Killer 3.0 „Anonymous“
Hersteller: USBKill.com
Preis: 55 Euro
Aufwand:
Gefahr:

Sendepause

TV-B-Gone Kit

Weder neu noch gefährlich – aber immer wieder lustig: Der TV-B-Gone sorgt für Ruhe, wenn Fernseher diese stören.

Von David Wischnjak

Es läuft mal wieder irgendwo ein Fernseher und Ihr Gesprächspartner ist abgelenkt. Dabei haben Sie grad angefangen, von einem spannenden Artikel zu berichten, den Sie letztens in Ihrer Lieblings-Computerzeitschrift entdeckt haben. Ärgerlich, doch der TV-B-Gone schafft Abhilfe! Bei dem kleinen batteriebetriebenen Gerät handelt es sich um eine Art Mini-Fernbedienung, deren einziges Ziel es ist, Fernseher auszuschalten. Der Aufbau ist simpel und besteht im Wesentlichen aus einem Mikrocontroller und einer oder mehreren Infrarot-LEDs. Drückt man auf den Knopf, werden der Reihe nach über hundert Ausschaltcodes für verschiedene Fernseher durchprobiert. Das dauert bis zu zwei Minuten, häufig verwendete Codes kommen jedoch schon nach wenigen Sekunden dran.

Erstmals 2004 von Mitch Altman entwickelt, gibts den TV-B-Gone heute in den verschiedensten Varianten, oft auch zum Selberlöten und -programmieren. Der von uns getestete Bausatz von Adafruit enthält vier IR-LEDs, zwei davon sind fokussiert. Damit sollen laut Hersteller Reichweiten von bis zu 50 Meter möglich sein. Wir konnten damit alle TV-Geräte, die uns begegnet sind, erfolgreich aus einiger Distanz ausknipsen.

Die Aufbau-Anleitung (ct.de/y5ny) richtet sich primär an Anfänger, die gerne löten lernen möchten. Dazu gibt es Schaltpläne und den Quelltext für den Microkontroller. Das TV-B-Gone-Set ist ein guter Einstieg in das Hardware-Hacking. Man sollte es aber möglichst nicht im Elektronikfachmarkt um die Ecke ausprobieren. *(rei@ct.de)* c't

TV-B-Gone Kit
Hersteller: Adafruit
Preis: 20 US-Dollar
Aufwand:
Gefahr:

Hackzeugkasten

USB Armory

Der USB Armory ist ein vielseitiger Linux-PC im USB-Stick-Format. Pentester stecken ihre gewohnte Arbeitsumgebung damit einfach in die Hosentasche.

Von Ronald Eikenberg

Zu den vielseitigsten Hacking-Gadgets in unserer Auswahl zählt der USB Armory: Es handelt sich um einen Linux-PC im handlichen USB-Stick-Format. Der Kleinstrechner wird immerhin von einer 800 MHz schnellen ARM-Cortex-A8-CPU angetrieben, der 512 MByte RAM zur Seite stehen. Das Betriebssystem wird auf einer microSD-Karte gespeichert. Man hat die Wahl unter Linux-Distributionen wie Debian und Kali Linux. Letzteres ist der De-facto-Standard in der Pentesting-Szene, da es die wichtigsten Werkzeuge mitbringt.

Aufgrund der kompakten Bauform gibt es wenig Anschlüsse: Speicherkartenleser, USB-Anschluss und fünf GPIO-Anschlüsse. Über den USB-Host-Adapter kann man an der USB-Schnittstelle zum Beispiel WLAN- oder Bluetooth-Adapter betreiben. Gesteuert wird das System über SSH. Dazu verbindet man den USB Armory mit einem Rechner, woraufhin es sich als USB-Netzwerkkarte meldet. Anschließend konfiguriert der Armory den Rechner über DHCP und man kann schließlich eine SSH-Verbindung zu dem Stick aufbauen. Über ein USB-Netzwerkinterface kann der Stick auf bestehende Netze zugreifen, alternativ kann man ihn auch über den Rechner ins Netzwerk hieven, unter Windows etwa mithilfe der Internetverbindungsfreigabe.

Der Armory erlaubt seinem Betriebssystem weitreichenden Zugriff auf die USB-Schnittstelle und meldet sich auf Wunsch auch als USB-Eingabegerät für HID-Angriffe (siehe Seite 75) oder als Massenspeicher. Der Stick erfordert Einarbeitung und Linux-Kenntnisse – wer sich davon nicht abschrecken lässt, kann ihn jedoch vielfältig einsetzen. *(rei@ct.de)*

USB Armory
Hersteller: Inverse Path
Preis: 155 US-$
Aufwand:
Gefahr:

Piratensender

HackRF One

Das HackRF One kann nahezu beliebige Funksignale senden und empfangen. Damit können Pentester Smarthome-Alarmanlagen außer Gefecht setzen, Autos öffnen und SMS abfangen. Sogar Telefongespräche lassen sich abzapfen – oder man hört damit schlicht Radio.

Von David Wischnjak

Software Defined Radios (SDR) sind programmierbare Funksender oder -Empfänger, die hardwaretechnisch nicht auf einen Einsatzzweck beschränkt sind. Stattdessen bestimmt Software ihre Sende- oder Empfangsfrequenz und übernimmt die Signalverarbeitung. Das HackRF One zählt zu den beliebtesten Einsteiger-SDRs. Es hat einen Sende- und Empfangsbereich von 1 MHz bis 6 GHz. Es läuft im Half-Duplex-Betrieb – kann also nur abwechselnd senden und empfangen. Angesteuert wird es etwa mit der SDR-Entwicklungsumgebung GNU Radio.

Mit dem HackRF lassen sich allerhand Angriffe auf Funkverbindungen durchführen. Besonders beliebt sind Replay- und Jamming-Attacken. So konnten wir im Labor vernetzte Alarmanlagen überlisten, indem wir das Entschärfsignal der Handsender aufzeichneten und wieder abspielten (siehe c't 3/17, Seite 90). Auch Lauschangriffe auf GSM sind damit möglich (siehe Seite 76). In der Forschung, Hardware-Entwicklung und Maker-Szene findet das vergleichsweise günstige HackRF großen Anklang. *(rei@ct.de)*

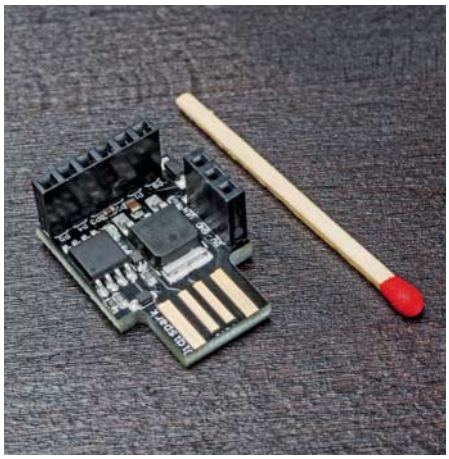
HackRF One
Hersteller: Great Scott Gadgets
Preis: 300 US-$
Aufwand:
Gefahr:

Klein, aber gefährlich

Digispark USB Development Board

Für wenig Geld kann das kompakte Digispark-Board viel: zum Beispiel die Kontrolle über einen Rechner übernehmen.

Von Ronald Eikenberg



Das Digispark-USB-Board ist das mit Abstand kleinste und auch günstigste der vorgestellten Gadgets: Wer es etwa über eBay versandkostenfrei direkt in Asien bestellt, zahlt mit etwas Glück weniger als zwei Euro, hierzulande kostet es sieben Euro. Dennoch sollte man das winzige Platinchen nicht unterschätzen: Es handelt sich um einen Arduino-kompatiblen Kleinstrechner, den man direkt in die USB-Schnittstelle eines Rechners, Smartphones oder anderen Geräts stecken kann. Dann wird der Digispark mit Strom versorgt und spult umgehend das auf ihm gespeicherte Programm ab. Wie USB Rubber Ducky und Bash Bunny kann sich der Digispark als USB-Eingabegerät am Rechner anmelden und anschließend beliebige Befehle absenden (siehe S. 75).

Je nach Einsatzzweck meldet das Board sich als USB-Tastatur, -Maus oder Joystick. Wir konnten mithilfe der Arduino-IDE im Handumdrehen ein kleines Programm schreiben, das eine ausführbare Datei aus dem Netz lädt und ausführt. Etwas kompliziert wurde die Sache lediglich dadurch, dass zwangsläufig das US-Tastaturlayout zum Einsatz kommt – ein „Z“ im Code tippt auf einem hiesigen System also ein „Y“ und umgekehrt. Man behilft sich, indem man die Eingabesprache des PCs auf US-Englisch umstellt, wenn man die vom Digispark einzutippenden Befehle einprogrammiert.

Natürlich gibt es für ein solches Arduino-System auch allerhand legitime Einsatzzwecke – etwa als kompakte Plattform für Hardware-Basteleien. Das Digispark-USB-Board hat sechs KByte freien Programmspeicher und kann über sechs I/O-Ports sogar Schalter, Sensoren und Funkmodule ansteuern. *(rei@ct.de)*

Digispark USB Development Board
Hersteller: Digistump
Preis: 7 €
Aufwand:
Gefahr:

RFID-Multifunktionstool

Proxmark3

Der Proxmark3 hat es auf alles abgesehen, was einen RFID-Chip hat. Damit lassen sich Zugangskarten klonen oder etwa Guthaben manipulieren. Doch es gibt auch legitime Einsatzmöglichkeiten.

Von David Wischnjak

Der Proxmark3 ist der De-facto-Standard für jeden, der sich tiefergehend mit NFC, Smartcards, RFID-Tags & Co. beschäftigt. Das Hardware-Design und die Software stehen unter einer Open-Source-Lizenz, er ist von mehreren Herstellern in unterschiedlichen Varianten erhältlich. Unsere Ausführung hat zwei Antennen, einen micro-USB Anschluss und einen optionalen Akku-Steckplatz für den autonomen Betrieb. Unterstützt werden eine Vielzahl von RFID-Standards auf 125-kHz-, 134-kHz- und 13,56-Mhz-Basis.

Ein typischer Einsatzzweck ist das Auslesen, Manipulieren und Klonen von Smartcards (siehe Seite 76). Letzteres gelang uns unter anderem bei einer Karte des Typs MIFARE Classic 1K, einem seit Jahren geknackten, aber weiterhin oft eingesetzten Smartcard-Typen. Außerdem kann das Gerät Übertragungen mitschneiden und beliebige RFID-Hardware emulieren. Jeder, der sich intensiver mit RFID-Technik beschäftigt, dürfte das vielseitige Proxmark3 auch für Entwicklungs- und Testzwecke zu schätzen wissen.

Die Inbetriebnahme kann sich für Einsteiger etwas knifflig gestalten. Zunächst muss man den Proxmark zusammenschrauben und die dazugehörige Software kompilieren. Danach ist noch etwas Einarbeitung nötig, um das Gerät ans Laufen zu bekommen. Im offiziellen Wiki (siehe ct.de/yyry) gibt es Anleitungen für mehrere Betriebssysteme, allerdings sind sie teilweise nicht ganz aktuell. *(rei@ct.de)* c't

Proxmark3 RDV2 Kit
Hersteller: Elechouse
Preis: 300 US-$
Aufwand:
Gefahr:

WLAN-Router aus der Hölle

WiFi Pineapple Nano

Der WiFi Pineapple demonstriert die Unsicherheiten von WLANs. Ein Angreifer kann damit einen Hotspot aufspannen, der Smartphones, Tablets und Notebooks magisch anzieht – und angreift.

Von David Wischnjak

Es gibt viele schmutzige Tricks, um WLAN anzugreifen. Der WiFi Pineapple beherrscht sie fast alle. Das Gerät ähnelt am ehesten einem WLAN-Router, es ist aber, anders als etwa eine Fritzbox, darauf ausgelegt, Daten abzugreifen und den Nutzern das Leben schwer zu machen. Dazu ist es mit einer ganzen Reihe bekannter Pentesting-Tools ausgestattet. Als Betriebssystem kommt OpenWRT zum Einsatz.

Mit seinen zwei WLAN-Modulen ist der WiFi Pineapple prädestiniert für Man-in-the-Middle-Attacken. Ein Pentester würde mit dem einen Modul einen verlockend klingenden Hotspot wie „Telekom“ oder „Free Wifi“ aufspannen und das andere mit einem legitimen Netz in der Nähe verbinden, um seinen zukünftigen Opfern den Zugriff aufs Internet zu ermöglichen. Alternativ lässt sich Internet über den USB-Port des Pineapple einspeisen. Dazu schließt man einen Mobilfunkstick oder ein Android-Smartphone an. Das hat den Vorteil, dass beide WLAN-Module für andere Zwecke nutzbar bleiben.

Um nichts dem Zufall zu überlassen, kann der Pentester mit Deauthentification-Paketen dafür sorgen, dass Smartphones & Co. die Verbindung zum derzeit genutzten Netz verlieren und mit einer guten Wahrscheinlichkeit in sein Netz fallen (siehe S. 77). Sobald sich ein Nutzer mit dem Pineapple verbindet, kann der Pentester den gesamten Traffic mitlesen und manipulieren. Mit dem Tool Responder kann der Spezialrouter gezielt nach Zugangsdaten und NTLM-Hashes greifen (siehe S. 75).

Verschlüsselung knacken

Der Pineapple versucht auf Befehl auch, verschlüsselte Netze in Reichweite mit Aircrack-NG zu knacken. Zudem kann er verwundbare Router mit Reaver-WPS über die WPS-Schnellkonfiguration attackieren. Nichts davon erfordert für den Pentester die Nähe zum Tatort: Ähnlich wie beim LAN Turtle kann man mit AutoSSH eine Reverse Shell zum Pineapple einrichten (siehe S. 77). Ist das Gerät erst mal irgendwo platziert, kann der Pentester von jedem Ort der Welt mit dem lokalen Netz und dessen Teilnehmern sprechen.

Die Pentesting-Werkzeuge werden über eine Web-Oberfläche konfiguriert und ausgeführt. Dort findet sich auch ein Paketmanager zur Installation weiterer Module. Zur Steuerung verbindet man den Pineapple per USB mit dem Rechner. Das Gerät meldet sich dann als USB-Netzwerkinterface, über das der Rechner mit dem internen Netz verbunden wird. Alternativ kann man auch ein passwortgeschütztes Konfigurations-WLAN aufspannen, welches allerdings eines der beiden WLAN-Module belegt.

Den WiFi Pineapple gibt es in zwei Varianten: kompakt als „Nano“ oder leistungsfähiger in der „Tetra“-Ausführung. Äußerlich wirkt der Nano wie ein etwas überdimensionierter USB-WLAN-Adapter, der Tetra erinnert an einen WLAN-Accesspoint. In beiden Geräten stecken aber vollwertige Embedded-PCs auf ARM-Basis. Der Tetra beherrscht im Unterschied zum Nano auch das 5-GHz-Band und bietet eine höhere Sendeleistung, hat einen Ethernet-Anschluss und einen schnelleren Prozessor.

Selbst wenn man sich für die (Un-)Sicherheit kabelloser Netze nur geringfügig interessiert, kann man mit dem Pineapple seine Freude haben. Dank der offenen Architektur und guten Erweiterbarkeit kann man damit untypische Netzwerkkonfigurationen bewerkstelligen – beispielsweise taugt das Gerät als mobiles Tor-Gateway oder als WLAN-Repeater, der im Falle einer WLAN-Störung auf einen per USB angeschlossenen LTE-Stick ausweicht. Wer das volle Potenzial des WiFi Pineapple ausschöpfen möchte, sollte Vorkenntnisse in puncto Linux-Netzwerkkonfiguration mitbringen. *(rei@ct.de)*

WiFi Pineapple Nano
Preis: 100 US-$ (Tetra: 200 US-$)
Hersteller: Hak5
Aufwand: ■■■□□
Gefahr: ■■■■■

GSM-Wanze

X009

Bereits ab 13 Euro bekommt man ein Überwachungsgerät im Format einer Streichholzschachtel, das sowohl Ton als auch Bild per Mobilfunk überträgt.

Von Ronald Eikenberg

Das winzige Multifunktionsgerät X009 wird zur Überwachung von Kindern, Senioren und Haustieren sowie als Diebstahlschutz beworben. Stattet man es mit einer SIM-Karte aus, nimmt es Kontakt zum Mobilfunknetz auf und lässt sich anschließend über SMS-Befehle konfigurieren und steuern. Das akkubetriebene Gerät ist sowohl mit Mikrofon als auch Kamera ausgestattet, beides in mäßiger Qualität. Wird ein einstellbarer Lärmpegel überschritten, ruft das X009 auf Wunsch eine vorher festgelegte Rufnummer an und überträgt die Umgebungsgeräusche. Wer etwas Verdächtiges hört, kann per SMS ein Foto anfordern, welches das Gerät per MMS verschickt. Zudem gibt es Befehle, die eine Ton-, Foto- oder Videoaufzeichnung auf MicroSD-Karte auslösen.

Betätigt man den roten SOS-Knopf, sendet das X009 eine fest eingestellte Notfall-SMS an bis zu fünf Rufnummern. Darüber hinaus kann das Kistchen über GPRS seinen ungefähren Standort an einen Webdienst übertragen. Das X009 wird in mindestens drei Revisionen verkauft, die man kaum auseinanderhalten kann. Damit scheint selbst der Hersteller ein Problem zu haben: Das mitgelieferte Handbuch war offensichtlich für eine andere Revision bestimmt, ausgerechnet die abgedruckten SMS-Befehle waren nicht korrekt. Wer in China bestellt, bekommt das Gerät bereits ab 13 Euro. *(rei@ct.de)*

X009
Hersteller: verschiedene
Preis: ab 13 €
Aufwand: ■■□□□
Gefahr: ■■■□□

Blaues Wunder

Ubertooth One

Das Ubertooth One erlaubt Entwicklern und Hackern tiefe Einblicke in Bluetooth-Verbindungen.

Von Michael Link

Eigentlich ist der Ubertooth-USB-Stick eine Open-Source-Entwicklungsplattform für Bluetooth-Geräte, die mit Bluetooth-Funk auf dem 2,4-GHz-Frequenzband kommunizieren. Das sind beispielsweise Fitnesstracker, aber auch Smartwatches, Bluetooth-Schlösser und Tastaturen.

Mit dem Ubertooth-Stick kann man aber auch die Kommunikation zwischen Bluetooth-Geräten untereinander belauschen, ohne dass man mit ihnen verbunden sein muss. Daher bleibt man als Mitschneider unentdeckt. Weil der Stick auch senden kann, lassen sich damit sogar Man-in-the-Middle-Attacken ausführen, zum Beispiel, um die Kombinationen besagter Schlösser zu ändern. All das funktioniert nicht nur mit herkömmlichem Bluetooth, sondern auch mit der mittlerweile sehr verbreiteten Stromsparvariante Bluetooth Low Energy (BLE). Gelingt es einem Angreifer, den Pairing-Prozess mitzuschneiden, kann er mit einer hoher Wahrscheinlichkeit sogar verschlüsselte Verbindungen knacken.

Um den Ubertooth-Stick nutzen zu können, braucht man Rechner mit Linux oder macOS und die Kenntnis einiger grundlegender Konsolenbefehle, um Treiber, Bluetooth-Baseband-Protokolle und die Ubertooth Tools zu installieren. Bei dem populären Wireshark-Programm zur Analyse von Datenverkehr ist das nötige Plug-in seit Version 1.12 bereits vorinstalliert.

Als Startpunkt für eigene Vorhaben findet sich im Github-Repository von Great Scott Gadgets (ct.de/y2rw) eine Anleitung, die erklärt, wie man Bluetooth-LE-Verkehr mitschneidet und auswertet. *(mil@ct.de)*

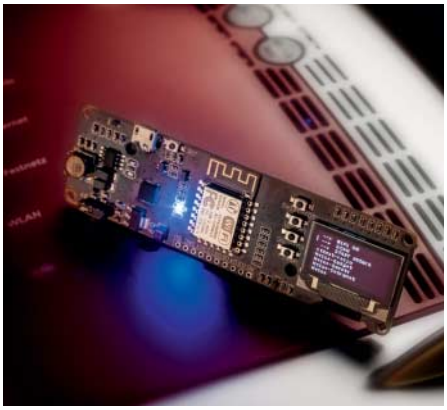
Ubertooth One
Hersteller: Great Scott Gadgets
Preis: 115 US-$
Aufwand:
Gefahr:

WLAN-Ausknipser

WiFi Deauther OLED

Klein und gemein: Der WiFi Deauther packt WLAN-Geräte an ihrer Achillesferse und blockiert effektiv die Verbindung zwischen Router und Clients.

Von Ronald Eikenberg



Obwohl der WiFi Deauther OLED kinderleicht zu bedienen ist, kann er für viel Ärger sorgen: Er stört beliebige WLAN-Netze auf Knopfdruck bis hin zur Unbenutzbarkeit. Das Gerät verschickt sogenannte Deauthentification-Pakete, mit denen sich WLAN-Verbindungspartner gegenseitig anweisen können, die Verbindung zu kappen. Diese Pakete sind selbst bei WPA2-Verbindung nicht geschützt und lassen sich leicht fälschen. Es genügt, öffentlich einsehbare Informationen über das WLAN wie den Netzwerknamen (SSID) sowie die MAC-Adresse des Routers als Absender anzugeben.

Auf Knopfdruck scannt der WiFi Deauther zunächst nach Netzen in Funkreichweite und listet sie auf seinem winzigen, aber knackig scharfen OLED-Display auf. Über die vier Knöpfchen startet der Angreifer anschließend die Attacke. Der Effekt ist erstaunlich: In unserem Labor hat das kleine Gerät mit Start des Angriffs augenblicklich sämtliche Smartphones und Rechner aus dem Netz gekegelt. Bis wir die Attacke manuell stoppten, hatten die Clients keine Chance, die Verbindung wiederherzustellen.

Der Deauther spannt auf Wunsch ein eigenes WLAN auf, über das man sein Webinterface zur Konfiguration erreicht. Das Herzstück des Deauther ist der flexible Mikrocontroller ESP8266, der mit einem WLAN-Modul ausgestattet ist. Dieses ist allerdings auf das 2,4-GHz-Band begrenzt, Geräte im 5-GHz-Band bleiben also verschont. Das Hacking-Gadget wird per Akku oder über Micro-USB mit Strom versorgt. *(rei@ct.de)* c't

WiFi Deauther OLED
Hersteller: DSTIKE
Preis: 25 US-$
Aufwand:
Gefahr: