CanSecWest 2014: UEFI, das neue BIOS

Erbfolge

Joshua Tiago

Gleich mehrere Vorträge der Sicherheitskonferenz CanSecWest, die Mitte März in Vancouver stattfand, beschäftigten sich mit der Frage, ob das neue „Unified Extensible Firmware Interface" weniger angreifbar ist als sein Vorgänger.

Das neue „Unified Extensible Firmware Interface" (UEFI), Nachfolger des BIOS, ist noch immer eine Schnittstelle zwischen Hardware und Betriebssystem. Ein wesentliches Merkmal aktueller UEFI-Versionen ist die Secure-Boot-Funktion. Sie soll verhindern, dass sich Malware im System einnistet und von dort vor dem Starten des Betriebssystems ausgeführt wird. In der Praxis heißt das: Nur das Booten mit signierten Bootloadern ist gestattet.

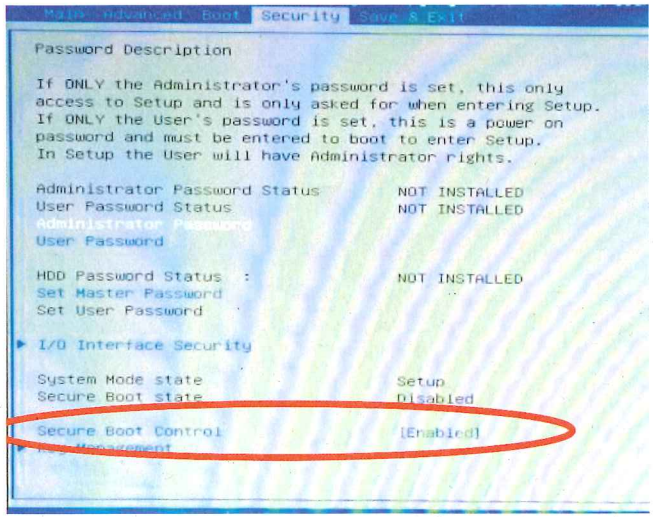
Im Vortrag „All your boot are belong to us" stellten Forscher von Intel Security und MITRE verschiedene Schwachstellen in den Implementierungen aktueller UEFI-Firmware-Versionen vor. Sie ermöglichen einem Angreifer, sicherheitsrelevante UEFI-Funktionen zu deaktivieren oder zu umgehen. Secure Boot lässt sich mittels Enable/Disable Control jederzeit deaktivieren. Zum Verhängnis wird das für UEFI, wenn das zuständige Flag in einem Bereich gespeichert wird, der für Malware aus dem laufenden Betriebssystem heraus beschreibbar ist, etwa Runtime_Access-UEFI-Variablen. Außerdem zeigten die Forscher, dass es möglich ist, die BIOS-Kompatibilitätsschicht (CSM-Modus; Compatibility Support Module) so zu missbrauchen, dass das Gerät trotz aktiviertem Secure Boot im Legacy-Modus startet.

Einen interessanten Ansatz, sich vor manipulierter UEFI- und BIOS-Firmware zu schützen, stellten die Sicherheitsexperten Kovah, Butterworth, Kallenberg und Cornwell von der MITRE Corporation vor. Das als „Copernicus 2" präsentierte Werkzeug ist in der Lage, einen Dump der vorhandenen Firmware mit einer Referenz zu vergleichen. Das Werkzeug schützt sich mit dem TPM (Trusted Platform Module) vor Angriffen, die das Ergebnis verfälschen könnten.

iOS-Kernel: Alles Zufall?

Ein sicherer Zufallszahlengenerator ist für kryptografische Zwecke unerlässlich. iOS verwendet mindestens zwei verschiedene Pseudozufallszahlengeneratoren (PRNG). Im Vortrag „Revisiting iOS Kernel (In)Security: Attacking the Early Random PRNG" stellte Tarjei Mandt das Zusammenspiel der beiden vor. Während des Boot-Vorgangs (iBoot) steht dem Betriebssystem der als „Early Random" bekannte PRNG so lange zur Verfügung, bis der Entropie-Pool des Kernels aktiv ist.

Mandt fand heraus, dass Schwachstellen im Early-Random-PRNG Rückschlüsse auf die nächsten Zufallszahlen erlauben. Da die Ausgabe des Early-Random-PRNG als Eingabe für den sonst sicheren Yarrow-PRNG dient, können diese Schwachstellen im laufenden iOS-Betrieb ausgenutzt werden. Mandt stellte anhand eines iPhone 5 vor, wie man das Zone-Cookies-Konzept, das das Ausführen von Exploits erschweren soll, aushebeln kann.



Auch das Secure-Boot-Feature ist nicht unüberwindbar, wie einige Forscher herausfanden.

Turnschuhe funken

Mit der Einführung der Bluetooth-Spezifikation 4.0 LE (Bluetooth Low Energy) ist ein Weg für Wearable Electronics bereitet. In den letzten Monaten kamen zahlreiche Produkte aus diesem Segment auf den Markt, vornehmlich aus den Bereichen Sport und Fitness, Schmuck, Brillen und Medizintechnik. In der Regel sammeln Sensoren Daten über den Benutzer wie die zurückgelegte Strecke beim letzten Lauftraining. Mittels App lassen sich die Daten dann gebündelt oder in Echtzeit abrufen.

Bei vielen Produkten haben die Verantwortlichen das Thema Sicherheit nicht berücksichtigt, wie Mike Ryan im Vortrag „Outsmarting Bluetooth Smart" darlegte. Mit geeigneten Werkzeugen lassen sich Geräte im Umkreis ermitteln. Ryan demonstrierte, dass sich in einigen Fällen Daten von solchen Geräten ohne Authentifizierung abfragen lassen. Die Vorträge finden sich unter https://cansecwest.com/csw14archive.html (ur)