VON IDG
COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/festplattenverschluesselung-durch-speicherattacke-zu-knacken,1882928

Perfider Angriff

Festplattenverschlüsselung durch Speicherattacke zu knacken

Datum: 30.12.2008
Autor(en): Uli Ries

Entgegen weit verbreiteter Meinung verliert der Hauptspeicher in Servern und Clients seinen Inhalt nicht sofort nach dem Abschalten des Systems. 30 Sekunden und länger bleiben die Speicherinhalte nach Verlust der Energieversorgung intakt, so dass sich beispielsweise Kryptoschlüssel von Webservern oder Festplattenverschlüsselungstools extrahieren lassen.

Speicher im Visier: Der Inhalt von Hauptspeichern lässt sich noch nach dem Herunterfahren des Systems weitgehend intakt auslesen.

Wie der amerikanische IT-Experte Jacob Appelbaum erläutert, verlieren Speichermodule nicht alleine durch das Herunterfahren des Systems ihre Inhalte. Daher lassen sie sich auch später noch auslesen. Untermauert werden diese Aussagen durch ein **Video**[1] einer erfolgreichen Demonstration.

Bei der so genannten Cold Boot Attack lässt der Datendieb das laufende System abstürzen, startet es dann wahlweise per USB neu oder setzt die Speichermodule in einen anderen Rechner ein, um den Inhalt dort zu extrahieren. Perfide: Die Attacke funktioniert auch remote, wenn die Maschine nach dem Absturz per PXE-Boot mit einem bösartigen Boot-Image gestartet wird, das die – im Quellcode erhältliche – **Software**[2] zum Auslesen des Speichers enthält. Der Speicherdump lasse sich laut Appelbaum dann an die Broadcast-Adresse im Intranet schicken. Dies erschwert das Aufdecken des Lauschers immens, da keine Punkt-zu-Punkt-Verbindung zwischen Opfer und Angreifer besteht.

Die Speicherattacke funktioniert, da DRAM seinen Inhalt auch ohne Energieversorgung noch einige Zeit weitgehend intakt hält. So lassen sich laut Appelbaum schon bei Raumtemperatur Spannen von bis zu 30 Sekunden überbrücken. Selbst nach dem Ausbau der Module aus dem Mainboard sind die Zellen noch gefüllt. Greift ein Angreifer vor dem Auslesen zu einem Kältespray, mit dem er die Module herunter kühlt, sind noch wesentlich längere Zeitspannen möglich.

Interessant wird eine solche Attacke aus Sicht des Angreifers bei Maschinen, deren Festplatte verschlüsselt ist. Ins Visier könnten auch Web-Server geraten, die mit RSA-Keys hantiere. In beiden Szenarien legt das Betriebssystem beziehungsweise die jeweilige Anwendung meist unverschlüsselt im Hauptspeicher ab. Appelbaum gibt an, dass sich gängigen HDD-Verschlüsselungsprogramme wie Microsofts **Bit Locker**[3], **dm-crypt**[4] (Linux), **File Vault**[5] (Mac OS X) oder auch die weit verbreitete Open-Source-Lösung **TrueCrypt**[6] aushebeln lassen. Eine speziell zu diesem Zweck programmierte Software kann die Keys selbst dann anhand spezieller Muster aus im Speicherextrakt finden und rekonstruieren, wenn 70 Prozent der Inhalte nur verloren gingen.

Links im Artikel:

[1] **http://citp.princeton.edu/memory/**
[2] **http://citp.princeton.edu/memory/code**
[3] **http://technet.microsoft.com/de-de/windows/aa905065.aspx**
[4] **http://www.saout.de/misc/dm-crypt/**
[5] **http://docs.info.apple.com/article.html?path=Mac/10.4/de/mh1877.html**
[6] **http://www.truecrypt.org/**
