Cold Boot Attacks on Encryption Keys

Es geht doch nichts über den physischen Zugriff auf einen Rechner, wenn man an die Daten herankommen will. Das Center for Information Technology Policy der Universität von Princeton hat jetzt bewiesen, dass die meisten Verschlüsselungssysteme, unter anderem auch Truecrypt, unter bestimmten Bedingungen unsicher sind: „Contrary to popular assumption, DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard. Although DRAMs become less reliable when they are not refreshed, they are not immediately erased, and their contents persist sufficiently for malicious (or forensic) acquisition of usable full-system memory images.“

Die *Technology Review* hat ein ausführliches Interview dazu mit Edward W. Felten im Angebot – Felten ist Professor für Informatik an der Princeton University und hat die ausführliche Studie verfasst.

Worum geht es? Die DRAM-Speicherchips (für: Dynamic Random Access Memory) erinnern sich an bestimmte Daten, auch wenn der Rechner schon abgeschaltet wurde. Das kann man wieder sichtbar machen – also auch bestimmte Passworte und Schlüssel, die der Chip temporär speichert. Ein Angreifer msus also, soll die vorgeschlagene Methode funktionieren, den Rechner aus- und zeitnah wieder anschalten. Als Pointe haben die Forscher die Chips sogar mit Stickstoff abgekühlt. Dann dauert es noch länger, bis alle Daten nach dem Ausschalten des Computers verschwunden sind.

> *TR: Kann Ihre Methode tatsächlich jedes Festplattenverschlüsselungssystem knacken, das heute auf dem Markt ist?*
> *Felten: Alle, die wir getestet haben, darunter Microsoft BitLocker, Apple FileVault, dm-crypt unter Linux und TrueCrypt. Microsofts System ist in bestimmten Konfigurationen etwas sicherer, aber es sieht wohl so aus, als seien die meisten oder gar alle verfügbaren Festplatten-Verschlüsseler mit großer Wahrscheinlichkeit angreifbar.*

Fazit: Man muss zum Beispiel einen Laptop immer ausschalten,

der „Hibernations“- oder Stand-by-Modus nutzt überhaupt nichts, auch wenn die Festplatte verschlüsselt ist.

> *TR: Der physische Zugriff auf eine Maschine bleibt also immer ein Risiko.*
> *Felten: Ja. Zuvor dachte man aber eben, dass eine Festplattenverschlüsselung die Dateien auf einem Laptop schützt, selbst wenn dieser verloren oder gestohlen wurde. Unsere Ergebnisse zeigen nun, dass das nicht stimmt.*