FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Cold Boot Attacks auf RAM Bausteine

Simon Lindenlauf

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Agenda

- Hintergrundinformationen
- Was sind Cold Boot Attacken?
- Auslese Möglichkeiten
- Aufgabenstellung
- Umsetzung

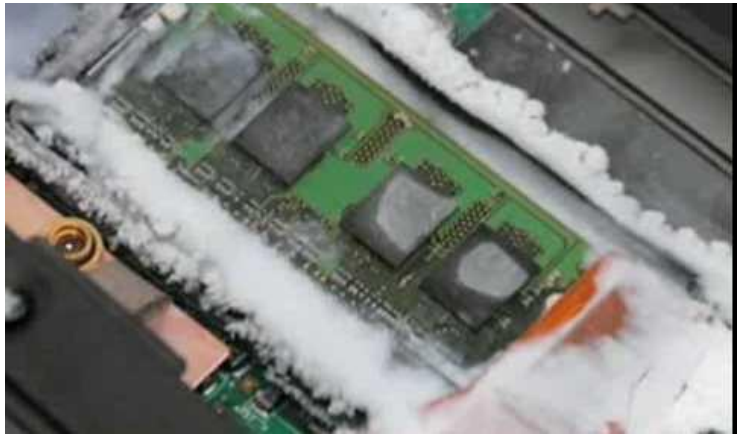
Hintergrundinformationen

- Daten im Arbeitsspeicher sind unverschlüsselt
- Festplattenverschlüsselungs-Key liegt in RAM
  - Bei Software Verschlüsselung
- RAM auslesbar bei physischen Zugriff auf PC
  - Auch wenn PC gesperrt ist

- RAM verliert Inhalt nicht direkt nach Ausschalten

Cold Boot Attacke

- RAM kann Daten einige Sekunden ohne Strom behalten
  - Durch runterkühlen Verlängert sich Zeitraum



- PC wird ausgeschaltet
  - Schnellstmöglich wieder mit Strom versorgt
  - Auslesesoftware wird gestartet
  - RAM Image wird erzeugt

Auslese Möglichkeiten

- Am untersuchten PC auslesen
  - PC wird (kalt) neugestartet
  - Probleme:
    - BIOS Passwort
    - Power-on self-test (RAM wird gelöscht)

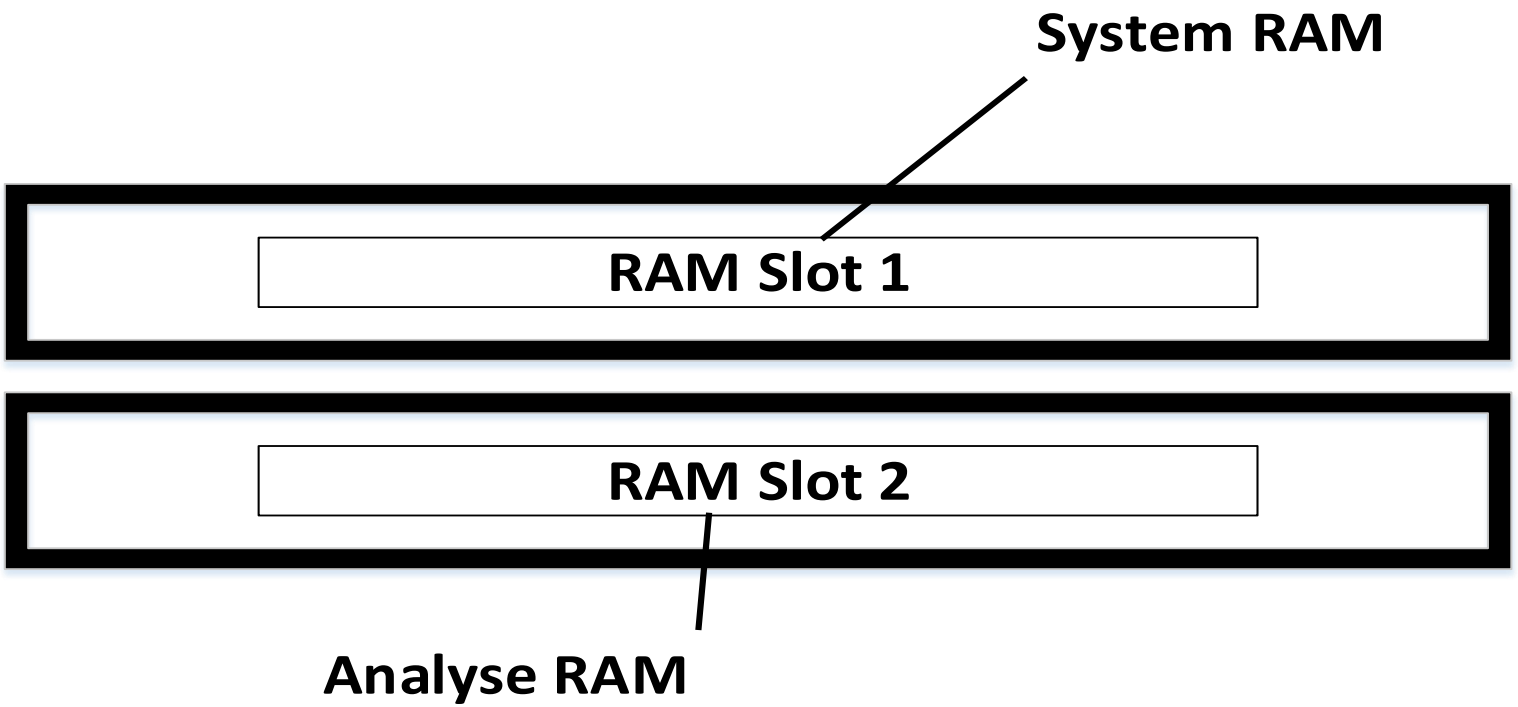
- Am Analysecomputer auslesen
  - RAM wird aus dem zu analysierenden Rechner entfernt
  - Schnellstmöglich in Analyserechner gesteckt
  - Analyserechner mit Auslesesoftware gebootet

Aufgabenstellung

- RAM auslesen (möglichst) ohne Veränderung der Daten
- Tests wie lange Daten erhalten bleiben
  - Temperatur
  - Verwendete Technik
- Analyse des RAM Image
  - VOLIX II

Umsetzung

- Analyserechner zum RAM auslesen
  - Cold Boot Gegenmaßnahmen umgehen



Ende