FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

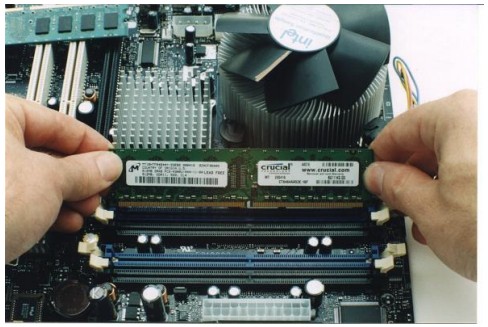
Cold Boot Attacken auf DDR2 und DDR3

Simon Lindenlauf

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

RAM ist (langsam) flüchtig


http://www.ifitjams.com/ibuild3.htm

- Hauptspeicher DDR DRAM
  - DDR1, DDR2, DDR3, DDR4
- Speicher verliert Daten wenn nicht mit Strom versorgt
- Temperaturabhängiger Refresh notwendig
  - bis zu 85°C: alle 64 ms (standard refresh time)
  - zwischen 85°C und 95°C: 32 ms
  - je höher Temperatur, je schneller Verlust (und umgekehrt)

Was ist ein Cold Boot Angriff?

- Grundidee
  - DRAM Speicherinhalt kann ausgelesen werden nachdem Maschine vom Strom getrennt wurde
  - niedrige Temperaturen verbessern den Effekt
- Zwei Möglichkeiten… Speicher auslesen auf
  - Originalmaschine
    - DRAM bleibt im Board
    - Originalmaschine wird kalt gestartet
  - oder auf einer zweiten Maschine
    - DRAM wird entfernt und in zweiter Maschine eingebaut
    - zweite Maschine wird kalt gestartet

Warum das Ganze?

- Hauptzweck: Schlüssel von verschlüsselten Festplatten wiederherstellen
  - Festplattenverschlüsselungs-Key liegt in RAM
  - Daten im Arbeitsspeicher sind unverschlüsselt

- Cold Boot Angriff kann helfen
  - man erhält RAM Image
  - mag teilweise fehlerhaft sein… trotzdem Methoden, Schlüssel zu rekonstruieren

Ablauf

- Cold Boot Angriff
  1. Auslese-USB-Stick mit Cold Boot PC verbinden
  2. Kühle DRAM auf laufender Originalmaschine
  3. Originalmaschine ausschalten oder DRAM umstecken
  4. Von USB-Stick booten
  5. Program auf USB-Stick liest und speichert RAM Image
  6. RAM Image kann offline analysiert werden

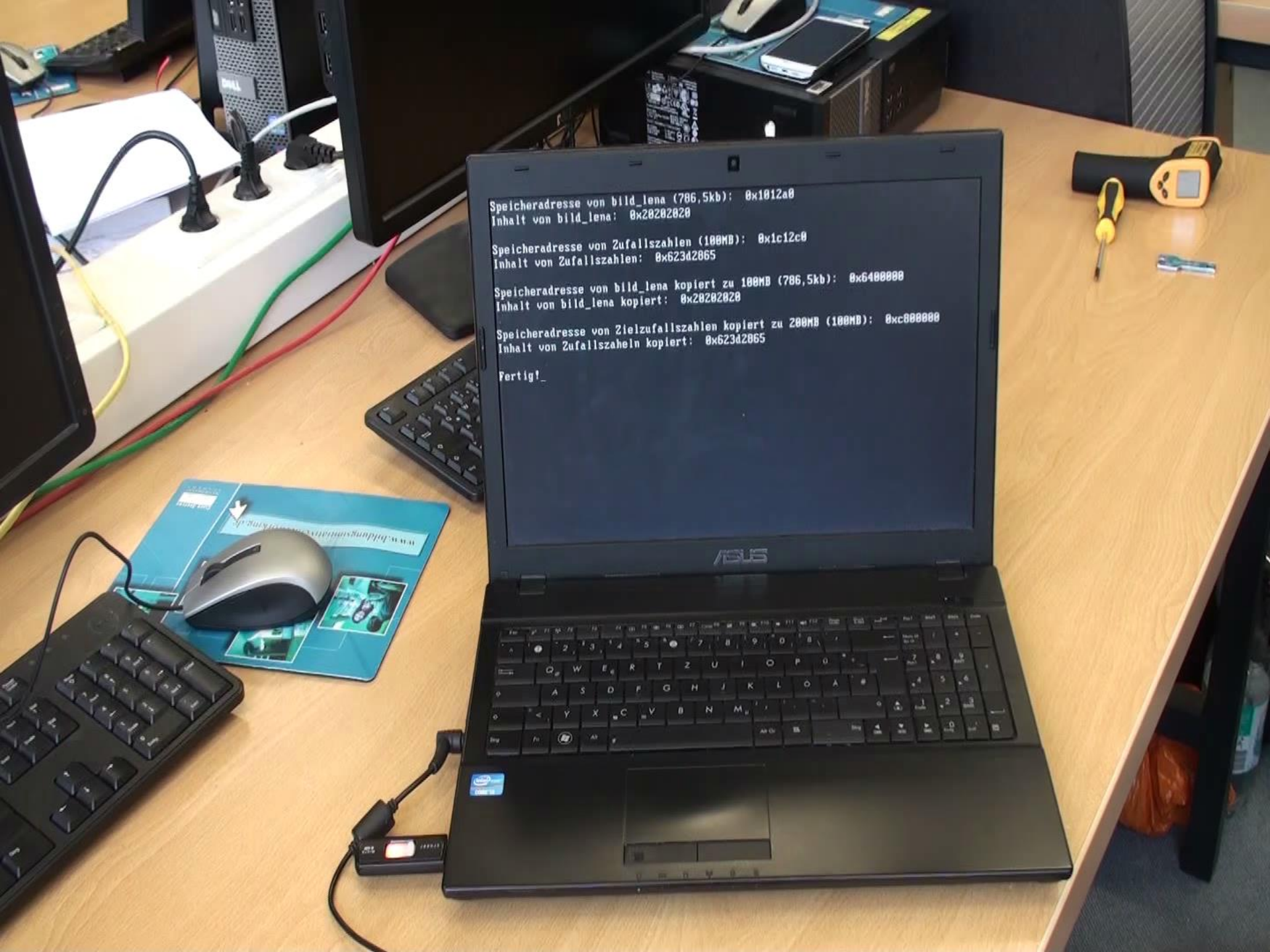
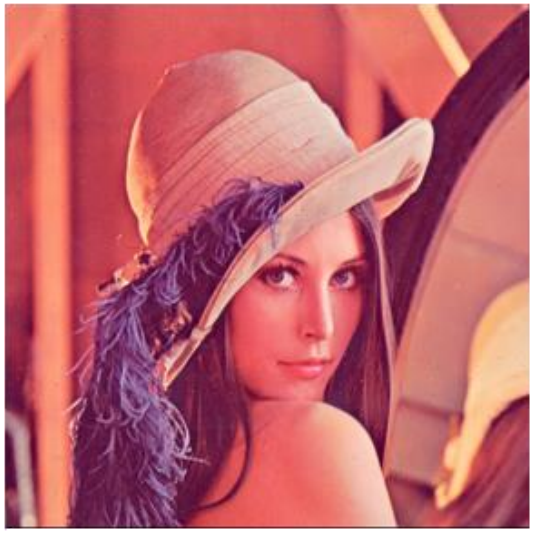

Speicheradresse von bild_lena (786,5kb): 0x1012a0
Inhalt von bild_lena: 0x20202020
Speicheradresse von Zufallszahlen (100MB): 0x1c12c0
Inhalt von Zufallszahlen: 0x623d2065
Speicheradresse von bild_lena kopiert zu 100MB (786,5kb): 0x6400000
Inhalt von bild_lena kopiert: 0x20202020
Speicheradresse von Zielzufallszahlen kopiert zu 200MB (100MB): 0xc800000
Inhalt von Zufallszaheln kopiert: 0x623d2065
Fertig!_
ASUS

Bild aus RAM Image nach Cold Boot



(a) -35°C and 0,041% Byte Error Rate

(b) -5°C and 0,273% Byte Error Rate

(c) +15°C and 1,756% Byte Error Rate

(d) +30°C and 34,284% Byte Error Rate

Ergebnisse DDR2 SDRAM

- 10s ohne Strom bei -35°C bis -30°C

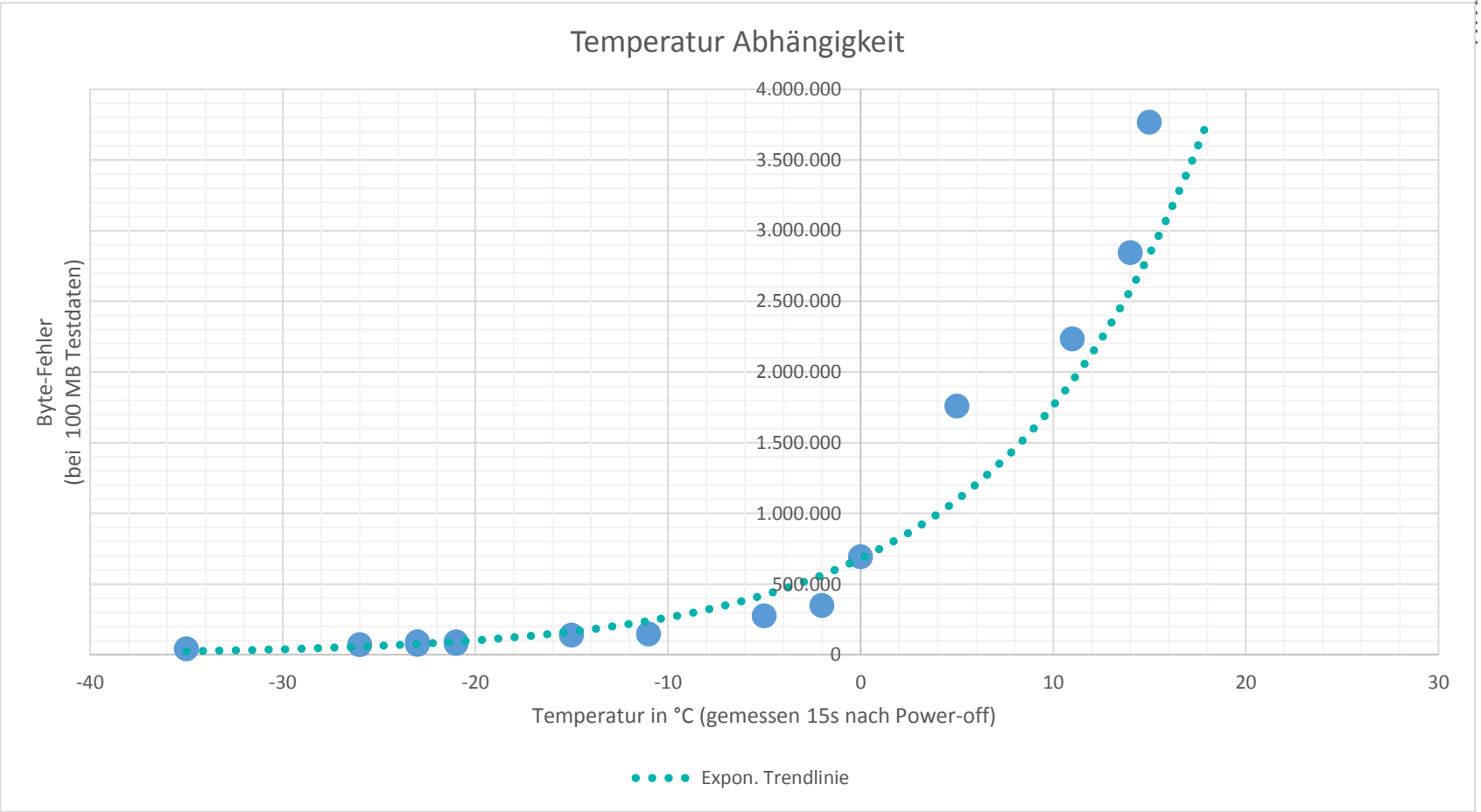
DDR2	RAM	Byte Errors	Bit Errors	Byte Error Rate	Bit Error Rate
1	B	236	236	0,000236%	0,000030%
2	F	2.204	2.212	0,002204%	0,000277%
3	G	3.675	3.943	0,003675%	0,000493%
4	C	82.539	85.766	0,0825%	0,0107%
5	H	239.263	558.522	0,239%	0,070%
6	D	729.380	795.702	0,729%	0,099%
7	J	2.248.293	2.477.976	2,248%	0,310%
8	I	4.763.617	7.862.582	4,764%	0,983%
9	A	12.870.663	28.379.907	12,87%	3,55%
10	E	20.997.916	71.909.648	21,00%	8,99%
11	K	35.475.736	88.992.338	35,48%	11,12%

Ergebnisse DDR3 SDRAM

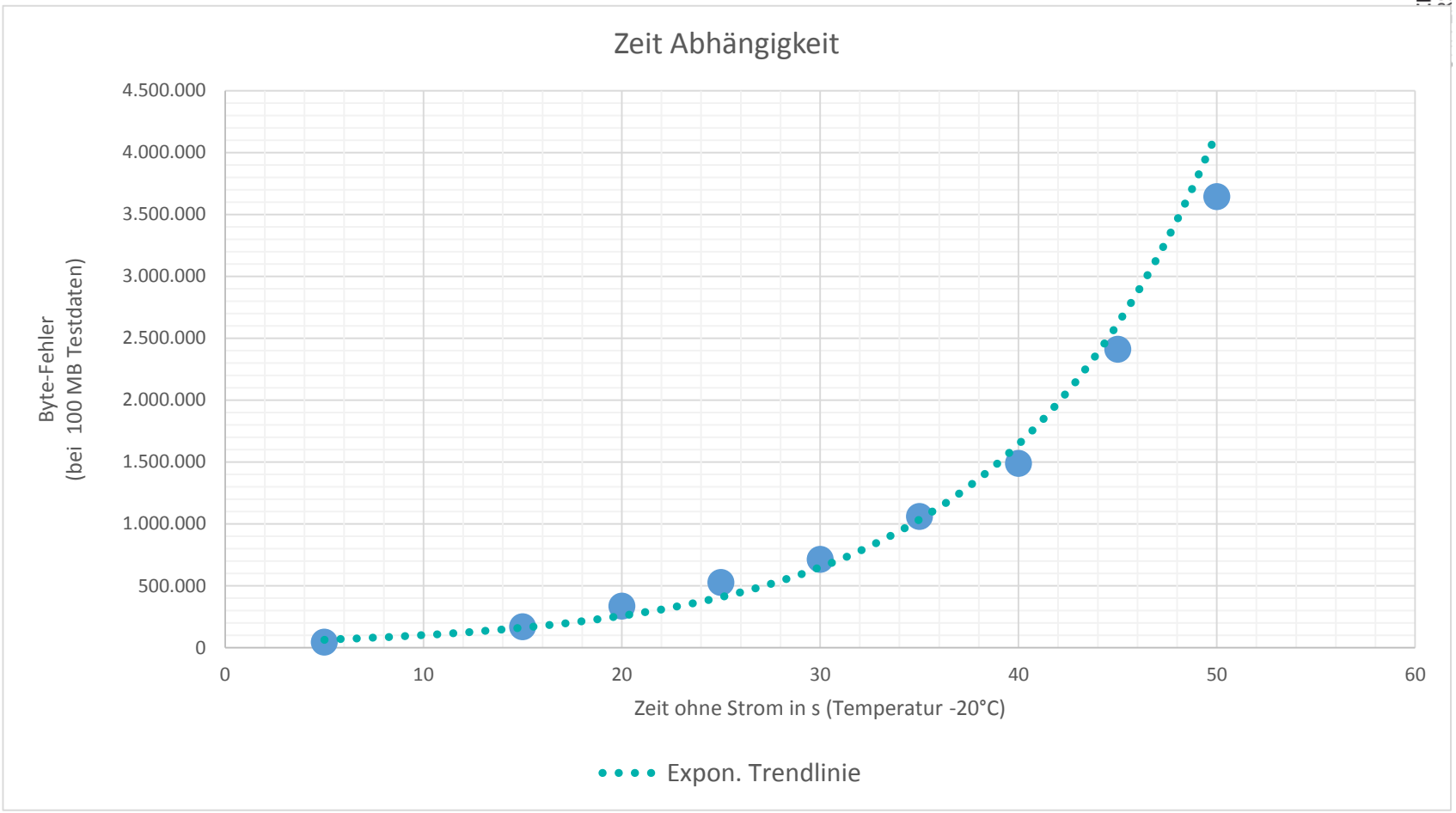
- 10s ohne Strom bei -35°C bis -30°C

DDR3	RAM	Byte Errors	Bit Errors	Byte Error Rate	Bit Error Rate
1	N	1.604	5.624	0,001604%	0,000703%
2	M	4.435	8.275	0,004435%	0,001034%
3	L	460.860	534.566	0,461%	0,067%

Fehler – abhängig von Temperatur



Fehler – abhängig von Zeit ohne Strom



Ende