DRAMA: Exploiting DRAM Buffers for Fun and Profit

Michael Schwarz

07.06.2018

www.iaik.tugraz.at

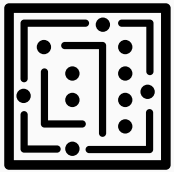
Seitenkanäle

- Seitenkanäle sind Seiteneffekt, die Informationen liefern
- Bekannt aus der echten Welt
  - Lügendetektor (Mimik, Gestik, Puls)
  - Tresor (Klickgeräusche)
  - Türschloss (Widerstand)
- Sind oft auch in fehlerfreien Systemen vorhanden

Seitenkanäle in Software

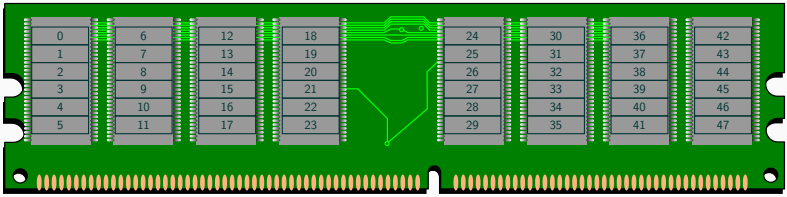
- Seitenkanäle gibt es auch in Software
- Können auch für Attacken ausgenutzt werden
- Statt Geräusche misst man meistens Zeitunterschiede
- Zeitunterschiede durch die Mikroarchitektur gegeben

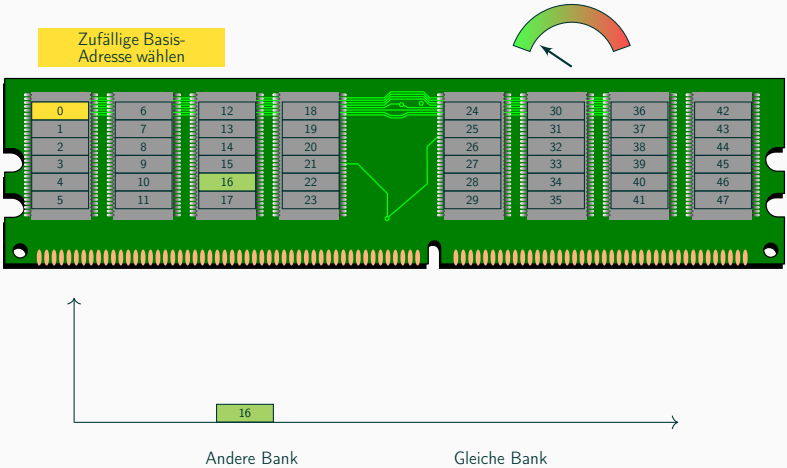
Mikroarchitektur



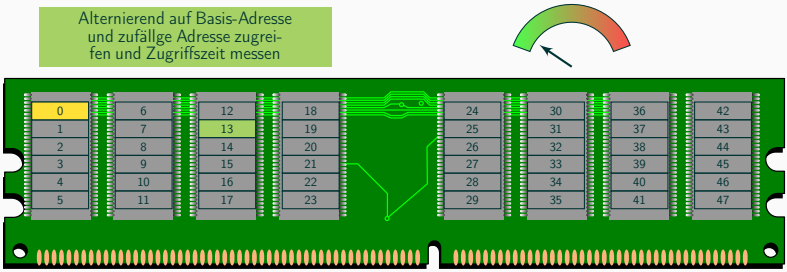
- Mikroarchitektur beschreibt die interne Art wie CPUs arbeiten
- Nicht sichtbar für Benutzer oder Programmierer
- Ist großteils nicht dokumentiert und kann nicht direkt beobachtet werden
- In dieser Arbeit: Arbeitsspeicher (DRAM)

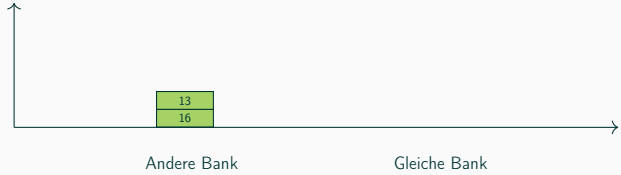
Reverse Engineering von DRAM



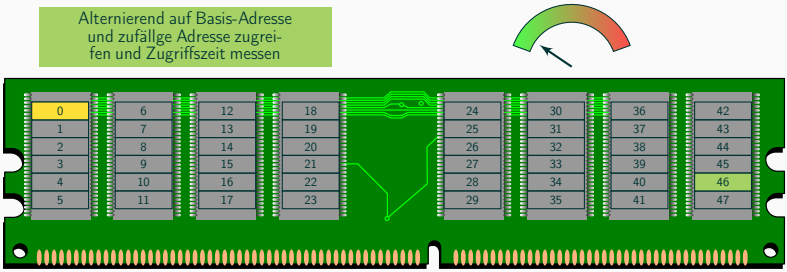

Zufällige Basis-Adresse wählen
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
16
Andere Bank
Gleiche Bank

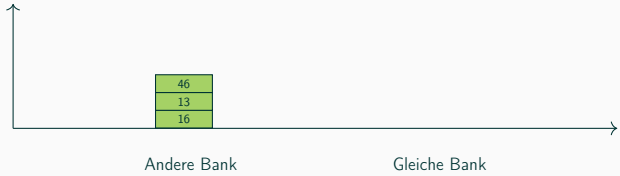
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen



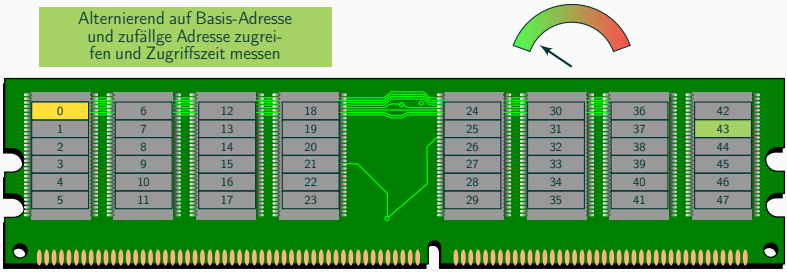


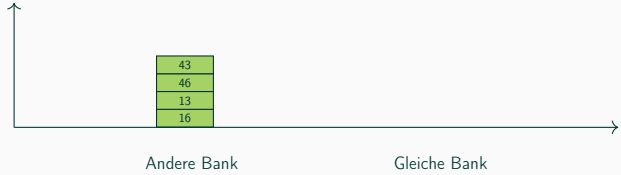
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen



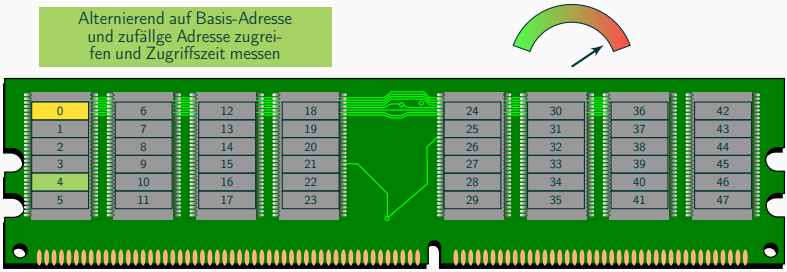


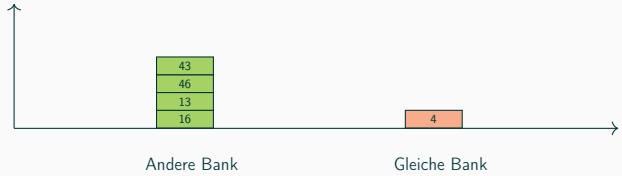
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen



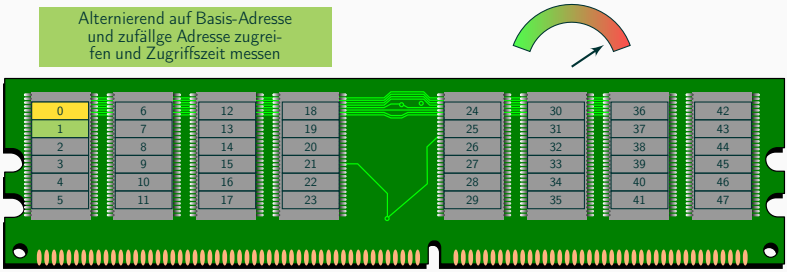


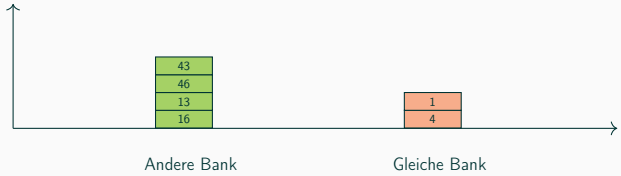
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen



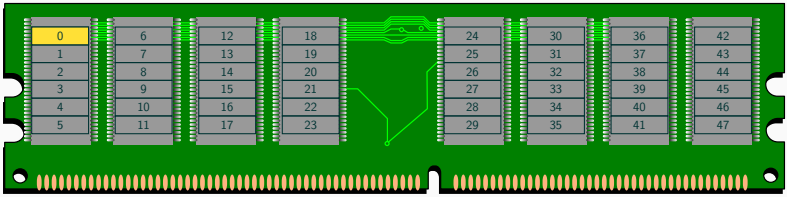


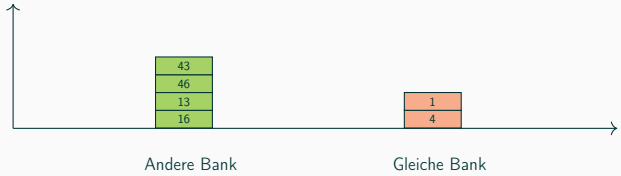
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen

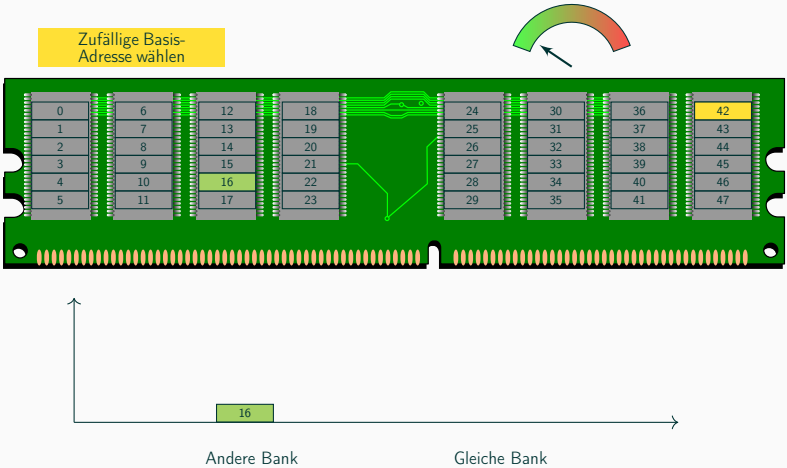




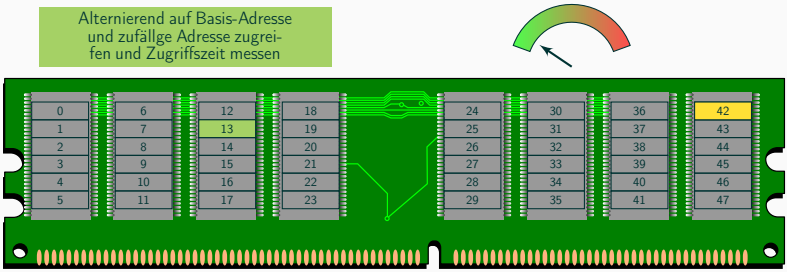
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen

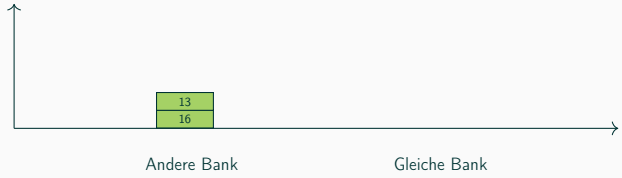




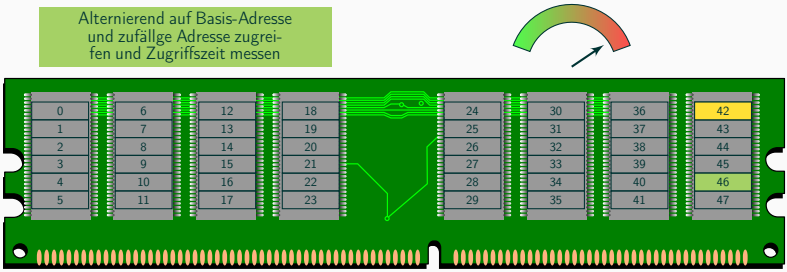

Zufällige Basis-
Adresse wählen
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
16
Andere Bank
Gleiche Bank

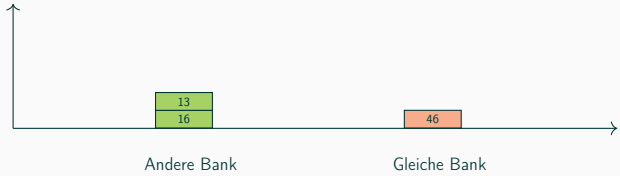
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen

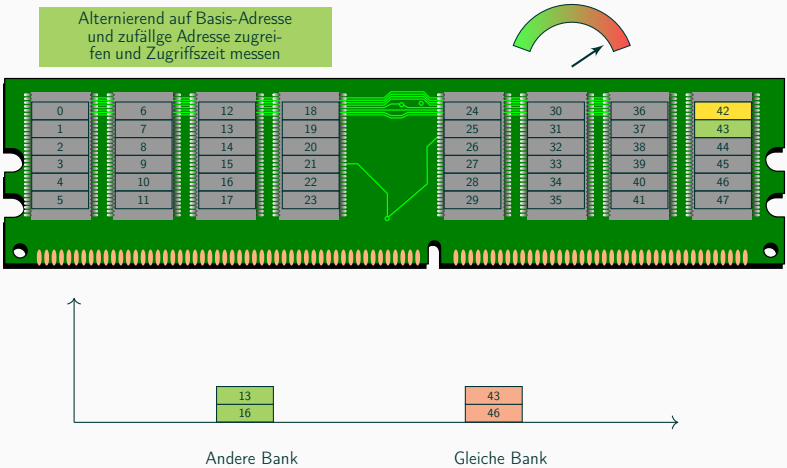




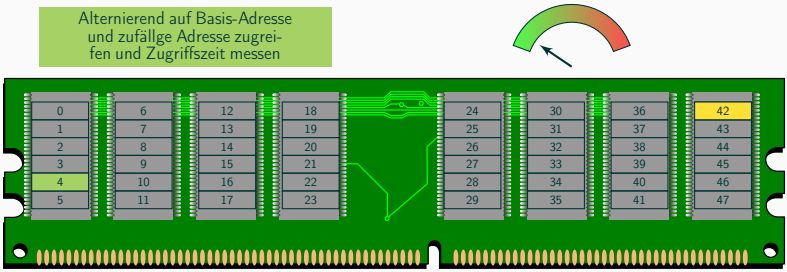
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen

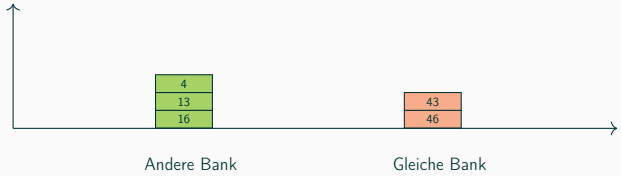




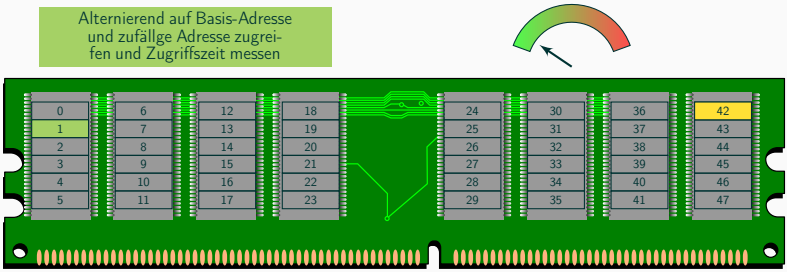

Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
13
16
43
46
Andere Bank
Gleiche Bank

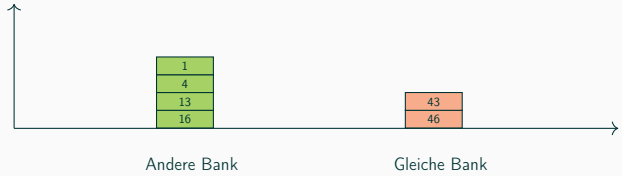
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen





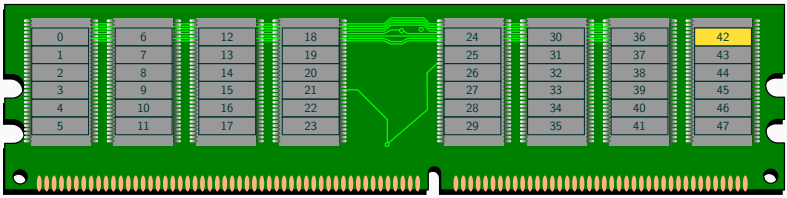
Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen

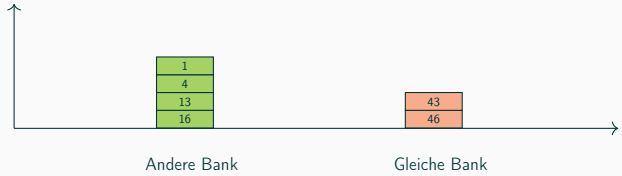




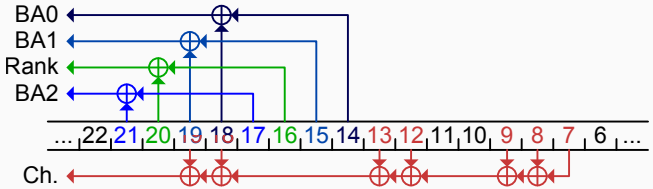
Reverse Engineering von DRAM

Alternierend auf Basis-Adresse und zufällge Adresse zugreifen und Zugriffszeit messen



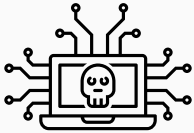


Ergebnis

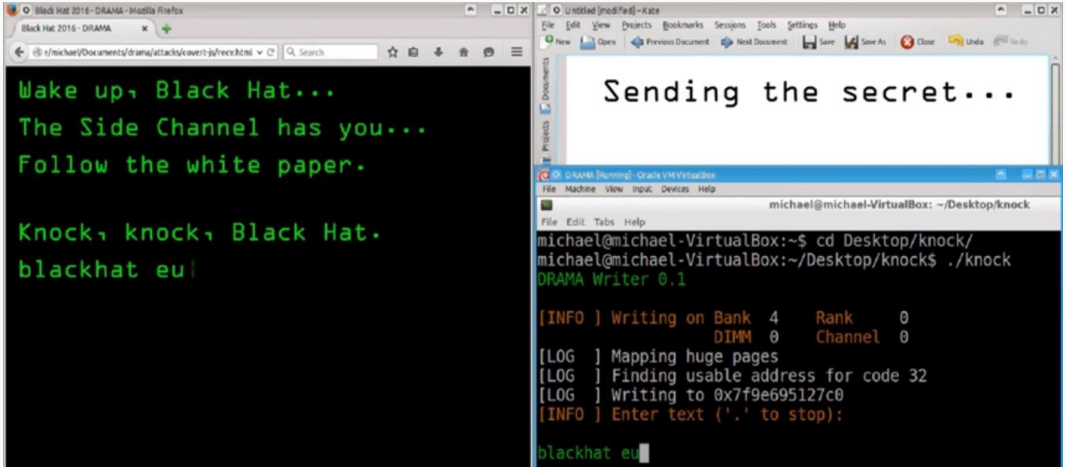


- Gleichungssystem lösen liefert eine Funktion
- Unterschiedlich für verschiedene Systeme
- Ansatz ist vollständig automatisiert

Angriffe

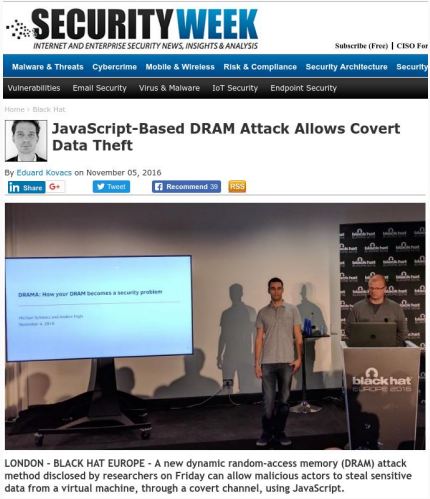


- Zeitunterschiede erlauben indirekt Aktivität zu beobachten
- Benutzereingaben können ausspioniert werden
- Daten können exfiltriert werden
- Grundlage für effiziente Rowhammer Angriffe


Black Hat 2016 - DRAMA - Mozilla Firefox
Black Hat 2016 - DRAMA
Wake up, Black Hat...
The Side Channel has you...
Follow the white paper.
Knock, knock, Black Hat.
blackhat eu
Sending the secret...
michael@michael-VirtualBox: ~/Desktop/knock
michael@michael-VirtualBox:~$ cd Desktop/knock/
michael@michael-VirtualBox:~/Desktop/knock$ ./knock
DRAMA Writer 0.1
[INFO] Writing on Bank 4 Rank 0
DIMM 0 Channel 0
[LOG] Mapping huge pages
[LOG] Finding usable address for code 32
[LOG] Writing to 0x7f9e695127c0
[INFO] Enter text ('.' to stop):
blackhat eu

Reaktionen

- Ergebnisse bei BlackHat Europe 2016 präsentiert
- Co-Autor bei einer Top Security Konferenz (USENIX Security 2016)
- Weitere Publikationen in meinem PhD: Mozilla und Google entwickeln Gegenmaßnahmen
- Bereits 4 neue Angriffe die diese Techniken verwenden



Sichtbarkeit

- Seitenkanal Angriffe erlebten Aufschwung durch Meltdown und Spectre
- Erfahrung aus dieser Arbeit half Meltdown zu entdecken
- Wir zeigten mit Meltdown den einfachsten und mächtigsten Angriff
- Gegenmaßnahmen wurden wichtig

Reaktionen

Mozilla Security Blog

JAN 3 2018

Mitigations landing for new class of timing attack

> Initially, we are removing support for SharedArrayBuffer from Microsoft Edge (originally introduced in the Windows 10 Fall Creators Update), and reducing the resolution of performance.now() in Microsoft Edge and Internet Explorer from 5 microseconds to 20 microseconds, with variable jitter of up to an additional 20 microseconds. These two changes substantially increase the difficulty of successfully inferring the content of the CPU cache from a browser process.

Protecting users with Site Isolation

Chrome has been working on a feature called Site Isolation which provides extensive mitigation against exploitation of these types of vulnerabilities. With Site Isolation enabled, the amount of data exposed to side-channel attacks is reduced as Chrome renders content for each website in a separate process. This allows websites to be protected from each other by the security guarantees provided by the operating system on which Chrome is running.

News Byte

February 14, 2018

Share this Article

EXPANDING INTEL'S BUG BOUNTY PROGRAM: NEW SIDE CHANNEL PROGRAM, INCREASED AWARDS

- Offering a new program focused specifically on side channel vulnerabilities through Dec. 31, 2018. The award for disclosures under this program is up to $250,000.

Fazit

- Seitenkanal-Angriffe wurden zu lange unterschätzt
  - Grundlegende Konzepte gibt es schon lange
- Es wird zu wenig Wert auf Sicherheit gelegt
  - Wir brauchen mehr Fokus auf Sicherheit
  - Performance darf nicht mehr das einzige Kriterium bei Prozessoren sein
- Mehr Forschung ist notwendig um Probleme endgültig zu beheben