On the Applicability of Time-Driven Cache Attacks on Mobile Devices

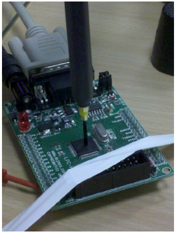
Raphael Spreitzer and Thomas Plos

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

raphael.spreitzer@iaik.tugraz.at

Motivation

- Related work
  - Bogdanov *et al.* [BEPW10]
  - Gallais and Kizhvatov [GK11]
  - Weiß *et al.* [WHS12]:
    "…further research has to examine
    …real noise"
- Our goal
  - More realistic environments
  - State-of-the-art Android-based devices
    - Acer Iconia A510
    - Samsung Galaxy S3
    - Google Nexus S



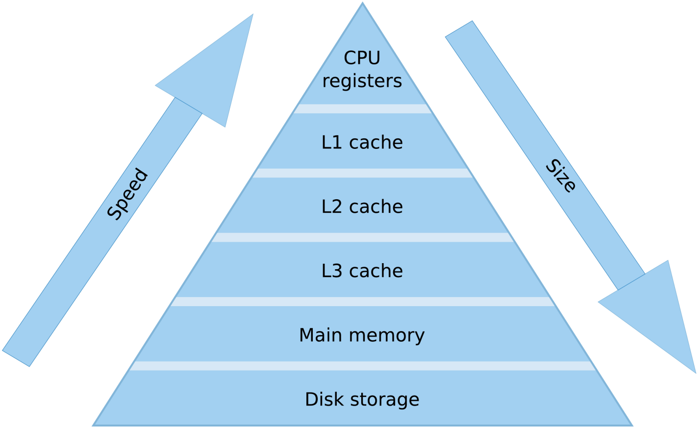
(src: [GK11])

(src: [Chi12])

Advanced Encryption Standard (AES)

- Block cipher operating on 128-bit states
- 4 round transformations
- Software implementations employ T-tables
  - T-tables consist of 256 4-byte elements
  - Look-up operation $\mathbf{T}[\mathbf{s}_i]$

Memory Hierarchy



Cache Attacks

- Side-channel attacks
  - Insecure implementations of secure algorithms
  - Execution time, power consumption, etc.
- Cache attacks on the AES
  - Timing variations due to the memory hierarchy
  - Look-up operations are key dependent $\mathbf{T}[\mathbf{p}_i \oplus \mathbf{k}_i]$

Timing Attack by Bernstein [Ber05]

- Encrypt **P** under a known key **K**
- Encrypt $\widetilde{\mathbf{P}}$ under an unknown key $\widetilde{\mathbf{K}}$
- Similar timing profile if pairs satisfy

$$\widetilde{\mathbf{p}}_i \oplus \widetilde{\mathbf{k}}_i = \mathbf{p}_i \oplus \mathbf{k}_i$$
$$\widetilde{\mathbf{k}}_i = \mathbf{p}_i \oplus \mathbf{k}_i \oplus \widetilde{\mathbf{p}}_i$$

- Exhaustive key search

Practical Results - Bernstein's Attack (1/2)

Sample output of Bernstein's attack on the Samsung Galaxy S3

# of key candidates	Key byte	Possible values									
3	0	**b5**	b4	b8							
125	1	00	a2	be	c2	b8	1d	f6	...	**93**	...
165	2	87	03	51	17	1b	1f	c7	...	**11**	...
2	3	**66**	67								
104	4	59	1d	10	a5	34	06	50	...	**af**	...
6	5	**bc**	bd	b9	b8	ba	bb				
8	6	cc	**cd**	ca	cf	cb	c8	ce	c9		
2	7	**8d**	8c								
115	8	1e	ea	c9	ee	e6	11	**12**	cc	02	...
2	9	b8	**b9**								
153	10	76	7d	56	b3	5b	4b	3c	...	**55**	...
2	11	**12**	13								
23	12	83	9f	82	96	94	97	**92**	9d	98	...
2	13	**4a**	4b								
40	14	6a	7a	7b	74	61	7c	64	**6b**	78	...
2	15	9c	**9d**								

- Exhaustive key search $\sim 2^{58}$

Practical Results - Bernstein's Attack (2/2)

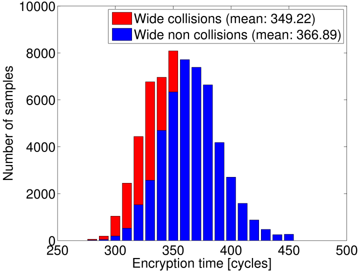
- Timing information leaks
- Reduced key space from 128 bits to 58–73 bits
- Too large for exhaustive key search

Collision Attack by Bogdanov et al. [BEPW10]

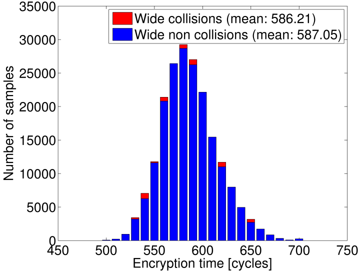
- Empty cache
- Encryption of chosen $\mathbf{P}_1$ ($\mathbf{s}_i = \mathbf{p}_i \oplus \mathbf{k}_i$)
- Encryption of chosen $\mathbf{P}_2$ ($\mathbf{s}_i = \mathbf{p}_i \oplus \mathbf{k}_i$)
- Encryption time indicates whether a collision occurred
- Infer relations between key bytes

Practical Results - Bogdanov et al.'s Attack (1/2)

- Histogram of encryption times for the ARM Cortex-A8



Histogram for a 3-round AES



Histogram for a 7-round AES

Practical Results - Bogdanov et al.'s Attack (2/2)

- Collisions are hard to detect (cache-line size)
- Reduced key space from 128 bits to 52 bits
- Too large for exhaustive key search

Conclusion and Future Work

- Conclusion
  - Cache attacks are applicable in real-world environments
  - Remaining key space too large
  - Though, we consider time-driven cache attacks a real threat
- Future work
  - Reduce the key space even further
  - Countermeasures
- **Cache attacks threaten the user's privacy and security**

On the Applicability of Time-Driven Cache Attacks on Mobile Devices

Raphael Spreitzer and Thomas Plos

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

raphael.spreitzer@iaik.tugraz.at

Bibliography

[BEPW10] Andrey Bogdanov, Thomas Eisenbarth, Christof Paar, and Malte Wienecke.
Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs.
In *CT-RSA*, pages 235–251, 2010.

[Ber05] Daniel J. Bernstein.
Cache-timing attacks on AES.
Available online at `http://cr.yp.to/antiforgery/cachetiming-20050414.pdf`, 2005.

[Chi12] Chip.de.
Das beste Android-Tablet.
Available online at
`http://www.chip.de/artikel/Acer-Iconia_Tab_A510-Tablet-PC-Test_56138304.html`, 2012.

[GK11] Jean-François Gallais and Ilya Kizhvatov.
Error-Tolerance in Trace-Driven Cache Collision Attacks.
In *COSADE*, pages 222–232, Darmstadt, 2011.

[WHS12] Michael Weiß, Benedikt Heinz, and Frederic Stumpf.
A Cache Timing Attack on AES in Virtualization Environments.
In *FC*, pages 314–328. Springer Berlin Heidelberg, 2012.