Side-Channel Cryptanalysis

Lecture notes and suggested reading

Joseph Bonneau
Research Students' Lectures
University of Cambridge Computer Laboratory

May 4, 2010

Most cryptosystems are designed and evaluated at a mathematical level. Attackers, however, will always target the physical realisation of a system which is much more complicated (see [14] for discussion of this disconnect). Real-world electronic implementations of ciphers will usually leak additional information to attackers in the form of *side-channels* such as timing, power consumption, electromagnetic radiation, heat, noise, and more. In many cases, an attacker can combine side-channel information with the observed input and/or output of a cryptographic algorithm to recover secret information.

It is important to draw a distinction between side-channel cryptanalysis and related physical attacks. *Compromising Emanation attacks* or *tempest attacks* utilise electromagnetic emanations from computers to recover secret data, for example using electromagnetic radiation from a computer screen to recover the text being displayed [11] (for a survey, see chapter 17 of [1]). Tempest attacks target secret information directly, completely bypassing the cryptographic keys. *Invasive* or *semi-invasive* attacks, in contrast, involve physical manipulation of a target system to extract secret information, for example by unpackaging a chip and reading secret data stored in its memory using a micro-probe or a microscope (see [4, 2] for a survey of physical attacks and defences).

In contrast, side-channel attack present a unique challenge in that an attacker gains some additional information which the cryptographic designers did not anticipate, but is usually only weakly correlated to secret data. Recovering the secret data thus requires a combination of side-channel data collection, statistical processing to eliminate noise, and cryptanalysis to deduce secret keys. Side-channel attacks can be very powerful, however, in that they can completely compromise real systems without physical access. This presentation will overview the wide variety of side channel attacks in the existing literature and discuss the details of several specific attacks as case studies:

- **Branch Timing Attacks**– A cryptographic algorithm's running time can be data-dependent if it branches based on the value of secret data. This is characteristic of many public key algorithms such as RSA and discrete-log based systems (in either $\mathbb{Z}_q$ or elliptic-curve groups) which involve complex number-theoretic calculations. We will describe the original RSA timing attacks introduced by Kocher in 1996 [9] and the 2003 implementation of Brumley and Boneh which successfully used them to extract an SSL server's private key over a campus-wide network [6].

- **Power Analysis**– Many devices, such as smart-cards widely deployed in payment systems, expose their power connection to attackers which may be in possession of the device. Kocher introduced power analysis attacks in 1998 which use power consumption traces to extract secret keys [10], these attacks have since spawned an entire sub-field of cryptanalytic research [12]. We will describe Kochers's "simple" power analysis attack against RSA, as well as more powerful differential power analysis attacks against the Data Encryption Standard (DES).

- **Cache Timing Attacks**– Symmetric-key algorithms such as the Advanced Encryption Standard (AES) typically contain no conditional statements and thus were originally thought to be invulnerable to timing attacks. However, the cache architecture of modern processors introduces data-dependent timing characteristics, as certain data-access patterns will be more cache-efficient than others. These small effects were surprisingly used in 2006 to break AES given accurate timing samples. We will describe Bonneau and Mironov's collision-based timing attack against AES [5], as well as the access-based timing attack of Tromer et. al [15].

References

[1] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*, chapter 17. Wiley, second edition, 2008.

[2] Ross Anderson, Mike Bond, Jolyon Cluloq, and Sergei Skorobogatov. Cryptographic processors – a survey. Technical Report UCAM-CL-TR-641, University of Cambridge, 2005.

[3] Ross Anderson and Markus Kuhn. Tamper resistance: a cautionary note. In *WOEC'96: Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce*, pages 1–1, Berkeley, CA, USA, 1996. USENIX Association.

[4] Ross J. Anderson and Markus Kuhn. Low Cost Attacks on Tamper Resistant Devices. In *Proceedings of the 5th International Workshop on Security Protocols*, pages 125–136, London, UK, 1998. Springer-Verlag.

[5] Joseph Bonneau and Ilya Mironov. Cache-Collision Timing Attacks Against AES. *Cryptographic Hardware and Embedded Systems - CHES 2006*, 4249:201–215, October 2006.

[6] David Brumley and Dan Boneh. Remote timing attacks are practical. In *SSYM'03: Proceedings of the 12th conference on USENIX Security Symposium*, pages 1–1, Berkeley, CA, USA, 2003. USENIX Association.

[7] Scott A. Crosby, Dan S. Wallach, and Rudolf H. Riedi. Opportunities and Limits of Remote Timing Attacks. *ACM Trans. Inf. Syst. Secur.*, 12(3):1–29, 2009.

[8] Saar Drimer, Steven J. Murdoch, and Ross Anderson. Thinking Inside the Box: System-Level Failures of Tamper Proofing. In *SP '08: Proceedings of the 2008 IEEE Symposium on Security and Privacy*, pages 281–295, Washington, DC, USA, 2008. IEEE Computer Society.

[9] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, pages 104–113, London, UK, 1996. Springer-Verlag.

[10] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 388–397, London, UK, 1999. Springer-Verlag.

[11] Markus Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays. In *SP '02: Proceedings of the 2002 IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2002. IEEE Computer Society.

[12] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Advances in Information Security. Springer, 2007.

[13] Colin Percival. Cache missing for fun and profit. *BSDCanada '05*, 2005.

[14] S. W. Smith. Fairy Dust, Secrets, and the Real World. *IEEE Security and Privacy*, 1(1):89–93, 2003.

[15] Eran Tromer, Dag Arne Osvik, and Adi Shamir. Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology*, 23(1):37–71, January 2010.