

# Preface

Cryptography plays a vital role in securing e-business and e-commerce transactions. The algorithms used have been rigorously analyzed and tested for their ability to conceal information. However, these algorithms are needed to be realized in systems that are used in a variety of applications. As the saying says, *there's many a slip 'twixt the cup and the lip*, these implementations may leak sensitive information via unintended timing channels. Over the past 20 years, several attacks have been developed that use these *side-channels* to reveal secrets from ciphers. These attacks, known as timing attacks, are powerful enough to break a mathematically robust cipher in few minutes on standard computing platforms.

Starting from its inception to the present day, timing attacks and the underneath statistics have evolved. Enhancements made to computer architecture over the years have also influenced timing channels. To develop a system secure against these threatening channels, one needs to be abreast of the interplay between cryptographic algorithms and computer architecture. Here is where this book steps in. It brings on a single platform aspects of computer architecture and cryptography that are essential to understand *how* timing attacks work and *why* they work. It describes the attacks and analyzes the relationship between the cipher implementation, system micro-architecture, and the attack threat. Various timing channels arising due to cache memories and branch prediction units are presented. The book would help engineers and researchers understand timing attacks and thereafter develop platforms that can tolerate these attacks.

The following topics are covered.

- **Modern Cryptography.** Attackers make use of the cipher's structure to extract the secret key from execution time. The attacks are made even more powerful when ideas from classical cryptanalysis are used with the timing information. The book therefore begins with a review of a variety of modern ciphers ranging from symmetric algorithms like the Advanced Encryption Standard (AES) to asymmetric algorithms like the Rivest-Shamir-Adleman (RSA), and some popular classical cryptanalysis techniques.

- **Superscalar Processor Architectures.** To address how timing channels arise in a system, the book provides a background of the internal micro-architecture of processors. An introduction to modern superscalar architectures has been provided, with an emphasis on the components in them that affect the execution time of ciphers.
- **Time-Driven Cache Attacks on Block Ciphers.** Memory load instructions that cause a cache miss takes considerably longer than those that result in a cache hit. Attackers utilize this difference to build a variety of attacks on block ciphers. A detailed discussion on how these attacks are implemented is presented, with emphasis on various accurate time measurement techniques and analysis methods to observe the cache hit miss phenomenon.
- **Advanced Time-Driven Cache Attacks on Block Ciphers.** Combination of classical cryptanalysis with side-channel attacks paves way to powerful attack methodologies. A combination of classical differential cryptanalysis with cache timing attacks has been discussed in the book to describe this threat.
- **Formal Analysis of Time-Driven Cache Attacks.** Developing suitable metrics for comparison of secured implementations and using them to guide the design flow is an important aspect in security engineering. In this pursuit, the book provides formal modeling of time-driven cache attacks on block ciphers and suggests metrics for evaluation and comparison of such implementations. A discourse on how micro-architectural features, such as pipelining and out-of-order execution, affect cache attacks is presented. These guidelines form a framework for developing ideal implementations of the block ciphers with respect to time-driven cache attacks.
- **Profiled Time-Driven Cache Attacks on Block Ciphers.** There are various types of cache attacks, of which profiled cache attacks are arguably the most powerful. The book provides a detailed description of such profiled attacks, which rely on building timing profiles in a learning phase before mounting the attack. The book also provides insights into developing metrics for estimating the information leakage and relates the leakage to micro-architectural features in modern computers, such as hardware prefetchers.
- **Access-Driven Cache Attacks on Block Ciphers.** Cache attacks come in different flavors, one of them, called access attacks, relies on a spy program running along with the encryption program. The spy uses timing measurements to determine memory access patterns made by the encryption. By monopolizing the OS scheduler, the spy program can accurately determine every memory access made, thereby leading to powerful attacks. The book provides a comprehensive overview on the topic to understand the theory and develop the procedure of such access attacks.
- **Branch Prediction Attacks.** Branch prediction units are artifacts in computer architectures to reduce performance penalties due to branch instructions. They predict whether a branch instruction will be taken or not taken, thereby reducing processor stalls. Although this can boost performance of an application significantly, it can also lead to timing channels that are catastrophic. Attackers have used these channels to break mathematically strong asymmetric key ciphers such

as the RSA. Several of the attack strategies developed are discussed in detail in the book.

- **Countermeasures.** To circumvent timing attacks, a variety of countermeasures have been proposed at various levels in the system: from the application level and architectural level to the Operating System. The book tries to provide an overview on these countermeasures, how they are applied, their effectiveness, and the consequent overheads involved.

IIT Kharagpur, India  
November 2014

Chester Rebeiro  
Debdeep Mukhopadhyay  
Sarani Bhattacharya

Timing Channels in Cryptography

A Micro-Architectural Perspective

Rebeiro, C.; Mukhopadhyay, D.; Bhattacharya, S.

2015, XVII, 152 p. 75 illus., 14 illus. in color., Hardcover

ISBN: 978-3-319-12369-1