RISE:2016
RESEARCH, INNOVATION AND SCHOLARSHIP EXPO
Undergraduate/Graduate
Category: Engineering and Technology
Degree Level: Undergraduate
Abstract ID# 1222

Northeastern University

Hacking Your Data – The Hard(ware) Way

Zachary Marcus, Andrew Tu, Alex Interrante-Grant, Saoni Mukherjee, David Kaeli

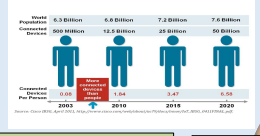
Abstract

1. Embedded devices, such as smartphones and tablets, handle sensitive information (like financial transactions)
2. Newer devices incorporate Graphics Processing Units (GPUs) to accelerate processes, which opens them to hardware-level vulnerabilities
3. Side channel attacks (SCA) target the physical characteristics of a cryptographic system, not its inherent algorithm weaknesses, to leak secure information such as the encryption key
4. Rivest-Shamir-Adleman (RSA) encryption, a classic example of public-key cryptography, is used extensively in secure online transactions
5. Runtime optimizations make RSA vulnerable to SCA
6. One optimization, Montgomery Multiplication (MM), used in this work, significantly reduces compute time when operating on larger numbers
7. Timing information leaked by MM optimized RSA can be used to factor the RSA modulus using a "binary search" like attack, an attack which targets small differences in timing when working with the most significant, to the least significant, bits.
8. After factoring the modulus, both the private and public keys can be produced trivially.

Introduction

Where do we stand?

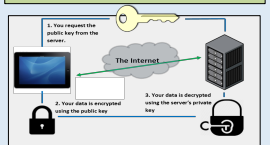
Mobile devices a part of life now
- Provide global communication capabilities
- Store personal data
- Often used for financial transactions



What is the problem?

Should you be worried?
- Unencrypted transactions
- Vulnerable wireless messages
- Access may lead to data/identity theft
- Potential vulnerability in encryption!

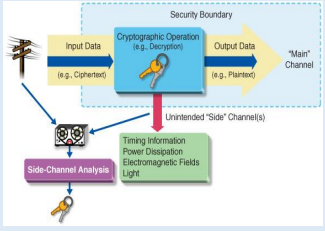
RSA: An Overview



Basic uses
- Encryption and Decryption
- Identity Verification (web transactions)

Mathematical Strength
- Relies on the factoring problem
- Factoring problem:Hard to factor multiplication of two large prime no.s

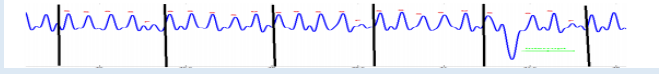
Side Channel Analysis (SCA)



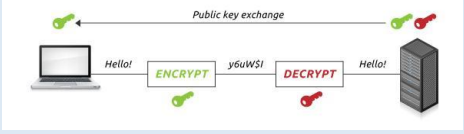
But What Are They?

- Attacks to exploit the physical behavior of a cryptographic system

- Encryption algorithms follow a pattern, where there is a relationship between, for example, the time taken and the value of the key that was used.



Encryption Process



Why use a GPU for encryption?

- Graphics processing units (GPUs) allow for parallel execution of tasks
- Example: With proper coordination, 32 judges can more quickly grade a room of posters than a group of 4 judges can
- Modular operations as used in RSA - can be split, using either Chinese Remainder Theorem or the Montgomery Space, to run on parallel, programmable chips.

Goal

To develop an understanding of a tablet's encryption behavior (on the GPU) via side channel attacks
- By breaking the tablet using side channel attacks
- AND eventually hardening the security of the very systems we seek to break.

Platform

Device used: Sony xperia z5 tab
Encryption platform: Qualcomm Adreno 810
OS: Android 5.01 (Marshmallow)

Method

Attacking RSA

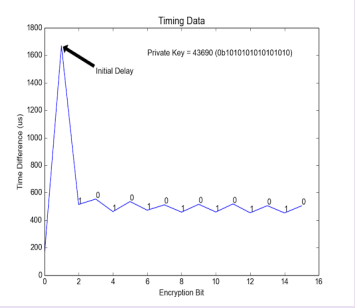
Is RSA vulnerable?
- Optimized run time leads to timing data emission.
- Timing data can be gathered by listening passively or through active queries.
- Statistical analysis of timing data can expose the factorization of RSA primes.
- Once the primes are known, a host/user can be impersonated, traffic decrypted, etc.

Results

How can we test our attacks?
- Idealized timing models of individual algorithms and optimizations.
- Using an ideal model, we can validate our approach before testing it on real-world data.
- Models can vary the level of background noise in timing data, testing the robustness of the attacks.

Relationship

- Very evident delta in between the time taken for the encryption to be performed, based on whether the current bit is a zero or a one.
- Can develop model to accurately predict the value of an encryption key based upon how long it takes to perform an operation.



Conclusion and Future Work

Looking at the initial testing done against RSA done on a standard processor, it is apparent that the computation's timing is data-dependent
- Timing attacks against the RSA done on a GPU might be similarly vulnerable.
- The GPU-based versions of RSA with its optional optimizations are currently under development
- Will be tested on an Android tablet as soon as they are proven to be working.

Will develop the necessary statistical models for a successful timing attack and apply to determine the level at which a GPU-based RSA algorithm leaks information.

Acknowledgements

NSF
NUCAR
NJ EESS

References

Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." *Advances in Cryptology—CRYPTO'96*. Springer Berlin Heidelberg, 1996.
Brumley, David, and Dan Boneh. "Remote timing attacks are practical." *Computer Networks* 48.5 (2005): 701-716.
Public-key. Digital Image. *Https://www.digicert.com/code-signing/code-signing.htm*. DigiCert Inc, n.d. Web. 14 March 2016
SideChannel Analysis. Digital Image. Http://www.microsemi.com. MicroSemi Corporation, n.d. Web. 14 Mar. 2016.
Snapdragon Image. Digital Image. *Http://www.androidauthority.com*. Android Authority, n.d. Web. 14 Mar. 2016. <http://www.androidauthority.com/wp-content/uploads/2012/06/qualcomm-snapdragon-s4.jpg>.