

Side Channel *TIMING* Attack

ZhiWei Ling
Sichuan University
email address

QuanBi Feng
Southern University of
Science and Technology
email address

XinMeng Liu Southern
University of Science and
Technology
email address

Tao Dan
school
email

pr
school
email

ABSTRACT

Briefly introduce this summer work camp, introduce side channel attack, timing attack

Categories and Subject Descriptors

Side Channel [Timing attack]: Miscellaneous

General Terms

Not sure what to say

Keywords

side channel attack

1. INTRODUCTION

Introduction to the side channel attack (consider several columns), and then move to the section on timing attacks, introducing our three sections: 1. The original channel test attack. 2. Attacks based on HTTP/2. 3. Extended attacks

2. THREAT MODEL

3. IMPLEMENTATION

Detailed principles, ready for three implementations

3.1 Simple demo

Introduce the first impl

3.2 HTTP/2

Introduce the second impl

3.2.1 subsubsection

We may need this

3.3 Extension

Introduce our design in HTTP/1

4. DEFENSE

How to defend the attack

5. CONCLUSION

Say something to conclude the project

6. ACKNOWLEDGMENTS

Compliment each other. Hand out chocolate fish to everyone

7. REFERENCES

- [1] AL-BASSAM, M., SONNINO, A., BANO, S., HRYCYSZYN, D., AND DANEZIS, G. Chainspace: A sharded smart contracts platform. arXiv preprint arXiv:1708.03778 (2017).
- [2] ANATI, I., GUERON, S., JOHNSON, S., AND SCARLATA, V. Innovative technology for CPU based attestation and sealing. In International Workshop on Hardware and Architectural Support for Security and Privacy (HASP) (2013).

APPENDIX

Do we really need an appendix?