ECE 5770 : Resilient Computer Systems
Surveying Efficient Low-Cost Memory Protection Techniques

Udit Gupta, Monica Jean Lin

School of Electrical and Computer Engineering, Cornell University, Ithaca, NY
ug28@cornell.edu, mjl256@cornell.edu

Abstract

1. Introduction

1. Talk about growth of mobile devices, connectivity and how mobile devices handle increasing amounts of sensitive data.
2. Memory encryption has become a prominent research topic - providing low cost (money, area, power and design complexity) and high performance (high throughput, low latency) memory encryption primitives is very important.
3. Generally memory encryption has been studied for general purpose processors (GPP) where power constraints are not as stringent however for mobile devies power is a first order design constraint.
4. Providing low power memory encryption is very important to enable memory encryption for mobile devices.
5. Characterizing the power overhead of the memory system is still an open problem - especially in the context of encryption.
6. Talk about the two main sources of power consumption [add pictures of dram chip toplogies]
7. We use first order approximations to model the power overhead of encrypting data on the memory system.
8. We verify that encrypted data has a significant power overhead [add numbers]
9. Outline the paper's sections

2. Problem Formulation

1. General - Explore the impact of memory encryption on power consumption
2. Use various computer architecture analysis tools to simulate a series of memory accesses and model the energy overhead of encryption on DDR4 memory technology

3. Methodology

[Add general picture of proc -¿ aes -¿ memory] Describe the general computer architecture design that we are considering for memory encryption. Generally use AES-CTR mode encryption

3.1 Model

1. Talk about DBI - AC and DC [Add picture of DBI DC impact]
2. Introduce equation

$$P_t = A \times P_{dc} + B \times P_{ac}$$

3. Talk about encrypted data : A = 0.5, B = 0.5 : Assumption that Data is Completely random once encrypted
4. Say that DBI aims to reduce A, B by using program structure

3.2 Experimental Setup

1. PIN - dynamic binary instrumentaiton tool : describe cache settings
2. Computer architecture analysis tool
3. MiBench - Justify why MiBench (mobile) —- SPEC is not as good
4. DRAMSim - Did not work for us.
5. Python Script to analyze the loads and stores from the trace outptted from PIN

4. Evauation

5. Group Dynamics

6. Related Work

7. Conclusion

[1]

References

[1] R. Elbaz, D. Champagne, C. Gebotys, B. R. Lee, N. Potlapally, and L. Torres. Hardware Mechanisms for Memory Authentication: A Survey of Existing Techniques and Engines. *Transactions on Computational Science IV, Lecture Notes in Computer Science (LNCS)*, 2009.