Template for Operating Systems: Design and Security

First Last, First Last, First Last
Computer Science Department, University of Bucharest, Romania

Abstract

Write here one or two paragraphs about what you will treat in the current paper: topic, methods, solutions, comparison results etc.

1 Introduction

In this section you introduce the problem and existing research or similar results in the field.

When citing remember you can use the quotes button from `https://scholar.google.com` to get the bibtex entry.

In this article we are going to investigate side-channel attacks [1] with focus on cache implementations [2].

2 Technical description of the problem

In this section you describe the technical details of the articles you surveyed.

Here is Algorithm 1

Algorithm 1: Attack Algorithm

Data: samples, $Y \in \mathcal{R}^{m \times N}$
number of iterations I
Result: secret, S

Initialize: $D = \emptyset$, $S = 0$
for $i = 1 : I$ **do**
  Initialize iteration dictionary D_i
  Compose $D = D \cup D_i$
  Compute X
  if $i = 1$ **then**
    Compute error threshold $e_{mean} = \frac{1}{N} \sum_{i=1}^{N} e_i$
  Update $\mathcal{A} = \{y_i \mid e_i > e_{mean}\}$
Secret estimates $l_i = 1$ if $y_i \in \mathcal{A}$

3 Possible solution

Here you describe possible solutions or workarounds to the problems described in the former section.

Here is Equation (1)

$$D \leftarrow D + \alpha r u^T \tag{1}$$

4 Experiments and Results

In this section you depict the manifestation of the vulnerabilities and the effect of the proposed solutions on dampening the attack effect.

Look at our experiments in Figure 1 and Table 1

Method	Dictionary	Representations
MOD	$O(m^3N + m^6)$	$O(m^5N)$
TMOD	$O(mN^2 + m^3)$	$O(m^4N)$
SuKro	$O(m^3N + m^6)$	$O(m^5N)$

Table 1: Total number of instructions for various methods.

5 Conclusion

In this section sum-up what you presented and talk a bit about what you found in the results section.

This differs from the abstract because now you can assume that the reader has processed the entire paper, whereas in the abstract you were only baiting him into reading it. In the abstract he does not posses the knowledge that he has now.

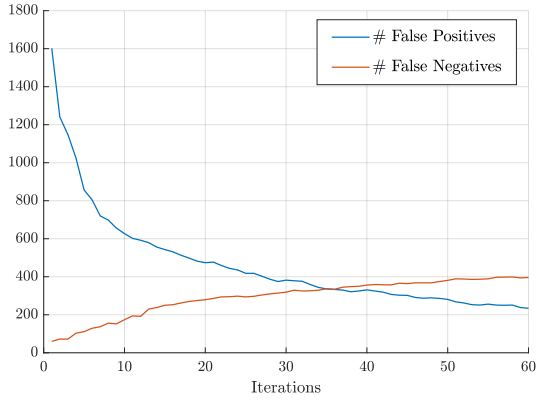

Figure 1: Unsupervised DL with error threshold

Otherwise abstract and conclusions are pretty similar in length and description.

References

[1] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[2] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, et al. Meltdown: Reading kernel memory from user space. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 973–990, 2018.