1

Deep Learning Techniques for Side Channel Analysis

Nimar Blume

***Abstract*—Put the abstract here. The abstract should be 200-300 words long and must answer the following questions:**

- **Why is this topic important and interesting?**
- **What is the topic?**

It's a good writing style to answer the "why" question first by putting the topic in a broader context.

***Index Terms*—deep learning, side channel analysis, side channel attack, encryption, AES**

I. Introduction

Data encryption is commonly employed to restrict data access to selected people or endpoints. Proper encryption provides privacy, integrity and authenticity of data exchanged between two or more parties over an insecure connection. Therefore, an encryption key (or a pair of keys for asymmetric encryption) is generated and selected data is encrypted with it, so that the data can only be read or modified by an endpoint who owns the same encryption key. For symmetric encryption, where the same secret key is used to encrypt and decrypt data, the key has to be shared over a secure connection beforehand, whereasa symmetric encryption provides key pairs, one of which is used to encrypt and one is used to decrypt data. That enables two parties to exchange data securely over an insecure connection by publishing the key used for encryption and keeping the key used for decryption private. This paper will only consider symmetric encryption, although techniques discuessed could also in part be applied to asymmetric encryption algorithms.

A. The Advanced Encryption Standard

While there are many encryption algorithms available, this paper focuses on the most popular symmetric block cipher: the Advanced Encryption Standard (henceforth AES) with a 128bit key. AES expands a single 128bit key to 11 round keys which are then used to encrypt the given data. It is important to note, that a compromise of any of the 11 round keys enables an attacker to reconstruct the initial 128bit key and thus decrypt the whole encrypted data set. The AES algorithm encrypts data in blocks of 128bits or 16bytes. Should a block be smaller than 16bytes, padding will be appended until the block size reaches 16bytes.

B. Side Channel Analysis

Side Channel Analysis (henceforth SCA) refers to a technique used to break encryption schemes by using data indirectly generated by the implementation of the cryptographic algorithm. Even a theoretically perfectly safe cryptographic algorithm can be subject to SCA and be broken by it. SCA uses side channels such as the power consumption of an integrated circuit (IC), electro magnetic emissions or even emitted sound to reconstruct the entire or parts of the secret key used to encrypt the data. It is possible to infer the secret key, because some algorithms' implementations have a program flow which is dependant on the secret key data. That means, that a certain loop will only execute if the current key bit is zero, therefore the power consumption of the IC will measurably increase. Furthermore, power modelling is used to predict an ICs power consumption based on the secret key data. For example, HAMMING WEIGHT, HAMMING DISTANCE... Therefore, to protect against SCA it is vital to pay attention not only on the theoretical safety of an encryption algorithm but also on its implementation.

What is side channel analysis with regard to cryptography?

Fabrizio Desantis, Chair of Security in Information Technology of the Technical University of Munich

II. State of the Art

Where can SCA be applied?

A. The state of Side Channel Analysis

Side channel attacks were first developed in 1996 by Paul Kocher [1] in the form of timing attacks. Timing attacks exploit an implementation's execution flow dependance on secret key data, which results in a different execution time if a key bit is for example 0 rather than 1. Later, SCAs have been extended to infer a secret key by analysing a processor's power consumption and its dependance on secret key data.

1) Simple Power Analysis:

2) Differential Power Analysis:

3) High-order Differential Power Analysis:

4) Template Attacks: Current state of SCA: Simple power analysis, differential power analysis, template attacks How do they work/what is the difference between the three?

B. How Machine Learning used in Template Attacks

Machine learning used in template attacks -> path to using deep learning techniques? SVM / RF trained on template models -> used to extract key from "final" model

III. Theory

Regular research papers need at least two additional sections here. One section for contributions and methods and one section for the results. For seminar papers these sections can be omitted.

IV. Experimental results

Show the results from the paper which covered the same topic.

V. Conclusion

Put the conclusions of the work here. The conclusion is like the abstract with an additional discussion of open points.

References

[1] "Total wi-fi® device shipments to surpass ten billion this month," Website, 2015, available at https://www.wi-fi.org/news-events/newsroom/total-wi-fi-device-shipments-to-surpass-ten-billion-this-month; last accessed on 21.07.2016.