Neural network attacks using side-channel leakages to break ECC implementations on consumer electronics

Michele Corrias - 808746

Academic Year: 2020/2021
Stage: 09/08/2021 - 31/03/2022

1 Security Pattern

This work has been developed in collaboration with *Security Pattern*, supervised by Prof. Danilo Bruschi and co-supervised by Eng. Guido Bertoni. Security Pattern is a company founded in 2017 in Brescia (Italy), by the engineers Guido Bertoni and Filippo Melzani, both former researchers at STMicroelectronics. The company specializes in the security of embedded systems, and is also active in the scientific research, with more than 50 papers published in the areas of computer science security and cryptography. During the internship period, Security Pattern members provided their knowledge and the required tools for the development of this study.

2 Introduction

During cryptographic operations performed by a device, physical information might be leaked as timing differences, power consumption, or electromagnetic emissions in a specific time period. In the literature, a well known set of attacks exploits these unintended leakages to obtain sensitive information (generally a cryptographic secret key). They are called *Side-Channel Attacks* (SCA), since *side channel* convey the idea that the channel used to transfer information is not the intended channel (i.e., plaintext, ciphertext), but a lateral (*side*) one that was not supposed to exist by the developer.
This work stems from a project started in Security Pattern by the author of [Nav20] with his thesis, which is inspired from the work of [Rya19] presented in the conference on *Cryptographic Hardware and Embedded Systems* (CHES) of 2019. The study in [Nav20] was intended to show how a *Neural Network* (NN) can be trained to break the security of *Elliptic-Curve Cryptography* (ECC) (in detail, the *Elliptic Curve Digital Signature Algorithm*) (ECDSA) when implemented on a modern board via SCA. In particular, NNs have been successfully used in recent years in SCA contexts, as an alternative to several generally adopted statistical techniques, such as correlation [WPB19; Wei+20; WPP21; Per+21; Pic+21]. Despite the results achieved, unfortunately, there were some technical details and limitations to consider that made it difficult in [Nav20] to mount a complete attack. Thus, in this work we proceed to handle and bypass these specific problems which prevented the success of a practical attack.

3 Goals

The ultimate goal of this work is to provide all the requirements needed to mount a specific key-recovery attack (such as, those in [FGR12; Ara+20; Ben+14; Roc+21]), in order to retrieve a private key used by a consumer electronics device during a cryptographic computation. To achieve this goal, in this study we proceed to mount, with a *Long Short-Term Memory* (LSTM) network, a specific SCA based on power consumption leakage of an off-the-shelf microcontroller, running an ECC implementation. The LSTM performing the SCA allows to retrieve a few bits of the ephemeral key used in the ECDSA implementation on each digital signature. Such retrieved bits make it possible to mount a key-recovery attack to recover the ECC secret key in a few hundreds signatures.

4 Description

In this work, we apply different techniques. First, we have made a theoretical study of the topics of the work and we have conducted an analysis of the current state of the art. We have choosen an LSTM among the different possible structures of NNs for several reasons. It processes sequences of data and performs well with time series, it has temporal consciousness, maintaining memory over time. Moreover, we were inspired by the *Human Activity Recognition* (HAR) [Ang+13; OR16] methodology and literature, where the LSTM works well and accurately recognizes activity patterns. In this study, our approach is to start from the results achieved in the previous work [Nav20], and to reduce the number of variables with the implementation of a purpose-built simulation environment. Thus, monitoring and managing the target leakage model and the acquisition system of the power consumption traces, we aim to focus only on the NN. Once we have obtained perfect results with the NN in the simulation phase, we can move on and use it in the real use case, where there are more noise and difficulties to be tackled. Therefore, we have acquired some power consumption traces of the target microcontroller performing sensitive ECC operations, and we have used them to develop a supervised training of the LSTM from the previous phase. This is in order to exploit the leakage model related to the ECDSA implementation considered. Hence, thanks to the NN, it is possible to retrieve a few bits of the ephemeral key used in the ECC implementation. Such recovered bits allow an attacker to recover the entire private key.

5 Tools

We focus on the `STM32F415` microcontroller (and relative *STM32CubeIDE*), and on *micro-ecc* library, a widely used ECC implementation. We acquire the power consumption trace with the device `CW1200` *ChipWhisperer-Pro*. We build the LSTM network with the *TensorFlow* framework and *Keras* API. For free of charge access to computing resources like GPUs and TPUs, we use *Google Colab* and *Kaggle* to train the LSTM network we have developed. We implement a few ECC tests with the free open-source mathematics software system *SageMath*. More generally, the programming languages involved in the work are `C` and `Python` (including *Jupyter Notebooks* and a few of useful software libraries and modules).

6 Results

With the improvements of this work we are able to achieve successful results, with a NN accuracy of more than 97% on the real power consumption traces of the target device. We also provide different statistical metrics to evaluate the results obtained. These results allow to use the trained NN to find a few bits of the ephemeral key on each digital signature, under specific conditions. Thus, an attacker could mount a practical attack and recover the ECC private key in a few hundreds signatures collected. As a side effect, we introduce an innovating part in the application of the HAR technique, by which we were inspired, and of LSTM on off-the-shelf microcontrollers performing sensitive ECC operations. To the best of our knowledge, our approach constitutes the first application of using this technique in the state of the art, and this is the first time that a LSTM is employed in SCAs. This solution has the potential to affect all the boards where an attacker can perform power analysis. Finally, the publication of a scientific paper is planned for the presentation of the results achieved in this work. During the internship, through the development of this work, different knowledge and skills have been gained, such as a basic understanding of: (1) embedded systems; (2) elliptic curves and how they are applied to real-world contexts, with particular attention to scalar multiplication (the main ECC operation); (3) NNs, with focus on LSTM networks; (4) SCAs employed in real use cases. Finally, several difficulties have been experienced during this work, for instance: (1) the complexity of mathematical know-how about elliptic curves; (2) the technical details of an embedded system to handle; (3) the management of computing resources in order to train the network (a task of high computational cost).

References

[Ang+13] Davide Anguita et al. "A Public Domain Dataset for Human Activity Recognition using Smartphones". In: *Proceedings of the 21th International European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*. 2013, pp. 437–442.

[Ara+20] Diego F Aranha et al. "Ladderleak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 2020, pp. 225–242.

[Ben+14] Naomi Benger et al. ""Ooh Aah... Just a Little Bit": A Small Amount of Side Channel Can Go a Long Way". In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2014, pp. 75–92.

[FGR12] Jean-Charles Faugere, Christopher Goyet, and Guénaël Renault. "Attacking (EC)DSA Given Only an Implicit Hint". In: *International Conference on Selected Areas in Cryptography*. Springer. 2012, pp. 252–274.

[GBC16] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. `http://www.deeplearningbook.org`. MIT Press, 2016.

[HS97] Sepp Hochreiter and Jürgen Schmidhuber. "Long Short-Term Memory". In: *Neural Computation* 9.8 (1997), pp. 1735–1780.

[JMV01] Don Johnson, Alfred Menezes, and Scott Vanstone. "The Elliptic Curve Digital Signature Algorithm (ECDSA)". In: *International journal of information security* 1.1 (2001), pp. 36–63.

[Kob87] Neal Koblitz. "Elliptic Curve Cryptosystems". In: *Mathematics of Computation* 48.177 (1987), pp. 203–209.

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Annual International Cryptology Conference*. Springer. 1999, pp. 388–397.

[Koc+11] Paul Kocher et al. "Introduction to Differential Power Analysis". In: *Journal of Cryptographic Engineering* 1.1 (2011), pp. 5–27.

[Mei05] Marina Meilă. "Comparing Clusterings: an Axiomatic View". In: *Proceedings of the 22nd International Conference on Machine Learning*. 2005, pp. 577–584.

[Nav20] Lorenzo Nava. "Side-Channel Attack on ECC Cryptosystem by using Neural Networks". MA thesis. Università degli Studi di Milano, Dec. 2020.

[OR16] Francisco Javier Ordóñez and Daniel Roggen. "Deep Convolutional and LSTM Recurrent Neural Networks for Multimodal Wearable Activity Recognition". In: *Sensors* 16.1 (2016), p. 115.

[Per+21] Guilherme Perin et al. "Keep It Unsupervised: Horizontal Attacks Meet Deep Learning". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021), pp. 343–372.

[Pic+21] Stjepan Picek et al. "SoK: Deep Learning-based Physical Side-Channel Analysis". In: *Cryptology ePrint Archive* (2021).

[Riv11] Matthieu Rivain. *Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves*. Cryptology ePrint Archive, Paper 2011/338. 2011. URL: `https://eprint.iacr.org/2011/338`.

[Roc+21] Thomas Roche et al. "A Side Journey to Titan". In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 231–248.

[Rya19] Keegan Ryan. "Return of the Hidden Number Problem.: A Widespread and Novel Key Extraction Attack on ECDSA and DSA". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), pp. 146–168.

[WPB19] Leo Weissbart, Stjepan Picek, and Lejla Batina. "One Trace Is All It Takes: Machine Learning-based Side-Channel Attack on EdDSA". In: *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer. 2019, pp. 86–105.

[Wei+20] Leo Weissbart et al. "Systematic Side-Channel Analysis of Curve25519 with Machine Learning". In: *Journal of Hardware and Systems Security* 4.4 (2020), pp. 314–328.

[WPP21] Lichao Wu, Guilherme Perin, and Stjepan Picek. "The Best of Two Worlds: Deep Learning-assisted Template Attack". In: *Cryptology ePrint Archive* (2021).