Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks

[Extended Abstract]

Giacomo de Meulenaer*
UCL Crypto Group
Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium
giacomo.demeulenaer@uclouvain.be

François-Xavier Standaert†
UCL Crypto Group
Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium
fstandae@uclouvain.be

ABSTRACT

Node compromise is a critical issue in the security of Wireless Sensor Networks (WSN). A popular approach to thwart the problem relies on the detection of events that arise during the attack (removal of a node, etc.). However, certain attacks, such as side-channel attacks, might be furtive and defeat this type of defense. This work clarifies this question through a case study on power analysis attacks of AES and ECC implementations on the MICAz and TelosB nodes. We show how to perform the attacks in a stealthy manner. As a result, stealthy node compromises should be considered when securing WSN. This work underlines the importance of low-cost side-channel countermeasures for sensor nodes.

1. INTRODUCTION

Being deployed in a potentially hostile environment, Wireless Sensor Networks (WSN) are by nature exposed to node compromise. In this attack, an adversary tries to physically tamper with a node in order to extract the cryptographic secrets. Two main directions exist to circumvent this important threat to the security of WSN. The first one consists in improving the tamper resistance of the nodes, which can be costly for low-resource platforms. The second one adopts a surveillance-based approach, usually at the level of the network, which tries to detect events related to the node compromise. It assumes that a node capture will provoke some noticeable events, such as a loss of connectivity, a displacement or removal of a node, a loss of the node internal state, etc [1]. However, it remains to be verified whether this assumption holds for any kind of node compromise.

Side-channel attacks (SCA), which are efficient on many small devices, may be able to avoid the detection of node compromise countermeasures. In their passive form, these attacks are not supposed to interfere with the device operations. However, passive SCA might not remain unnoticed when implemented in practice on sensor nodes. Indeed, to remain furtive, the attacks must be performed on-site and without generating any of the detectable events listed earlier. The specificities of the WSN scenario can be challenging for the adversary for the following reasons:

Passive acquisition: Achieving fully passive SCA might be difficult with usual measurement setups. For instance, power analysis classically requires the insertion of a small resistor in the power line, depackaging the chip may be needed to efficiently measure electro-magnetic emanations, etc. This should be done without disrupting the device operations.

On-site acquisition: The accessibility to the target node for the attacker and his equipment depends on the context. Moreover, his presence might reveal the attack.

Uncontrolled Device: The attack should be feasible based on known ciphertexts and a few measurements since the frequence of use of the cryptographic primitive is beyond the control of the adversary. Moreover, the extraction of the useful portions in the acquired physical data cannot be made easier by the use of triggers.

Real-world device: With respect to a board dedicated to SCA, more noise is expected due to the presence of many components that work simultaneously. Also, components filtering the power supply complicate power analysis.

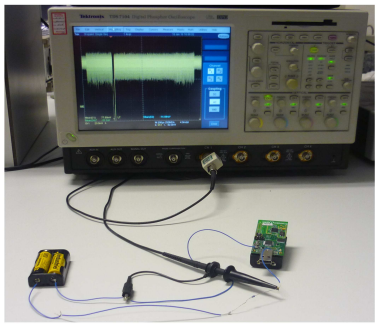

Figure 1: Measurement setup of our power analysis attack on the TelosB node.

Up to now, SCA have not been shown to enable stealthy node compromise in wireless networks yet. Also, few cryptographic implementations designed for WSN propose countermeasures against these attacks.

In this work, we study the feasibility of stealthy node compromises in WSN by performing power analysis attacks on AES and ECC implementations on the MICAz and TelosB nodes. Using our setup, the attacks are not detectable by the usual node compromise defenses.

Our contributions are the following. First, we prove the feasibility of furtive node compromises in the context of WSN.

*Supported by Walloon Region project Nanotic.
†Associate researcher of the Belgian Fund for Research.

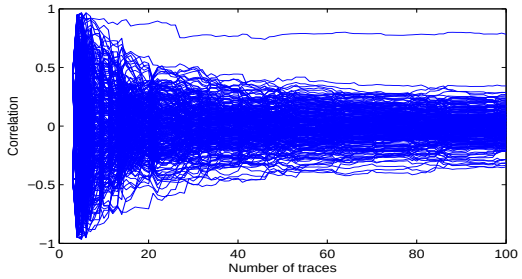

Figure 2: Correlation coefficients of the 256 guesses of the first key byte in function of the number of traces (MICAz). The right guess is already revealed with less than 20 traces.

Stealthy node captures should therefore be considered when designing secure WSN. Second, the low complexity of our stealthy power analysis attacks underline the importance of side-channel countermeasures in cryptographic implementations for sensor nodes.

In the following, we first detail the configuration of our furtive power analysis attacks. Then, we give the results of two attacks performed in this way: a Differential Power Analysis (DPA) on AES and a template-based Simple Power Analysis (SPA) on ECC, both achieved on the popular MICAz and TelosB sensor nodes. Finally we state the implications of our results.

2. ATTACK CONFIGURATION

We consider a typical WSN scenario where the nodes periodically exchange encrypted messages. For simplicity, we restrict ourselves to the case where the on-site acquisition is convenient for the adversary: the nodes are easily accessible and the presence of the adversary at the target node is not detected (e.g., in a large outdoor WSN).

For the acquisition of the power traces, we replaced the node power supply with a supply containing a 10-Ω sense resistor in its circuit. To obtain meaningful traces, we had to remove several capacitors and inductors filtering the power supply. Special care was taken to prevent any transient failure in the power supply while handling its circuit. For this, we temporarily introduced an additional power supply line to go on feeding the node components while interrupting the original power line. Throughout these manipulations, we checked the stability of the supply voltage with an oscilloscope. Only minor variations were observed. The smooth running of the node was also verified by checking the regularity and the content of the broadcasted messages. Remark that it appears feasible for an attacker to put the node board back in its original state in order to avoid any ulterior visual detection of the attack.

Our measurement setup is shown in Figure 1. The voltage drop across the resistor is measured on a Tektronix TDS7104 oscilloscope at a sampling frequency of 250 MHz. A more portable device could be used, like a PC-based oscilloscope for instance.

3. DPA ATTACK ON AES

Our first attack concerned a classical DPA attack (see [3] for a description) on a software implementation of AES-128. The power traces were acquired using the brief transmission state of the transceiver as a rough trigger. Resynchronizing the traces was successfully performed using the correlation based method suggested in Section 8.2.2 of [3]. The collection of the broadcasted ciphertexts allowed the attack on the last round key. Inverting the AES key schedule revealed the main key. The attack succeeded with a moderate complexity as shown in Figure 2 for the MICAz. Less than 40 and 80 traces were sufficient to recover the full AES key on the MICAz and TelosB respectively. This complexity is clearly reachable for an adversary. E.g., for a node sending a message every 5 seconds, less than 10 minutes allow the acquisition of enough traces to recover the key.

4. TEMPLATE-BASED SPA ON ECC

Our second attack was a template-based SPA on ECC-160 (following the description of [4]). This powerful attack requires the offline access to a similar device using the same ECC implementation. This is realistic assuming the use of commercial platforms and a freely available ECC implementation such as the TinyECC library [2] that we employed. Based on the acquisition of one single trace, we were able to recover one bit of the secret scalar. By repeating this one-bit key recovery step on the same trace, the whole key can be obtained with high confidence. This attack is really severe in WSN since it can expose the whole ECC key by acquiring a single trace of an ECC computation. The offline phase of the attack, during which the templates are built, lasts on the order of 10 hours with 100 traces per template. The templates are created on-the-fly, as suggested in Section 4.3 of [4].

5. CONCLUSION

In this work, we prove the feasibility of furtive power analysis attacks in the context of WSN. Using our setup, these attacks can be undetectable for surveillance-based node capture defenses. While limited to situations where the nodes are easily accessible and the adversary presence is not detected, they are still of concern in many realistic scenarios of WSN. They involve the manipulation of the power supply circuit without disturbing the node, which can be challenging if some of its components are hard to access. However, for a skilled adversary, the furtive power analysis attacks represent a really attractive option, thanks to the moderate amount of power traces to record. While defeated, surveillance-based defenses are not useless against furtive attacks as they prevent the attacker from actively speeding up the acquisition phase (e.g., by injecting messages).

The existence of furtive attacks has a severe implication on the security of WSN. To remain secure, WSN should either use security protocols which tolerate stealthy node compromises or make use of nodes that are protected against these attacks. The former option may be hard to achieve depending on the functionality of the protocol. Alternatively, the latter option necessitates on-board defenses that are as strong as the cryptographic algorithm employed. This underlines the need of robust and low-cost side-channel defenses for small devices like sensor nodes.

6. REFERENCES

[1] C. Krauß, M. Schneider, and C. Eckert. On handling insider attacks in Wireless Sensor Networks. *Inf. Secur. Tech. Rep.*, 13(3):165–172, 2008.

[2] A. Liu and P. Ning. TinyECC: A configurable library for Elliptic Curve Cryptography in Wireless Sensor Networks. In *IPSN*, pages 245–256, April 2008.

[3] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards.* Springer-Verlag New York, 2007.

[4] M. Medwed and E. Oswald. Template attacks on ECDSA. In *Information Security Applications: 9th International Workshop, WISA 2008*, pages 14–27. Springer-Verlag, 2009.