STRONG UNILATERAL AUTHENTICATION OF LOW-COST DEVICES INVOLVED IN INTERNET OF THINGS IN SMART HOMES

Vlastimil Clupek
Doctoral Degree Programme (4), FEEC BUT
E-mail: clupek@phd.feec.vutbr.cz

Supervised by: Vaclav Zeman
E-mail: zeman@feec.vutbr.cz

Abstract: In this paper we focused on authentication of low-cost devices involved in Internet of Things (IoT) in smart homes. We proposed a unilateral authentication protocol for authentication of low-cost devices involved in IoT with a Control Unit (CU) of a smart house. The protocol allows secure transmission of secret information between communication entities. Only cryptographic primitives as Hash functions, XOR operations and Physical unclonable functions (PUFs) are necessary for execution of the protocol. Security of the proposed protocol is described.

Keywords: Authentication, Physical unclonable functions, Low-cost devices, IoT, Smart homes.

1 INTRODUCTION

Nowadays, Information technology (IT) has become an inseparable part of human lives. The fastest growing part of IT is Internet. Internet is used by many people on the Earth everyday. The form of Internet is still in an evolution. Internet directs to its further phase now. The most important role in this phase will play IoT. According to [1] it is expected that IoT, which excludes PCs, tablets and smartphones, will grow to 26 billion units installed in 2020. This is a huge number and will play an important role in human lives. IoT usually uses low-cost devices (which represent computationally and resource constrained devices) to collect and exchange data from sensors and another equipment by Wireless sensor network (WSN), RFID technology, 3G and 4G connections, Wi-Fi, WiMAX and so on. It is presumed that these devices will be everywhere around us and will help us in our day lives. These devices will be implemented in smart homes, smart cities, hospital environment, industry monitoring applications and so on. Since data from these devices are crucial for specialized applications, it must be secured.

The most important terms in cryptographic security are authentication, confidentiality, integrity and non-repudiation. With using authentication protocols it is possible to verify authenticity of entities during electronic communications. Confidentiality ensures that only authorized entities can know the secret information. Integrity ensures that data were not modified during transmission between communication entities. Non-repudiation ensures that any communication entity cannot deny some fact which was done before. Authentication between communication entities can be unilateral or mutual. In case of unilateral authentication or one-way authentication, the first entity is authenticated to the second entity or the second entity is authenticated to the first entity. In case of mutual authentication communication entities are authenticated to each other. Mutual authentication is typically used to ensure an extra level of security, for example, in financial transactions between organizations or in some cases of access control.

2 PHYSICAL UNCLONABLE FUNCTIONS

Many PUFs concepts have been presented over the past thirty years. The first studies cannot be called PUFs by their authors, but they may have some PUF properties. This is due to the fact that the PUF concept was systematically written only by Ravikanth Pappu in 2001. Pappu described the concept of PUF in his dissertation thesis [2]. Pappu called PUFs Physical one-way functions (POWFs) and defined them as functions which are easy to compute but hard to invert. Most concepts of PUFs are based on heterogeneities and the differences between physical components of a device, which are caused by manufacturing differences. Heterogeneities of the produced components are random and they cannot be controlled by a manufacturing process. For this reason PUFs cannot be cloned. PUFs represent an alternative to classic store of secret keys, which are stored in nonvolatile memories. In PUFs secret keys are generated during an authentication process with using unique properties of the concrete device. These unique properties depend on variations in the manufacturing process. In case a secret key is stored in a nonvolatile memory, an attacker gets it. After that the attacker can perform a clonning attack. A protection against this attack can be ensured by encryption of secret data if a system is switched off. If the system is switched on, secret data are decrypted. PUFs can be used as an alternative to a protection against clonning attacks. Most PUFs exploit the differences from chips, which are caused by the differences in a manufacturing process, to generation unique keys by direct outputs from system circuits of chips without explicitly storing them. PUFs can be used for authentication (identification of chip) and generation of the secret keys. PUFs are functions with an internal random character, which mostly exploit manufacturing variabilities to generation unpredictable responses. Therefore, responses of PUFs are compared to fingerprints. An input of PUF is called *challenge* and an output of PUF is called *response*. PUFs are not really mathematical functions since these functions are able to produce several output values from one input value or from several input values they can produce one output value. $Challenge-response\ pair$ (CRP) is created by mapping of *challenges* to corresponding *responses* $(response = PUF(challenge))$. Authentication by PUFs consists of two phases. The first is an initialization phase in which a PUF is inquired and CRPs are stored in a database. In the second phase a *challenge* from the database is applied to a PUF and an obtained *response* is compared with the corresponding *response* which is stored in the database. If they are equal, the device will be authenticated. This phase is called an identification phase or a verification phase.

PUFs can be created by many ways. Many of them can be used to authentication on low-cost devices. Optical PUFs are represented in [3] and [4]. Other papers use a ring oscillator (RO) to build PUFs. In [5] a lightweight RO-PUF is described. In this work [6] are described two methods to extract secret keys from a ring oscillator. The papers [7] and [8] represent delay-based PUFs. The works [9] and [10] use SRAM memory to build PUFs. PUFs can be used to authenticate, generate secret keys and solve the "Night-shift problem". PUFs bring more security and simultaneously reduction of costs. PUFs do not require any permanent storage to save a unique secret information. PUFs are able to generate the unique secret information "on-the-fly". The main disadvantage of PUFs is their output noise. All PUFs produce unstable responses, some of them are very sensitive to the environmental conditions. These errors of outputs may have a random nature or a deterministic nature. Deterministic generated errors are caused by differences of environmental conditions, differences of supply power, ageing of components and so on. Random errors are caused by a peripheral noise. The noisy output of a PUF is a problem for authentication. An error correction code (ECC) can be used to solve this problem. The disadvantage is that an ECC requires a non-volatile memory. However, the PUF for authentication can be implemented without an ECC. In this case the parameters of one PUF must be different enough from the another PUF. Even a very noisy output can be identified correctly.

3 OUR PROPOSAL OF AUTHENTICATION PROTOCOL WITH SECURE TRANSMISSION OF INFORMATION FOR SMART HOMES

Many protocols for authentication of devices involved in IoT were proposed. [11] uses secret sharing scheme to authentication. The authors of [12] use Elliptic Curve Cryptography (ECC) to authentication. [13] uses Fermat Number Transform (FNT) and Chinese Remainder Theorem (CRT) to authenticated communication. The authors of [14] use some implicit certificates to authentication. [15] shows a comparative study on various authentication protocols in WSN. We have proposed a strong unilateral authentication protocol with secure transmission of information between a low-cost device involved in IoT and CU of a smart house. The proposed protocol uses only Hash functions, XOR operations and PUFs. Figure 1 shows the principle of the proposed protocol. On the left side of Figure 1 a concept of wireless communication between low-cost devices involved in IoT and a CU of a smart house is shown. The blue numbers represent the steps in the Figure 1 on the right side. On the right side of Figure 1 an exchange of messages between a low-cost device and the CU during in an authentication process can be seen.

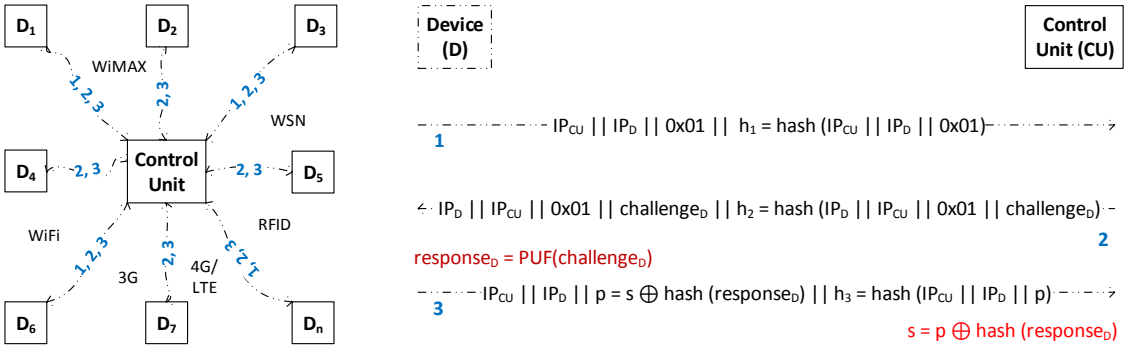

Figure 1: Principle of proposed protocol.

There are low-cost devices $(D_1 - D_n)$ and CU in the proposed protocol. The CU has a database of CRPs of PUFs implemented in low-cost devices $(D_1 - D_n)$. In case a low-cost device wants to send an authenticated secret information to the CU, it will act as follows. The device in the step 1 sends $IP_{CU}||IP_D||0x01||h_1$ to the CU. IP_{CU} represents the IP address of the CU. IP_D represents the IP address of a low-cost device. 0x01 represents a type of a transmitted secret information, which the device will send to the CU. The CU compares the received hash h_1 with its own hash $h_1^{'}$, which is computed by a Hash function with using received $IP_{CU}||IP_D||0x01$. If they are equal, integrity of transmitted data will be guaranteed. Subsequently, the CU in the step 2 sends $IP_D||IP_{CU}||0x01||challenge_D||h_2$ to the device. The device compares the received hash h_2 with its own hash $h_2^{'}$, which is computed by a Hash function using received $IP_D||IP_{CU}||0x01||challenge_D$. If they are equal, integrity of transmitted data will be guaranteed. The device D computes a $response_D = PUF(challenge_D)$ and a $hash(response_D)$. Now the device performs an operation XOR with a secret information and the $hash(response_D)$. The size of the transmitted secret information must be equal to the size of the $hash(response_D)$, in order to the conditions of the Vernam cipher [16] will be satisfied. The size of the output hash function can be equal for example 256 bits. The result of the operation XOR represents a public value $p = s \oplus hash(response_D)$. The device in the step 3 sends $IP_{CU}||IP_D||p||h_3$ to the CU. The CU compares the received hash h_3 with his own hash $h_3^{'}$, which is computed by a Hash function using received $IP_{CU}||IP_D||p$. If they are equal, integrity of transmitted data will be guaranteed. Subsequently, the CU computes $hash(response_D)$ from the corresponding $response_D$ from its database to the $challenge_D$, which CU sent to the device. The CU computes the secret information $s = p \oplus hash(response_D)$ using

the received value p and the $hash(response_D)$. The secret information can represent for example a temperature from a gas boiler. In case the CU starts protocol, the step 1 will be skipped. In the proposed protocol a light-weight variant of the Hash function SHA-3 or the light-weight hash function LOCHA for WSN [17] can be used. The PUF suitable for implementation on low-cost devices is presented for example in [5]. A suitable Error correcting code (ECC) must be included on outputs of the used PUFs. An ECC for output of a PUF is necessary to secure transmission of the secret information. In this case the Hamming distance between the save $response_D$ in the database and the computed $response_D$ must be zero, in order to decryption of the secret information will be successful.

Authentication of the device D to the CU is achieved by CRPs of the PUF, which is implemented in the low-cost device. Integrity of the received data is ensured by Hash functions (hashes $h_1 - h_3$). On inputs of Hash functions all transmitted values are inserted. Randomness of messages is achieved by CRPs, which are different for each PUFs. Unrepeatability is achieved by an assumption that each CRP can be used only once. Non-repudiation of authentication of the device and receiving secret information is achieved by CRPs. The corresponding $response_D$ to the specific $challenge_D$ can create only one specific PUF, which is implemented in one specific low-cost device. Confidentiality of the transmitted secret information is achieved by a Hash function, XOR operation and a PUF. The secret information is XORed with the $response_D$, which is known only to the CU and to the device D, which has implemented the corresponding PUF, which can be used to generate the corresponding $response_D$. The proposed protocol can be implemented in the constrained application protocol (CoAP) [18] or in the 6LowPAN [19].

4 CONCLUSION

In this paper a strong unilateral authentication protocol with secure transmission of information between a low-cost device involved in IoT and Control Unit of a smart house was presented. The protocol uses only PUFs, Hash functions and XOR operations. Our protocol is easy to implement on both ASIC and FPGA. The proposed protocol will be resistant to attacks coming from quantum computers, due does not use PKI, Elliptic curves, hyperelliptic curves, class groups and so on. In our feature work we will implement our protocol on suitable low-cost devices and we will test stability of PUFs outputs against local environmental and voltage fluctuations.

ACKNOWLEDGEMENT

Research described in this paper was financed by the National Sustainability Program under grant LO1401 and by the Czech Science Foundation under grant no. 102/12/1274. For the research, infrastructure of the SIX Center was used.

REFERENCES

[1] Janessa Rivera and Rob van der Meulen. Gartner says the internet of things installed base will grow to 26 billion units by 2020. *Stamford, conn., December*, 12, 2013.

[2] Pappu Srinivasa Ravikanth. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, 2001.

[3] Malcolm Spain, Benjamin Fuller, Kyle Ingols, and Robert Cunningham. Robust keys from physical unclonable functions. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pages 88–92. IEEE, 2014.

[4] Ulrich Rührmair, Christian Hilgers, Sebastian Urban, Agnes Weiershäuser, Elias Dinter, Brigitte Forster, and Christian Jirauschek. Revisiting optical physical unclonable functions. *IACR Cryptology ePrint Archive*, 2013:215, 2013.

[5] Chaohui Du and Guoqiang Bai. A novel relative frequency based ring oscillator physical unclonable function. In *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*, pages 569–575. IEEE, 2014.

[6] Onur Gunlu, Onurcan Iscan, and Gerhard Kramer. Reliable secret key generation from physical unclonable functions under varying environmental conditions. In *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*, pages 1–6. IEEE, 2015.

[7] Teng Xu and Miodrag Potkonjak. Stable and secure delay-based physical unclonable functions using device aging. In *Circuits and Systems (ISCAS), 2015 IEEE International Symposium on*, pages 33–36. IEEE, 2015.

[8] Zhi-Hua Xia, Xing-Ming Sun, and Xing-Wei Wang. Techniques for design and implementation of an fpga-specific physical unclonable function. 2016.

[9] Susumu Okumura, Shusuke Yoshimoto, Hitoshi Kawaguchi, and Masahiko Yoshimoto. A physical unclonable function chip exploiting load transistors' variation in sram bitcells. In *Design Automation Conference (ASP-DAC), 2013 18th Asia and South Pacific*, pages 79–80. IEEE, 2013.

[10] Yu Zheng, Maryam S Hashemian, and Swarup Bhunia. Resp: a robust physical unclonable function retrofitted into embedded sram array. In *Design Automation Conference (DAC), 2013 50th ACM/EDAC/IEEE*, pages 1–9. IEEE, 2013.

[11] Omaimah Omar Bamasag and Kamal Youcef-Toumi. Towards continuous authentication in internet of things based on secret sharing scheme. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, page 1. ACM, 2015.

[12] Ning Ye, Yan Zhu, Ru-Chuan Wang, Reza Malekian, and Lin Qiao-min. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics & Information Sciences*, 8(4):1617, 2014.

[13] Manali D Shah, Shrenik N Gala, and Narendra M Shekokar. Lightweight authentication protocol used in wireless sensor network. In *Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on*, pages 138–143. IEEE, 2014.

[14] Pawani Porambage, Corinna Schmitt, Pranaw Kumar, Andrei Gurtov, and Mika Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, pages 2728–2733. IEEE, 2014.

[15] S Raja Rajeswari and V Seenivasagam. Comparative study on various authentication protocols in wireless sensor networks. *The Scientific World Journal*, 2016, 2016.

[16] Gilbert S Vernam. Secret signaling system, July 22 1919. US Patent 1,310,719.

[17] Amrita Roy Chowdhury, Tanusree Chatterjee, and Sipra DasBit. Locha: A light-weight one-way cryptographic hash algorithm for wireless sensor network. *Procedia Computer Science*, 32:497–504, 2014.

[18] Zach Shelby, Klaus Hartke, and Carsten Bormann. The constrained application protocol (coap). 2014.

[19] Zach Shelby and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*, volume 43. John Wiley & Sons, 2011.