Demo: An RFID Based Secure Key and Configuration Distribution for Contiki

Mine Cetinkaya
University of Bremen, Germany
minecetin@uni-bremen.de

Jens Dede
University of Bremen, Germany
jd@comnets.uni-bremen.de

Anna Förster
University of Bremen, Germany
afoerster@comnets.uni-bremen.de

Abstract

Encryption and authentication are essential in nowadays communication systems. Under the keywords *Internet of Things*, *Smart Home*, *Industry 4.0*, etc., wireless sensor networks (WSNs) are deployed more and more to our everyday life. The nodes in these WSNs are usually constrained in energy, memory and processing power which prohibits the use of state of the art key exchange technologies, as for example Diffie–Hellman. In this demo, a key and configuration distribution system for constrained wireless sensor nodes is introduced, which offers an easy to deploy and easy to use secure communication inside WSNs.

1 Introduction

Wireless sensor networks (WSNs) are becoming more and more an essential part of our everyday life. Two out of the manifold application scenarios are controlling *Smart Homes* and the monitoring of goods in logistics. The possible attack scenarios are diversified [7, 8] and can lead to massive problems starting from unavailability of the service, knowing the presence of persons and ends in injecting misleading data packets. Hence, encryption and authentication are essential.

The nodes in WSNs are constrained in energy, memory and processing power, which prohibits the use of technologies known for example from Internet services. Currently, the configuration and key deployment in WSNs is often done

- Manually using a wired connection between node and computer.
- Automatically via an insecure (i.e. unencrypted or encrypted with a known key) connection.

Especially in logistics, the nodes have to be reconfigured often and quickly due to the high optimization of the processes. Additionally, the enclosures of the nodes have to be sealed which forbids in most cases an easy to open casing.

In this work, an easy to use implementation for key and configuration distribution for the WSN operating system *Contiki*[1] based on RFID is demonstrated. It allows a quick configuration of nodes based on RFID tags: The user presses a button on the nodes which triggers the readout of an RFID tag and the reconfiguration of the node. In this demo, the encryption key of the node is changed although the implementation can easily be adapted to also change other configuration parameters like sensing intervals, radio channel, target addresses etc.

2 RFID

RFID (radio-frequency identification)[3] is a near field radio technology, i.e., it operates in the range of a couple of centimeters. It is commonly used in billing, identification and time and attendance systems. RFID tags are available in different formats like in a card or coin format as depicted in Figure 1. These tags can be read out and – depending on the type – be written by an RFID interface which is also known as an RFID reader. This kind of devices are available for example in modern smartphones under the name of newer and extended standard *NFC* (Near Field Communication), which is compatible to RFID.

Each RFID tag has several blocks with different purposes. The first block is the immutable manufacturer's block containing a unique identifier. The content of the subsequent blocks depends on the exact type of the tag. Depending on the tag type, these values are either fixed or can be changed by the user. These blocks perfectly suited for storing the node configuration and encryption keys for sensor nodes.

3 Encryption in Contiki

Krentz et al. [4] introduced AES-128 based [2] encryption and authentication as a security sublayer to Contiki. This implementation is called "*noncompromise-resilient link layer security*" and is part of Contiki[2]. It is implemented on top of the IEEE 802.15.4 MAC[1]. This link layer security offers several stages of encryption and authentication. In this demo, it is used to encrypt all packets sent via the radio interface.

[1] http://www.contiki-os.org

[2] https://github.com/contiki-os/contiki/tree/master/core/net/llsec/noncoresec

International Conference on Embedded Wireless Systems and Networks (EWSN) 2018
14–16 February, Madrid, Spain

ISBN: 978-0-9949886-2-1

4 The Hardware Setup

The hardware setup in this demo consists of two Zolertia Z1 node[3] each connected to an inexpensive mfrc522 RFID reader[5]. Node and reader are connected via the SPI interface. For the configuration, MIFARE Classic 1 KB RFID tags[6] are used. One of these nodes with the RFID reader and two RFID tags – one in the card and one in the coin format – are shown in Figure 1.

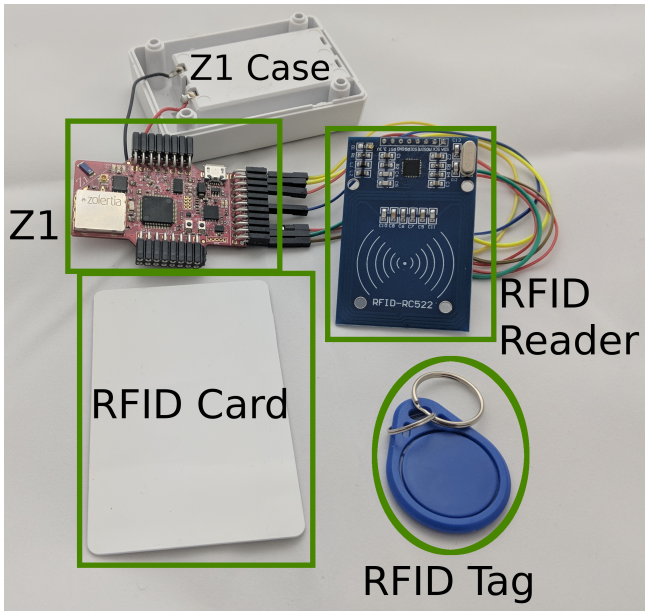

Figure 1. The hardware setup: The RFID reader is connected to the Z1 sensor node using jumper wires. RFID tags are used to configure the Z1 node.

5 The Software

The software in this demo consists of two parts: The driver and an example application. The first one offers an interface to access the content of an RFID tag, the latter uses this data to configure the node accordingly. Both are available as a pull request to the Contiki GitHub repository[4].

5.1 The RFID Driver Module

The driver module handles the access to the content of an RFID tag using the mfrc522 reader connected via SPI to the Z1 node. In case of the Z1, the SPI bus is shared with the radio interface. Hence, the driver has to ensure that it does not effect the communication with the radio interface. Using this driver, an arbitrary part of an RFID tag can be accessed and read out. This allows to retrieve and use a variety of parameters from an RFID tag.

5.2 The Example Application

The application for the evaluation of the system is based on the *simple-rpl-udp* example[5] delivered with Contiki. It sets the encryption key for the link layer security and performs the following steps on the node after reset or enabling the power supply:

- If a tag is available: Read out the key from a defined position of the tag. Store it in the flash of the node to be available after reboot.
- If no tag is available: Check whether a tag is available in the flash and use it. Otherwise, use a default key.
- Set the key for the link layer security and continue the normal boot.
- Transmit packets between the nodes.

Using this application, the user can set the key on nodes following these steps:

1. Hold an RFID tag close to the RFID reader of the sensor node.
2. Press the reset button on the node to trigger a readout.
3. Wait four seconds and remove the tag from the node.

Afterwards, the node will transmit encrypted data using the key read from the tag. This proceeding drastically eases the setting and changing of the configuration in WSNs. A demonstration video of the system can be found on Youtube[6].

6 Conclusions

In this demo, a new approach for key and configuration distribution in wireless sensor networks based on RFID tags is shown. In contrast to classical systems, this idea offers several advantages. First of all, the usage is easy as everything is configured by holding an RFID tag close to the sensor node for a couple of seconds. Secondly, no electrical connections are required and completely sealed casings can be used. Thirdly, no encryption keys are transmitted via the wireless sensor network.

7 References

[1] IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pages 1–314, Sept 2011.

[2] J. Daemen and V. Rijmen. AES proposal: Rijndael. 1999.

[3] K. Finkenzeller. *RFID Handbook Fundamentals and Applications In Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition*. Wiley, Chichester, 2010.

[4] K.-F. Krentz, H. Rafiee, and C. Meinel. 6LoWPAN Security: Adding Compromise Resilience to the 802.15. 4 Security Sublayer. In *Proceedings of the International Workshop on Adaptive Security*, page 1. ACM, 2013.

[5] NXP Semiconductors, Hamburg, Germany. *MFRC522 Standard Performance MIFARE and NTAG frontend Datasheet*. Rev. 3.9.

[6] NXP Semiconductors. *NFC Type MIFARE Classic Tag Operation*. Rev. 1.3, AN1304.

[7] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, June 2004.

[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security: A survey. *Security in distributed, grid, mobile, and pervasive computing*, 1:367, 2007.

[3] https://github.com/Zolertia/Resources/blob/master/Z1/Hardware/Revision C/Datasheets/Zolertia Z1 datasheet Revision C.pdf

[4] https://github.com/contiki-os/contiki/pull/2084/

[5] https://github.com/contiki-os/contiki/tree/master/examples/ipv6/simple-udp-rpl

[6] https://youtu.be/FZiLjATBjj8