Semi-Passive RFID Development Platform for Implementing and Attacking Security Tags

Thomas Plos, Manfred Aigner, Thomas Baier, Martin Feldhofer,
Michael Hutter, Thomas Korak, Erich Wenger
Institute for Applied Information Processing and Communications
Graz University of Technology
Inffeldgasse 16a, 8010 Graz, Austria

Abstract

In the last few years RFID technology has become a major driver of various businesses like logistics, supply-chain management, and access control. Many of these applications base on the successful implementation of security services on the RFID tag side but also on the reader side. In this paper we present an efficient tool for early prototype implementations of RFID applications. We show how the developed semi-passive RFID tags can help implementing and attacking security-enhanced RFID systems. The shown microcontroller-based and FPGA-based tag platforms can operate in the HF and the UHF range. They are very flexible in terms of functionality and support different communication standards like ISO 15693, ISO 14443, and ISO 18000-6C (EPC Gen2). Its main applications are in developing hardware prototypes of passive tags, extending RFID protocols with security functionality, and for attacking real RFID devices with side-channel analysis.

1. Introduction

Radio-Frequency Identification (RFID) is an emerging technology that becomes more and more popular. One major roadblock of this technology for its expected exponential growth is that until now an elaborated security concept is missing. Many proposals for security protocols and hardware implementations of cryptographic hardware extensions have been published. For most of them a proof of concept, which provides evidence that the proposer's assumptions fulfill the requirements of the technology was not given. Often, the suggested solutions are not compatible with the given throughput, latency or power requirements of existing RFID tags and communication standards. In many cases it is simply too expensive to build up a prototype consisting of a reader and tags due to the arising costs for dedicated tag and reader development.

Extending the functionality of RFID systems (e.g. with security features) and verifying their correct operation (e.g. withstanding certain attacks) is often a labor-intensive task. Commercially available passive RFID tags are typically implemented as dedicated hardware circuits and cannot be modified after production. Simulation of the contact-less communication protocol is difficult due to the demanding physical characteristics of those interfaces, especially when a high number of tags within the reader field is considered. Prototyping of new suggestions for RFID communication between tags and readers was therefore often skipped, which lead to reduced visibility of security-oriented research in the RFID community.

Our semi-passive tags (in the following also named DemoTags) are a platform that closes this gap. They are programmable and highly flexible, but appear to a reader like fully passive tags. They are an ideal prototyping tool for efficiently integrating new functionality into currently existing RFID and Near Field Communication (NFC) systems.

The DemoTag's firmware provides the implementation of the core functionality of several interface standards (ISO 15693, ISO 14443, NFC, EPC Gen2, etc.) in a way that it can be efficiently extended on basis of custom commands and dedicated subroutines for new extended functionality. The firmware framework provides flexible mechanisms to execute the additional functionality of the tags by sending custom commands, and provide the computed data to the reader via standardized frames. For prototype implementation the developer can therefore concentrate on the new features, rather than spending valuable resources into re-developing existing functionality.

In the following sections, we provide details about the architecture and components of four different DemoTag platforms. Two versions use a programmable microcontroller for extension by modification of their firmware. They differ in the used frequency range for communication with the reader, which are high frequency (HF) and ultra-high frequency (UHF) range. The other two platforms use

an FPGA to enable extension of the functionality on basis of digital hardware-design methods. The two platforms with the FPGA also differ in the used frequency range for communication (HF and UHF). Additional external sensors can be attached to all versions of the DemoTag. In difference to other published platforms with similar characteristics [1, 2, 3], the DemoTags are available for research purposes without any restrictions. They completely implement the mandatory functionality of the communication standard. Therefore, the DemoTags allow more flexibility for selection of the reader platform for prototyping.

After the architecture descriptions, we shortly present seven typical applications of the DemoTags. The first application presents how they can be efficiently used in the development process of RFID tags with additional functionality. The second project deals with development and evaluation of protocol extensions. The third use case illustrates how the DemoTags were used to develop an analysis setup for so called side-channel analysis (SCA) attacks on RFID tags. As fourth scenario we present a practical realization of an RFID relay attack on the ISO 14443 protocol, followed by an example implementation of Linux on a DemoTag. The last two scenarios deal with the usage of the prototype platforms in the Internet of Things and as NFC-Forum Type-4 compliant tags. We finalize our paper with conclusions we have drawn from developing and using the DemoTags in research projects towards secure RFID technology. So far, they turned out to be a very powerful tool for prototyping and evaluation. Additionally, we think that they can be useful during development, testing, and evaluation of new RFID-reader products.

2. Architecture Description of the DemoTags

The prototype tags are powered by a battery, but behave like fully passive tags in the reader field. We designed four devices. Two microcontroller-based devices, one for the HF range and one for the UHF range. Furthermore, we have two FPGA-based solutions (one for the HF and one for the UHF range). The tags, we call them DemoTags, are fully compatible to widely deployed RFID standards such as ISO 15693 [4], ISO 14443-A/B [5], and NFC [6] (HF range); or ISO 18000-6C/EPC Gen2 [7] (UHF range). The semi-passive tags mainly consist of an antenna which is directly integrated into the printed circuit board (PCB), an analog front-end, and a programmable device which is either a microcontroller or an FPGA. The devices provide additional communication interfaces like RS232 or USB to communicate with a PC in addition to the radio frequency (RF) link.

The prototype tags are designed for easy extension of their functionality. By using a special tool chain, custom commands and additional functionality can be integrated into the firmware/hardware of the microcontroller/FPGA with little effort. We have already used the microcontroller/FPGA-based prototype tags in several research projects for various applications, for example: detecting weaknesses in a parking access-control system, integrating strong cryptography to RFID protocols, testing and evaluating the digital hardware design of an RFID tag, conducting side channel and fault attacks on commercially available RFID tags, realizing RFID relay attacks, and demonstrating new security features for NFC systems. There are many other applications in which such programmable tags are indispensable, like verifying reader functionality and reader prototypes, evaluating reader-to-tag communication and RFID teaching. We have access to reader platforms operating in the HF and the UHF range, which allow an extension of the underlying protocols easily for prototype development. Moreover, sensors and actuators can be attached to the tags as well. In the following we first describe the two DemoTags with the microcontroller and then we show the two FPGA DemoTag platforms.

2.1 DemoTags with Microcontroller

An architectural overview of the two microcontroller-based tag prototypes can be seen in Figure 1. The HF prototype operates in the frequency band at 13.56 MHz and the other prototype works in the UHF frequency band at 868 MHz. Both devices have been assembled using discrete components which may result in reduced reading distance compared with commercial front-end chips, but allows for unrestricted use and later publication of the results. They consist of an antenna, an analog front-end, a microcontroller, a serial interface, a JTAG programming interface, and a power-supply connector. Both devices differ mainly in their antenna design, the analog front-end, and the software that runs on the microcontroller. The remaining components are the same. An ATXMega256 microcontroller [8] is used, which manages reader requests and tag responses, as defined in the specification of the selected RF communication protocol. The microcontroller connects with a PC over a serial interface. Furthermore, it supports in-system programming and on-chip debugging via a Program and Debug Interface (PDI) and a JTAG interface. Both devices are semi passive; the controller is powered by an external power source, typically a battery or via the USB port, while the RF communication is done passively without any signal amplification.

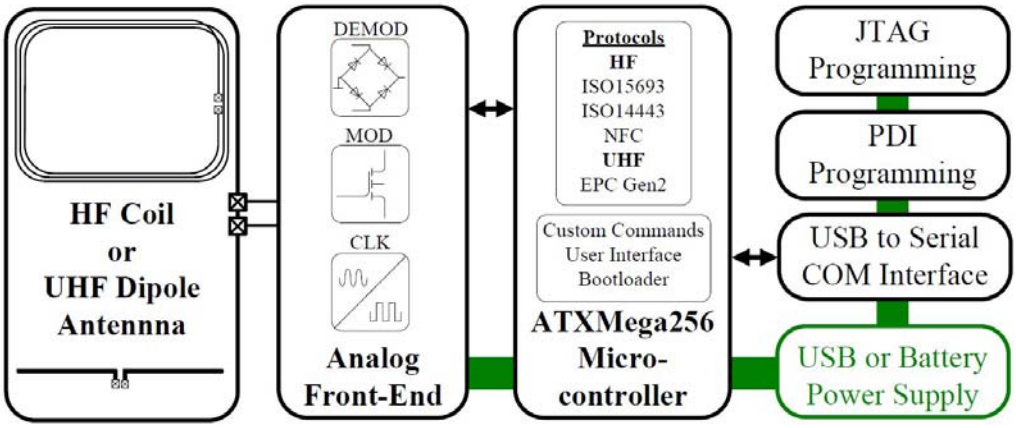

Figure 1. Architecture of HF and UHF microcontroller DemoTags.

The flexibility of the tag prototypes is provided by the support of different communication standards for the RFID interface. During our research in the area of RFID security we used them in very different applications. First, they proved useful during the evaluation of security holes in RFID systems. It is possible to easily reproduce published attacks like the one against the MIFARE classic protocol [9]. Prototyping solutions like the blocker tag [10] against privacy threats are easily possible. Testing custom commands for additional functionality is useful for the proof of concept but also for testing reader devices. In addition to simple functional tests, more sophisticated features like conformity to a certain standard and the correct error handling are possible which is difficult with commercially available tags that are not programmable. Finally, the DemoTags are perfectly suitable for conducting implementation attacks as shown by Hutter et al. [11] and Plos [12]. For such attacks it is often necessary to find a trigger point in the communication protocol to start power-trace measurements. In the following sections, the design of the HF and the UHF tag prototypes and their applications are described in a more detail.

2.1.1. HF DemoTag. The HF tag prototype uses a self-designed antenna according to ISO 7810 that is placed directly on the PCB. It consists of a coil with four windings that allows the communication with a reader over the air interface. The antenna is tuned to resonate at a carrier frequency of 13.56 MHz, which is realized by a matching RLC circuit. This circuit narrows the frequency range and can also be considered as a band-pass filter that passes the carrier frequency but attenuates unwanted and spurious frequencies. The analogue front-end preprocesses the received signals and transforms them into the digital domain. First, it rectifies signals using a bridge rectifier. Small-signal Shottky diodes assure low voltage drops and low leakage currents in the front-end. After that, a Zener diode limits the voltage. At the third stage, a comparator identifies the reader's amplitude-shift keying (ASK) modulations. The microcontroller samples the output of the comparator by triggering an interrupt to start the receiving process. A 13.56 MHz quartz crystal is placed on the board to clock the microcontroller. For sending data from the tag to the reader, a load-modulation circuit is available that consists of a shunt and a transistor. The microcontroller triggers the transistor that switches the shunt and thus modulates the tag response. The tag prototype can communicate using several protocol standards. It implements ISO 15693 [4], ISO 14443 [5] (type A and B), ISO 14443-4 and ISO 18092 [6] (NFC). The firmware is mainly written in C while some parts have been implemented in assembly language due to timing constraints. Moreover, it implements a user-command interface that allows easy administration over the serial interface. In Figure 2 (top), a picture of the HF DemoTag is shown. The coil antenna occupies the right half of the board while the discrete components of the analog front-end are placed on the other half. The ATXMega256 microcontroller is placed on a separate board that can be plugged on

Figure 2. Photo of HF DemoTag (top) and UHF DemoTag (bottom).

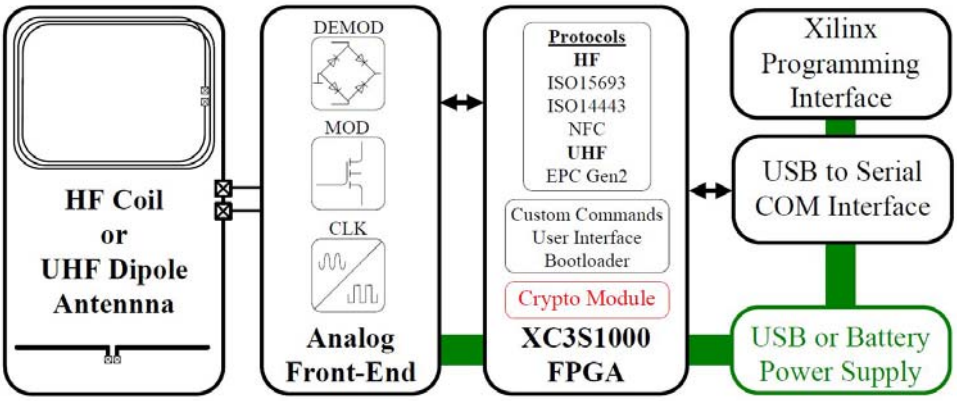

Figure 3. Architecture of the HF and UHF FPGA DemoTags.

top of the motherboard. This microcontroller board provides a special interface that allows attaching additional adaptors like memory or Bluetooth modules.

2.1.2. UHF DemoTag. The second microcontroller-based prototype operates in the UHF band. In contrast to the HF DemoTag it uses a half-wave dipole antenna consisting of two wires directly integrated to the layout of the PCB. The antenna, with a length of about 150 mm, is optimized for a frequency of 868 MHz and it is connected to the analog front-end. Similar to the HF version, an adjustable capacitor is placed in parallel to its antenna. This capacitor is used for matching the antenna to the input impedance of the analog front-end. Signals that are received by the antenna are first rectified by a charge-pump rectifier. This rectifier performs demodulation and voltage multiplication all at once. For the rectifier circuit we use special detector diodes, which have a low voltage drop and which are constructed to operate up to some GHz. Subsequently, signals are filtered and passed to a comparator before feeding them to the microcontroller. The backscatter-modulation circuit of the front-end performs the tag-to-reader communication. It works similar to the one used by the HF tag prototype, using a transistor to switch an impedance (shunt and capacitor) in parallel to the tag antenna. A 16 MHz quartz crystal is assembled on board in order to generate the system clock for the microcontroller. The UHF DemoTag supports the ISO18000-6C standard (EPC Gen2 [7]) which is the most widespread protocol in the UHF range. The protocol execution is programmed in software on the microcontroller. The firmware for the UHF tag prototype is mainly written in C with time-critical elements realized in fully optimized assembly code. Figure 2 (bottom) presents a picture of the UHF DemoTag. The dipole antenna is visible on top of the board while the ATXMega256 microcontroller board covers parts of the circuitry of the analog front-end.

2.2. DemoTags with FPGA

The latest development in the series of DemoTag prototype platforms are the HF and UHF FPGA DemoTags. A powerful development platform for implementation of the digital part of a real passive RFID tag is the main reason for this research work. Figure 3 presents the architecture of the FPGA DemoTags.

The motherboard of both the HF and the UHF FPGA tag are identical to the ones used by the microcontroller-based DemoTags. Hence, only the microcontroller board is replaced with a corresponding FPGA board. This underlines the flexibility of our development platform. The HF FPGA DemoTag can be configured to directly use the 13.56 MHz carrier signal extracted from the reader field as clock source for the FPGA (instead of the on-board clock signal). This allows testing the digital hardware part under the same conditions as in a real RFID tag. We use the Spartan-3 XC3S1000 [13] FPGA from Xilinx as programmable device, which provides a simple package footprint, is available for low cost and features reasonable hardware resources. This FPGA includes 17 280 logic cells, each of it consisting of a 4-bit look-up table, and a flip flop. Additionally, it provides 24 RAM blocks with up to 432 Kbits. Furthermore, it has four digital clock-manager circuits and dedicated multipliers, which are useful for the implementation of computational-intensive cryptographic operations.

On this FPGA we can implement the complete digital part of a passive RFID tag. This includes the protocol execution, the implementation of custom commands as well as the user interface via a serial port. It is also possible to attach sensors and actuators to its I/O ports. The main application of this platform is demonstrating early prototypes of security-enhanced passive RFID tags in the industry and in the academic community. We can demonstrate the integration of cryptographic functionality into standard tag hardware.

Configuration of the FPGA works via the USB interface or with a dedicated programming cable from Xilinx. The power supply comes from a battery or from the USB interface. In addition to tag prototyping, time-critical attack scenarios are also of interest for the FPGA DemoTag. With the support of specialized hardware it is easier to fulfill given timing constraints, which is for example relevant for relay attacks. A photo of the HF and the UHF FPGA DemoTag is presented in Figure 4. The FPGA DemoTags look similar to the microcontroller-based DemoTags—instead of a microcontroller board, the FPGA is connected to the motherboard.

Figure 4. Photo of HF FPGA DemoTag (top) and UHF FPGA DemoTag (bottom).

3. Application Scenarios

The following seven scenarios present typical applications where we used our developed DemoTags. The application domain is in most cases very restricted to security-related activities, but the prototype tags can be used also in many other areas.

3.1 Scenario 1: Development of Passive RFID/NFC Tags

The FPGA DemoTag has two major advantages. First, it provides an efficient platform for application-specific integrated circuit (ASIC) prototyping. It can be used to evaluate and test digital hardware designs of an RFID-tag implementation. By prototyping, both the development time and the risk of implementation failures can be significantly reduced. Second, it can be ideally used as a proof-of-concept demonstrator for new implementations and future RFID applications. Hutter et al. [14] proposed a hardware processor for passively powered RFID/NFC tags that can be easily synthesized on the FPGA DemoTag. In particular, the processor is able to compute digital signatures using the Elliptic Curve Digital Signature Algorithm (ECDSA). It consists of a tiny microcontroller, a memory unit, and an arithmetic-logic unit (ALU) to sign a digital message within 859 188 clock cycles, i.e. 127 ms at 6.78 MHz. Note that the design uses the internal Block RAMs of the FPGA as memory (RAM, ROM, and EEPROM) to reduce the number of needed LUTs. Together with the processor, a digital RFID front-end is implemented that is able to send and receive ISO 14443-A and ISO 7816-4 commands. The digital front-end module implements an 8-bit microcontroller to handle the commands and to provide NFC compatible and application-specific functionalities. On the one side, the microcontroller is connected to the ECDSA processor to support cryptographic operations. A 16-bit AMBA interface is used as a bus architecture. On the other side, two I/O pins of the FPGA allow a connection between the synthesized digital front-end and the discrete analog front-end of the FPGA DemoTag. After configuration of the FPGA, the DemoTag can be used as a conventional RFID/NFC tag and it can be challenged and evaluated by a reader device to perform cryptographic operations.

3.2 Scenario 2: Development of Protocol Extensions

A very interesting application scenario for all four types of DemoTags is the development of protocol extensions for a given RFID standard. This includes features like sensing data but especially in our case security extensions are of capital importance. With these extensions it is possible to support certain security services in passive RFID systems. For example, Dominikus et al. [15] extended the ISO 18000-3 standard with symmetric challenge-response authentication protocols according to ISO 9798-2. With the HF DemoTags it was possible to show how these protocols work in a real RFID application environment. In [16], Aigner et al. have presented a similar extension for the ISO 18000-6C standard (EPC Generation 2). There, UHF DemoTags have been deployed to demonstrate the feasibility of security-related protocol extensions in a real application. In very time-critical protocols like distance-bounding protocols [17] an early prototype is also very important because it can be shown whether the timings can be fulfilled by the tag and the reader. Furthermore, a concurrent development of tags and readers is possible when an already functioning reference demonstrator is available.

3.3 Scenario 3: Conducting Implementation Attacks against Passive RFID Tags

The proposed prototypes can be used to analyze the security of implementations against several attacks. Power and electromagnetic side-channel attacks represent the most powerful attacks against passive RFID tags [11]. In such attacks an adversary measures the power consumption or the electromagnetic (EM) emanation of the tags with

appropriate measurement setups. In Hutter et al. [18], two different HF RFID prototypes are used to perform such attacks on a software and hardware implementation of the Advanced Encryption Standard (AES). They successfully revealed the secret key by using less than 1 000 measured EM traces.

In [12], the EM emanation of the UHF prototype is measured. The emissions are gathered with special near-field probes that are placed close to the microcontroller of the prototype. Less than 200 measured EM traces are enough for successful attacks. Moreover, the UHF prototype has been used to enable remote side-channel attacks on commercially available passive UHF tags. For this attack scenario the prototype tag has been placed together with the passive tag inside the reader field. The prototype has been used to listen to the communication between reader and tag and provided appropriate trigger signals for measuring the EM emanation of the passive tag. This has allowed conducting remote side-channel attacks on passive UHF tags at distances up to 1 m with less than 10 000 traces.

The prototypes can also be used to analyze the impact of fault attacks on RFID. Fault attacks manipulate the device to provoke faulty computations. The faulty results are then used to extract secret information. In [19], Hutter et al. analyzed the impact of fault attacks on RFID. They demonstrated the vulnerability of passive RFID tags to electromagnetic interferences, optical inductions, and antenna-tearing attacks. The prototypes have been used to precisely trigger the injection of a fault. Especially, they have allowed performing automatic fault-injections sweeps where duration and point in time of the fault injection is varied over a certain range. Such fault-injection sweeps are very practical when only little information about the attacked RFID tags is available

3.4 Scenario 4: Performing RFID Relay and Eavesdropping Attacks

Another scenario where the tag prototypes can be used is evaluating the thread of RFID relay and eavesdropping attacks. Relay attacks are man-in-the-middle attacks which relay data over a longer distance from a tag to a reader [20]. In such a scenario, the DemoTag acts as a proxy token that receives and forwards data from a genuine reader to a proxy reader. The proxy reader, however, sends the data to a genuine tag, pretending to be the genuine reader in the proximity of the tag. In the work of Issovits et al. [21] the HF DemoTag has been used to perform practical relay attacks on the ISO 14443-A protocol. For this purpose a special adaptor board with a Bluetooth module has been designed. This adaptor board is plugged on top of the HF DemoTag's microcontroller board that provides a special interface for attaching additional adaptors, as shown in Figure 5. The Bluetooth module supports data rates up to 3 Mbps and is accessed through the Universal Asynchronous Receiver Transmitter (UART) interface of the microcontroller. The Bluetooth connection is used as relay channel between the HF DemoTag (proxy token) and a Nokia 6212 NFC mobile phone (proxy reader). The ability to attach a separate adaptor board underlines the flexibility of the prototype platform.

Also eavesdropping attacks can be performed using the prototypes by simply putting the prototype into the field of the reader. For this attack, the DemoTag operates in *silent mode,* which means that it does not respond to reader requests but simply monitors the transmitted data. An adversary can easily recover the data sent from a reader to a tag, as practically shown by Hancke in [22].

Figure 5. Photo of HF DemoTag with a Bluetooth adaptor board attached to the microcontroller board.

3.5 Scenario 5: Linux-Capable RFID Tags

Nowadays, Linux is installed on a magnitude of devices. Maybe in the (more distant) future Linux is also running on an RFID tag. However, already today we are able to use our FPGA DemoTag from Section 2.2 to build our own RFID tag running Linux. In order to achieve a working platform for Linux, it is necessary to extend the Spartan-3 module with external SD-RAM and Flash. Within the Spartan-3 module there are not enough resources available. By taking advantage of the extension interface of the FPGA board, an adaptor board with SD-RAM and Flash is connected to it. The logic within the FPGA can be separated in the following parts: a 32-bit Microblaze processor, a Multi-Port Memory Controller (MPMC), a hardware framing logic, and a serial port. The MPMC in connection with a clock generator is used to make the external memories accessible. The hardware framing logic is needed to interface the analog front-end. Internally, this component is accessed via a dedicated address range of the Processor Local Bus (PLB) and a custom Linux driver. The serial port is used to print debug statements and controls the running application.

3.6 Scenario 6: A Prototype for the Future Internet of Things

The DemoTags can be also used as prototyping platforms for the future Internet of Things. The term "Internet of Things" was first used by Kevin Ashton in 1999 where he linked the idea of RFID used in supply chains to the open Internet. Nowadays, the Internet is a network of computers that share information that is gathered by human beings. Any data that is found in the World Wide Web (WWW) has been captured and entered by people. The next step in this development would be a network of objects which allows autonomous gathering of information from their environments. These objects will have their own Internet Protocol (IP) address and are therefore addressable and identifiable over the Internet.

For a proper realization of the Internet of Things, the DemoTags can be equipped with different sensors. These sensors can measure the environmental temperature, light density, 3D acceleration, blood pressure, or other properties from objects in the proximity. The sensors can be assembled on adapter boards and they can be accessed by the microcontroller or FPGA of the DemoTag. Furthermore, appropriate RFID-network protocols are needed that support the access of tags from the Internet. Dominikus et al. [23] presented a way how to communicate with such tags using Mobile IPv6 technology. Each tag gets an own IPv6 address and is able to establish a secure communication channel using asymmetric cryptography [24].

A platform, which provides similar features, has been presented by Intel Research Seattle. They started a project in 2005 (in cooperation with the University of Washington) where they designed and developed a Wireless Identification and Sensing Platform (WISP) [25]. There exist several publications that make use of that platform to demonstrate sensing and monitoring applications [26, 27].

3.7 Scenario 7: The DemoTag as NFC-Forum Compliant Tag

In the presented scenario we use the HF DemoTag to act as an NFC-Forum Type-4 compliant tag. As a result NFC-Forum devices can exchange NFC Data Exchange Format (NDEF) messages with our prototype tag. The NFC Forum is a cooperation of companies with different fields of activities. The goal of this cooperation is to enforce the usage of NFC technology in electronic devices. According to the specification in [28] a Type-4 compliant tag must maintain a file system with at least two files. Furthermore, three commands have to be supported: select, read, and update. With the select command a specific file can be selected. In a second step the selected file can be read using the read command or modified using the update command. An NDEF message consists of one or more NDEF records. The purpose of these records is to enable an application to encapsulate several related documents into them, which can be transmitted to another device or temporarily stored on a tag (DemoTag). We used an NFC-enabled smartphone (Google/Samsung Nexus S) as NFC-Forum reader device.

Without installing a specific application on the smartphone it is possible to read the NDEF message stored on the DemoTag. The communication process starts by bringing the smartphone and the prototype close together (touch & go). In our scenario the NDEF message contains two records. Each record holds an URL that can be opened with the browser on the phone as it can be seen in Figure 6. For developing NFC applications on smartphones, it is convenient to have a flexible and quickly reconfigurable tag. The test of the application can be conducted with low effort.

During the development of reader applications, it showed that the DemoTag can effectively help in identifying communication problems and non-conformities of RFID standards. Furthermore, it helps in debugging and allows implementing workarounds in reader applications. The reader manufactures can then be informed to solve the issue.

Figure 6: Photo of a smartphone reading an NDEF message from the DemoTag.

4. Conclusions

In our work, we showed the implementation of four semi-passive RFID tag prototypes that are programmable either via a microcontroller or an FPGA. In addition to supporting the common RFID standards ISO 15693, ISO 14443, and NFC for the HF range and the ISO 18000-6C (EPC Gen2) for the UHF range, the prototyping tags allow extending the functionality. We showed how the presented

DemoTags are used in seven different application scenarios. The first showed how the DemoTags are used for the hardware development of passive RFID tags with security functionality. The second scenario depicted the use in extending existing RFID protocols with security services. The third application scenario presented the usage in analyzing the security of implementations against side channel and fault attacks. As fourth use case we illustrated the application of the prototypes for RFID relay and eavesdropping attacks, followed by a scenario where Linux is running on an FPGA DemoTag. The last two application scenarios presented the usage of our prototype platforms within the Internet of Things and as NFC-Forum Type-4 compliant tag. Future work consists of enhancing the latest research prototype, the FPGA DemoTag, with hardware libraries for the most common RFID standards and a comparison of the FPGA DemoTag with a real RFID tag.

10. References

[1] M. Lehtonen, A. Ruhanen, F. Michahelles, and E. Fleisch. "Serialized TID numbers - A headache or a blessing for RFID crackers?". *In IEEE International Conference on RFID (IEEE RFID 2009), Orlando, Florida, USA, April 27-28, 2009, Proceedings*, pages 233–240, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.

[2] M. Rieback, G. Gaydadjiev, B. Crispo, R. Hofman, and A. Tanenbaum. "A Platform for RFID Security and Privacy Administration". *In 20th USENIX/SAGE Large Installation System Administration Conference, Washington DC, USA, 3-8 December, 2006, Proceedings*, pages 89–102. USENIX, 2006.

[3] D. J. Yeager, A. P. Sample, and J. R. Smith. "RFID Handbook: Applications, Technology, Security, and Privacy, chapter WISP: A Passively Powered UHF RFID Tag with Sensing and Computation", pages 261–278. CRC Press, 2008.

[4] International Organisation for Standardization (ISO). "ISO/IEC 15693-3: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards – Part 3: Anticollision and transmission protocol", 2001.

[5] International Organization for Standardization (ISO). "ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit(s) Cards - Proximity Cards", 2000.

[6] International Organisation for Standardization (ISO). "ISO/IEC 18092: Information technology – Telecommunications and information exchange between systems – Near Field Communication - Interface and Protocol", April 2004.

[7] International Organization for Standardization (ISO). "ISO/IEC 18000-6: Information Technology AIDC Techniques— RFID for Item Management – Part 6: Parameters for air interface communications at 860-960 MHz", 2004.

[8] Atmel Corporation. "8/16bit AVR XMEGA A3 Microcontroller". Available online at `http://www.atmel.com/dyn/resources/prod_documents/doc8067.pdf`, December 2010.

[9] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. "Dismantling MIFARE Classic". *In S. Jajodia and J. Lopez, editors, 13th European Symposium on Research in Computer Security (ESORICS 2008), Malaga, Spain, 6-8 October, 2008, Proceedings*, volume 5283 of Lecture Notes in Computer Science, pages 97–114. Springer Verlag, 2008.

[10] A. Juels, R. L. Rivest, and M. Szydlo. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". *In 10th ACM Conference on Computer and Communication Security, Washington, DC, USA, October 27-30, 2003, Proceedings*, pages 103–111. ACM Press, October 2003.

[11] M. Hutter, T. Plos, and M. Feldhofer. "On the Security of RFID Devices Against Implementation Attacks". *International Journal of Security and Networks 2010*, 5(2/3):106–118, 2010.

[12] T. Plos. "Susceptibility of UHF RFID Tags to Electromagnetic Analysis". *In T. Malkin, editor, Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008, Proceedings*, volume 4964 of Lecture Notes in Computer Science, pages 288–300. Springer, April 2008.

[13] Xilinx, Inc. "Spartan-3 FPGA Family Data Sheet", June 2008. Available online at `http://www.xilinx.com`.

[14] M. Hutter, M. Feldhofer, and T. Plos. "An ECDSA Processor for RFID Authentication". *In B. Ors, editor, Workshop on RFID Security - RFIDsec 2010, 6th Workshop, Istanbul, Turkey, June 7-9, 2010, Proceedings*, Lecture Notes in Computer Science. Springer, 2010.

[15] S. Dominikus, E. Oswald, and M. Feldhofer, "Practical Security for RFID: Strong Authentication Protocols". *In P. Horster, editor, Proceedings of D.A.C.H. Mobility 2006*, *October 17-18, 2006, Graz, Austria*, pages 187–200. Syssec, 2006. ISBN 3-00-019635-8.

[16] M.Aigner, T. Plos, M. Feldhofer, C. Floerkemeier, Y. Na, A. Ruhanen, S. Coluccini, T. Burbridge. "Report on first part of the security WP: Anti-Cloning Tag (D4.3.1)", 2008.

[17] G. Hancke and M. Kuhn. "An RFID Distance Bounding Protocol". *In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005), Athens, Greece, 5-9 September 2005, Proceedings*, pages 67–73. IEEE Computer Society, September 2005.

[18] M. Hutter, S. Mangard, and M. Feldhofer. „Power and EM Attacks on Passive 13.56 MHz RFID Devices". *In P. Paillier and I. Verbauwhede, editors, Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of Lecture Notes in Computer Science, pages 320–333. Springer, September 2007.

[19] M. Hutter, J.-M. Schmidt, and T. Plos. „RFID and its Vulnerability to Faults". *In E. Oswald and P. Rohatgi, editors, Cryptographic Hardware and Embedded Systems – CHES 2008, 10th International Workshop, Washington DC, USA, August 10-13, 2008, Proceedings*, volume 5154 of Lecture Notes in Computer Science, pages 363–379. Springer, August 2008.

[20] G. P. Hancke. "Practical Attacks on Proximity Identification Systems". *In IEEE Symposium on Security and Privacy (S&P 2006), Berkeley/Oakland, California, USA, 21-24 May, 2006, Proceedings*, pages 328–333. IEEE Computer Society, May 2006.

[21] W. Issovits, M. Hutter. "Weaknesses of the ISO/IEC 14443 Protocol Regarding Relay Attacks", *In Conference on RFID-Technologies and Applications – RFID-TA 2011, IEEE International Conference, Barcelona, Spain, September 15-16, 2011, Proceedings*, Barcelona, Spain, September, 2011.

[22] G. P. Hancke. "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID". *Journal of Computer Security, 19(2): 259–288*, 2011.

[23] S. Dominikus, M. Aigner, and S. Kraxberger. "Passive RFID Technology for the Internet of Things". *In International Conference for Internet Technology and Secured Transactions (ICITST), London, November 8-11, 2010*, pages 1–8, IEEE.

[24] S. Dominikus, S. Kraxberger, M. Aigner, and H. Gross. "Low-cost RFID Tags as IPv6 Nodes in the Internet of Things". *In Radio Frequency Identification System Security, pages 114–128*, IOS Press, 2011.

[25] Intel Research Seattle. "Wireless Identification and Sensing Platform", Available online at `http://wisp.wikispaces.com/`.

[26] A. Sample, D. Yeager, and J. Smith. "A Capacitive Touch Interface for Passive RFID Tags". *In IEEE International Conference on RFID 2009, Orlando, Florida, April 27-28, 2009*, Proceeding, 2009.

[27] N. Saxena and J. Voris. "Accelerometer Based Random Number Generation on RFID Tags". *In Workshop on Wirelessly Powered Sensor Networks and Computational RFID (WISP Summit), Berkeley, California, USA, November 3,* 2009.

[28] NFC Forum. "Type 4 Tag Operation Specification", April 2009. Available online at `http://www.nfc-forum.org`.

11. Acknowledgements

This work has been supported by the Austrian Government through the research program FIT-IT Trust in IT Systems (Project PIT, Project Number 825743).

