

IT security of electronic communication systems in smart textile products

Prof. Manuela Bräuning
Faculty of Engineering
Albstadt-Sigmaringen University
Albstadt, Germany
braeuning@hs-albsig.de

Désirée Göbel
Faculty of Engineering
Albstadt-Sigmaringen University
Albstadt, Germany
goebeld@hs-albsig.de

Prof. Holger Morgenstern
Faculty of Computer Science
Albstadt-Sigmaringen University
Albstadt, Germany
morgenstern@hs-albsig.de

Prof. Dr. Martin Rieger
Faculty of Computer Science
Albstadt-Sigmaringen University
Albstadt, Germany
rieger@hs-albsig.de

Nele Schäfer
Faculty of Engineering
Albstadt-Sigmaringen University
Albstadt, Germany
schaefern@hs-albsig.de

Tobias Scheible
Faculty of Computer Science
Albstadt-Sigmaringen University
Albstadt, Germany
scheible@hs-albsig.de

Abstract— The SEKT research project, which is supported by the Federal Ministry of Education and Research, systematically investigates the integration and IT security of electronic communication systems in smart textile products. The main objectives are the scientific investigation of the IT security of Smart Textiles, the transfer of existing security concepts and the development of secure, innovative prototypes. The knowledge gained will be used to derive guidelines for the further procedure and courses for the textile and clothing industry will be developed, which will ensure an intensive multidisciplinary and cross-sectoral transfer of know-how. This challenge is to be met by an interdisciplinary team of scientists and companies from the textile and clothing industry and information technology. The actual status will be presented within the presentation.

Keywords - Smart Textiles, IT Security, WiFi, Bluetooth, RFID

I. INTRODUCTION

The textile industry is one of the oldest industries in the world. In addition to the automation of the loom, the development of synthetic fibres was one of the greatest revolutions in the industry. Synthetic fibres have opened up a multitude of new possibilities in addition to classic clothing. The field of technical textiles has been on the advance in the last decades and has opened up a multitude of industries with product innovations.

Electronic components are integrated into textiles and trigger the next revolution in textile and clothing technology. These textile products with extended functionalities are summarized under the term Smart Textiles. Although the development of Smart Textiles has been going on for decades, their use in everyday life is still in its infancy and there are numerous definitions. In the following, Smart Textiles are defined as textile products that interact with their environment and can thus actively support the user. The terminology used in this paper is divided into intelligent textiles, so-called I-textiles, and textiles with integrated electronic components, so-called e-textiles.

For this research work we concentrate exclusively on the field of e-textiles and divide them into adaptable, integrated and modified integration levels.

A. Market evolution

From automated communication with a washing machine and intelligent anti-theft protection to vital-sign monitoring – technology has the ability to make textile products more intelligent and this way “smarter”.. [1, p. 4] [2]. The market for Smart Textiles products is a young and dynamic area. The Centre for European Economic Research (ZEW) expects the global market volume to have increased thirtyfold by 2030. According to the study, the greatest growth is expected in the medical, industrial, military and fashion sectors. [3, pp. 3-7]. This trend can also be deduced from some megatrends such as connectivity, new work, health and individualization. [4]. E-Textiles are examples of the Internet of Things, which is why IT security is becoming increasingly important.

B. Cybersecurity

The report “The situation of IT security in Germany 2018” by the German Federal Office for Information Security (BSI) states that the threat situation for IT attacks has intensified and the focus of attacks is clearly spreading. The Smart Home and IoT areas are now also among the targets for attacks (see Figure 1). Regarding IoTs cybersecurity it is particularly important because, due to its physical integration, IoTs can have a direct impact on people's lives and health. Smart Textiles are assigned to the Internet of Things category and are therefore also a potential target for attackers. However, IT security in this area has not yet been systematically researched. [5]



Fig. 1. Focus of attacks broadening [5, p. 50]

II. THE PROJECT SEKT

Therefore, the interdisciplinary research project SEKT of the Faculties of Engineering and Computer Science at the Albstadt-Sigmaringen University takes up this approach and intensively combines the fields of textile and clothing technology and IT security. The SEKT project systematically

investigates the integration and IT security of electronic communication systems in smart textile products and develops practical security concepts and smart demonstrators. This challenge is to be met by an interdisciplinary team of scientists and companies from the fields of textile and clothing technology and IT security between December 2018 and November 2021. In addition to three professors a team of three employees and twelve project partners – ranging from Start-Ups to associations to large enterprises – are involved. The core objective is the scientific investigation of the area of IT security of smart textile products and the transfer of existing security concepts as well as the development of secure, innovative prototypes.

The project is divided into the following five phases:

- Investigation of current system solutions via survey and analysis of the latest product developments
- Examination of specific systems with which the integration of the electronic components into the textile products is evaluated as well as the safety concepts used are investigated.
- Development and adaptation of practice-relevant IT security concepts to smart textiles products
- Development, design and manufacture of three selected smart demonstrators
- Knowledge and technology transfer through guidelines and a teaching module in the blended learning process.

At the moment we are in phase two of the project and can already present some results from the survey and application scenarios as well as first hacked products.

A. Use of communication technologies in Smart Textiles products

Whilst conducting a market overview and a survey, the focus was to find out which wireless communication technologies are used most. When a transmission of data takes place, this is relevant for IT security. Since an attacker does not have to have direct access to the product, this is also the most likely attack scenario. The following Figure 2 shows the distribution of different technologies in different categories.

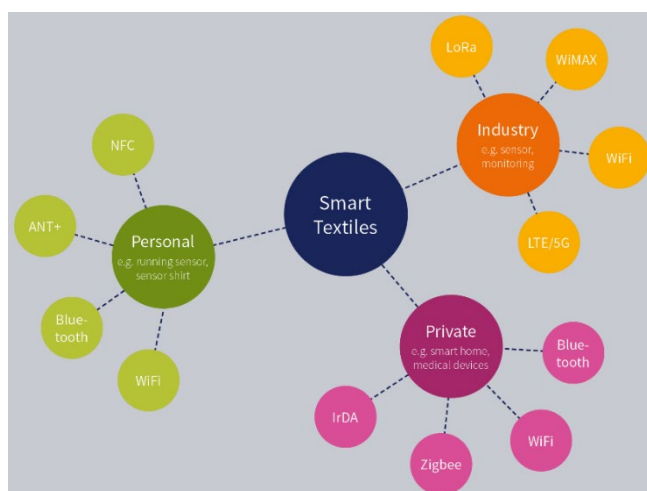


Fig. 2. Distribution of technologies in personal, private and industrial applications.

First attack possibilities and a hacked product are presented before an in-depth analysis of these most frequently used communication technologies is carried out. Performing this, we

will use well established methods as e.g. penetration testing in general and communication capturing followed by deciphering and replay attacks in particular. We will develop functional prototypes fulfilling as well a reasonable functionality as a good IT security. This will result in a recommendation as to which protocols should be used for safeguarding the individual technologies. An important part of this will be how to ensure systematic verification of compliance with the requirements through the textile companies that have purchased these components.

III. CONCLUSIONS

The IT security of electronic components in textiles and clothing products will become a new field; especially in the field of Smart Textiles an enormous development is predicted in the near future. As an interdisciplinary project, SEKT combines these two innovative areas of textile and clothing technology and information technology, thus creating the basis for future innovative product developments. It has been shown that wireless transmission methods are the most important key points for IT security. Effective protocols exist for all technologies to secure communication. However, the available safety methods must also be activated and applied correctly. Therefore, the verification of the mechanisms used is one of the most important factors.

ACKNOWLEDGMENT

The Federal Ministry of Education and Research (BMBF) funds interdisciplinary research and development projects in which universities of applied sciences cooperate with partners from industry and science. The current research project SEKT (funding code FKZ:13FH180PX6) is the first research team to focus on evaluating the cyber security of electronic communication systems in smart textile products. The project started in December 2018 and will last until November 2021. The project team works with well-known brands with backgrounds in textiles from different areas such as fashion, sports, military or medicine and cooperates with various partners from the IT sector. In addition, the group cooperates with various associations and the universities of Erlangen-Nuremberg and Hamburg – a consortium of 12 partners is involved. The SEKT project is funded by the FHprofUnt2016 initiative with approx. 500,000 Euros.

REFERENCES

- [1] Gesamtverband der deutschen Textil- und Modeindustrie e.V., „Mit jeder Faser intelligent - 2017: die deutsche Textil und Modeindustrie in Zahlen,“ Gesamtverband der deutschen Textil- und Modeindustrie e.V., Berlin, 2017.
- [2] Gesamtverband textil+mode, „Textilindustrie für ein starkes Europa,“ Gesamtverband textil+mode, 02 04 2019. [Online]. Available: <https://www.textil-mode.de/presse/detailseite/news/textilindustrie-fuer-ein-starkes-europa>. [Zugriff am 14 04 2019].
- [3] D. J. Ohnemus und D. F. Rasel, „FashionTech – Smart Textiles: Kurzexpertise im Auftrag des BMWi,“ ZEW - Zentrum für Europäische Wirtschaftsforschung GmbH, Mannheim, 2018.
- [4] Zukunftsinstitut GmbH, „Megatrends,“ 2018. [Online]. Available: <https://www.zukunftsinstitut.de/dossier/megatrends/>. [Zugriff am 14 04 2019].
- [5] Federal Office for Information Security (BSI), „The State of IT Security in Germany 2018,“ Federal Office for Information Security (BSI), Bonn, 2018.

