Zukunft Bau

SHORT REPORT

Title

Reduction of usability hurdles for the use of effective security mechanisms in the building automation of the future

Occasion / Starting Point

Networked building automation systems (BA) are increasingly integrated into public networks. However, these systems are exposed to a dramatically higher risk potential in public networks. The aim of this research project was to reduce usability barriers for security mechanisms, so that their establishment in terms of planning, installation and maintenance can be consistently implemented and made more economically attractive.

Subject of the Research Project

As part of this project (figure 1), safety aspects in building automation (BA) systems were examined in more detail. It addressed five hurdles in implementing security:

1. Lack of awareness and resulting low demand
2. Unknown security mechanisms and uncertainties regarding their benefits
3. Reservations regarding security mechanisms with regard to the extra work involved
4. Missing tools for risk assessment of BA systems
5. Initial safe and comfortable configuration of systems

In a first step, a brief overview about goals and areas of information security in general and building automation systems in particular was given (figure 2). Primarily, an awareness of security should be created. The reader is able to identify protection goals and risks in the operation of BA systems (figure 3). In addition, it should be encouraged to occasionally take the viewpoint of different attackers in the planning phase of BA systems and thus to detect weaknesses.

Subsequently, the state of the art was comprehensively analyzed and systematically evaluated with regard to risks and safety mechanisms. The goal was to educate about security measures of currently available protocols. This information serves as a tool to use currently available security mechanisms effectively. In addition, this part gives an insight into current research in this area. For the reader without a technical background, a guide was developed that briefly summarizes the results and includes the most important decision-making aids. For the providers of BA systems, it pays to take a closer look at the details in order to make better use of the possibilities of the individual technologies.

The subsequent work tries to provide impulses and ideas on how to make the application of security easier in the future.

The threat analysis of building automation systems through the use of the Building Information Model is one of these projects. It should make it possible to better account for safety aspects during planning. A prototype tool has been designed that extracts construction plans and information about BA devices from a BIM model. Subsequently, the user is guided through the annotation with security-relevant information. As a result, the tool provides a prioritized evaluation that assists in risk assessment and planning of security measures. The tool can be applied to both, new and existing buildings.

Device performance degradation through the use of security mechanisms and associated costs is often cited as a reason for opting out security. In order to quantify these performance losses, a comparison was made between the application of BACnet with and without security architecture (figure 4). It turns out that systems in the performance class of a Raspberry Pi 3 minicomputer (comparable to a powerful DDC) are capable of answering enough requests per second with security mechanisms. Based on the measurements, it is also possible to estimate more precisely what additional expenditure can be expected on the devices and in the network when security mechanisms are used. This helps with the dimensioning of systems and individual devices. In addition, suggestions were made as how the extra effort can be reduced.

Another reason for not using security mechanisms is the large effort and the security of procedures used during configuration. To counter this, an easy to use concept and prototype tool was developed to securely create the initial relationship of trust between devices in a building automation system (figure 5). The prototype was developed for use with the draft of BACnet Addendum IT. But the concepts can also be transferred to its successor BACnet Secure Connect or completely different technologies.

Conclusion

In this project, five hurdles for the implementation of security measures in building automation were addressed. In summary, many mechanisms are already available in principle. Their lack of implementation results from a lack of awareness about this topic for a long time. Currently there is a change in this regard, further education can create impulses here. The approaches to reduce the hurdles can be further developed and expanded in the future. As a result, security services can become a potential new business in BA. Missing update mechanisms remain another problem and should be given more attention in the future.

Key Data

Short title: Eusebius – Effective security mechanisms in building automation
Researcher / Project Management:
Dr. Frank Golatowski
M.Sc. Björn Butzin
Total Cost: 200.264,24 € €
Share of federal subsidy: 140.184,97 €
Project duration: 24 Months

Pictures:

Bild 1: Logo.png
The logo of the research project

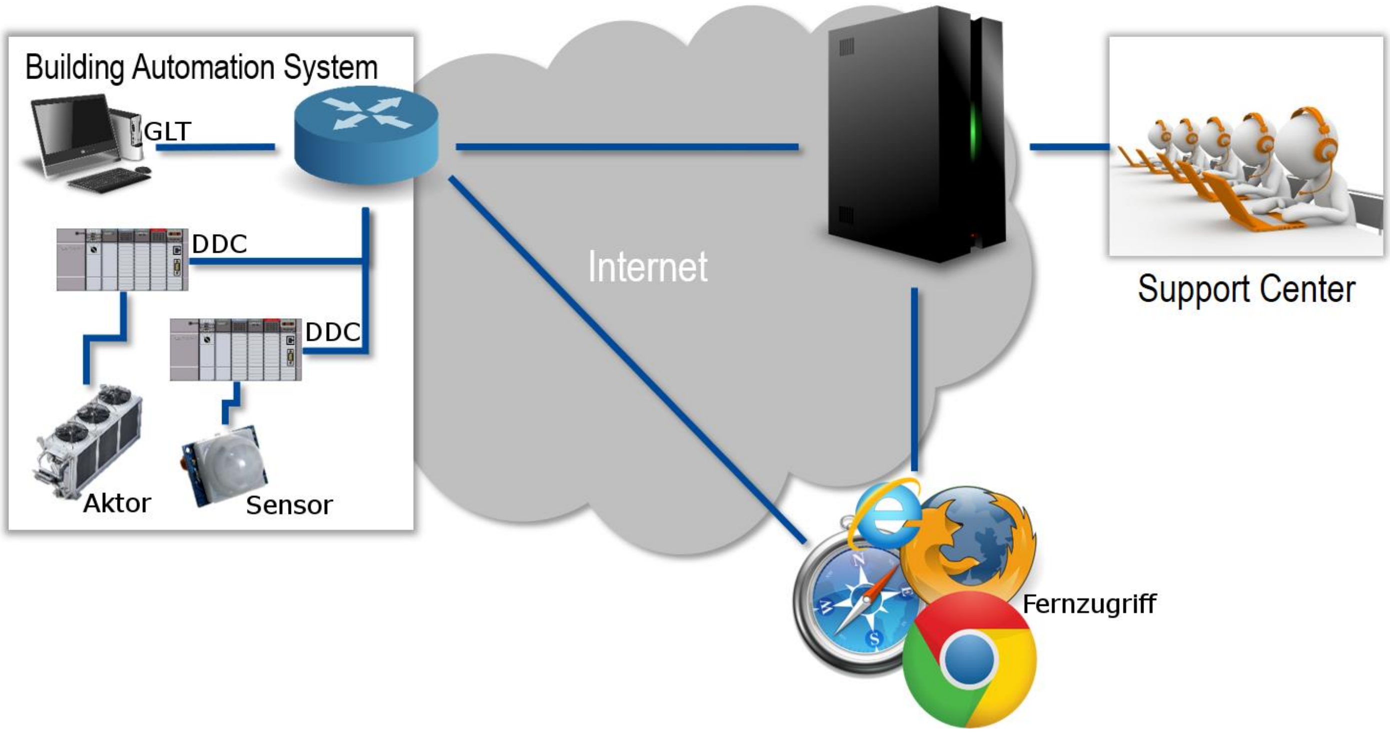

Bild 2: GA-System.png
Schema of a typical building automation system

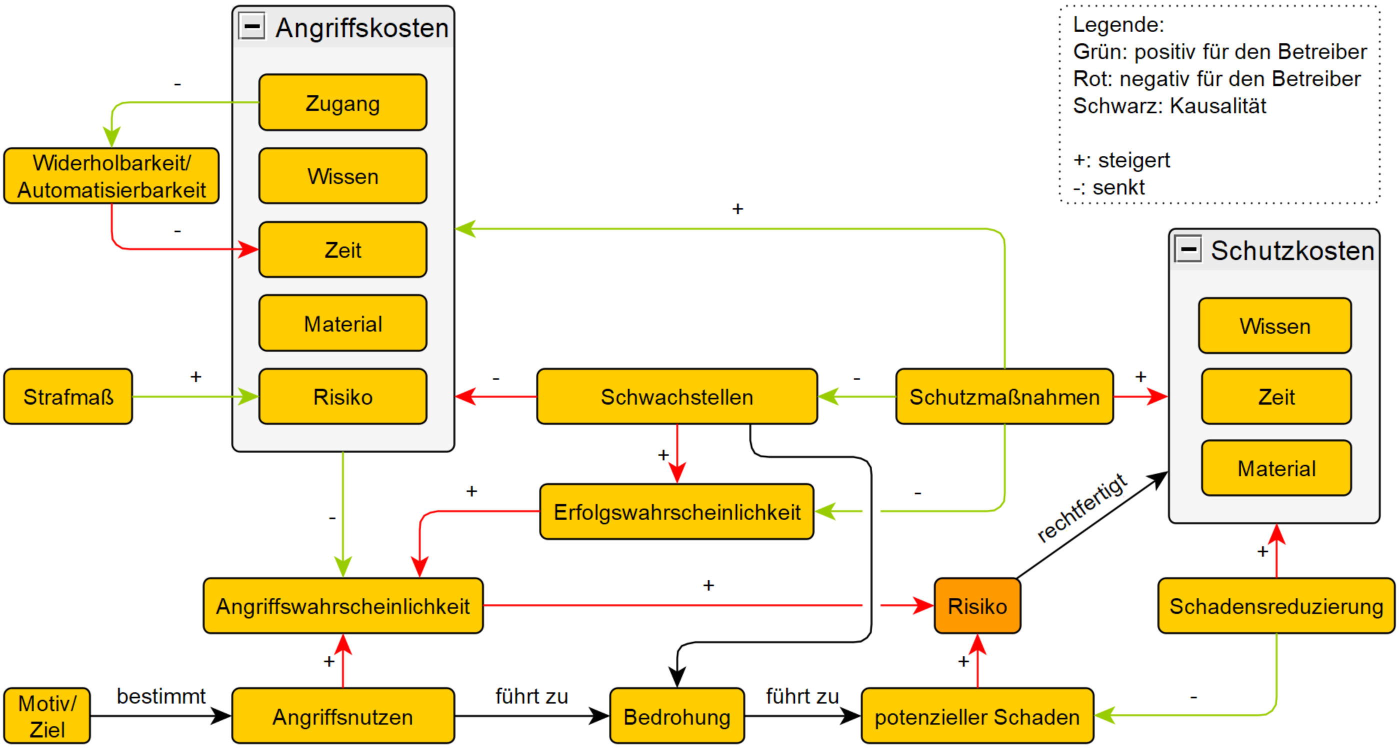

Bild 3: Kosten-Nutzen.png
Relationship of costs and benefits for attacker and defender

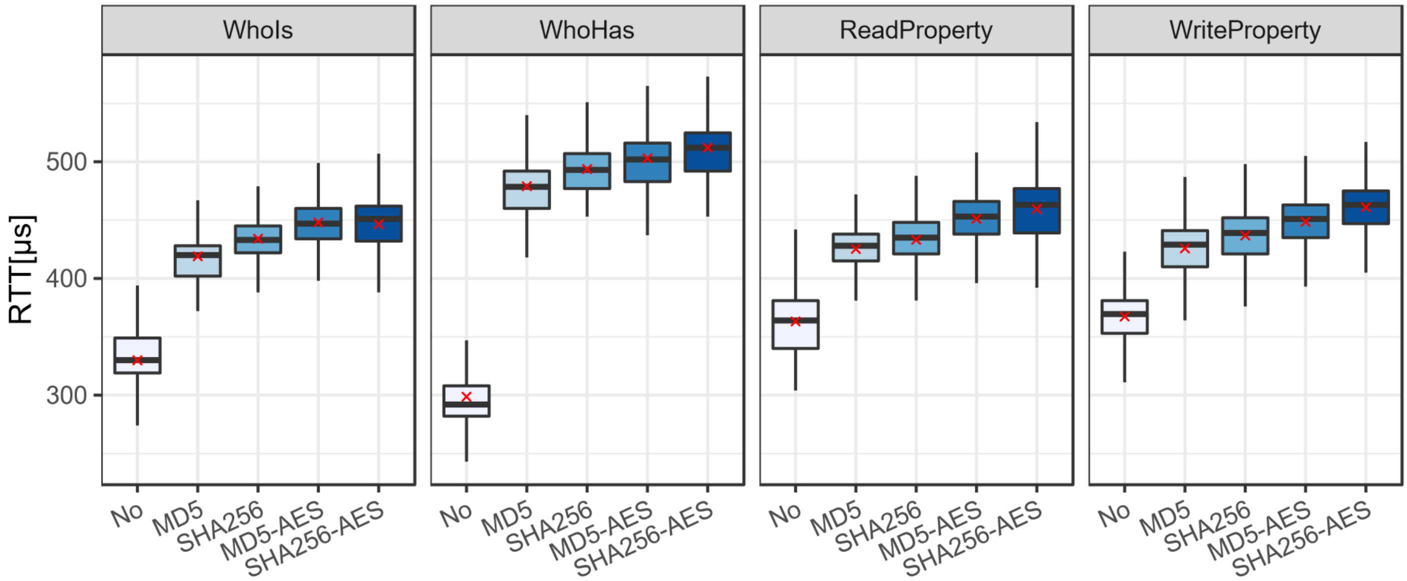

Bild 4: NetworkEval.png
Evaluation results: round trip times of BACnet messages with and without security applied

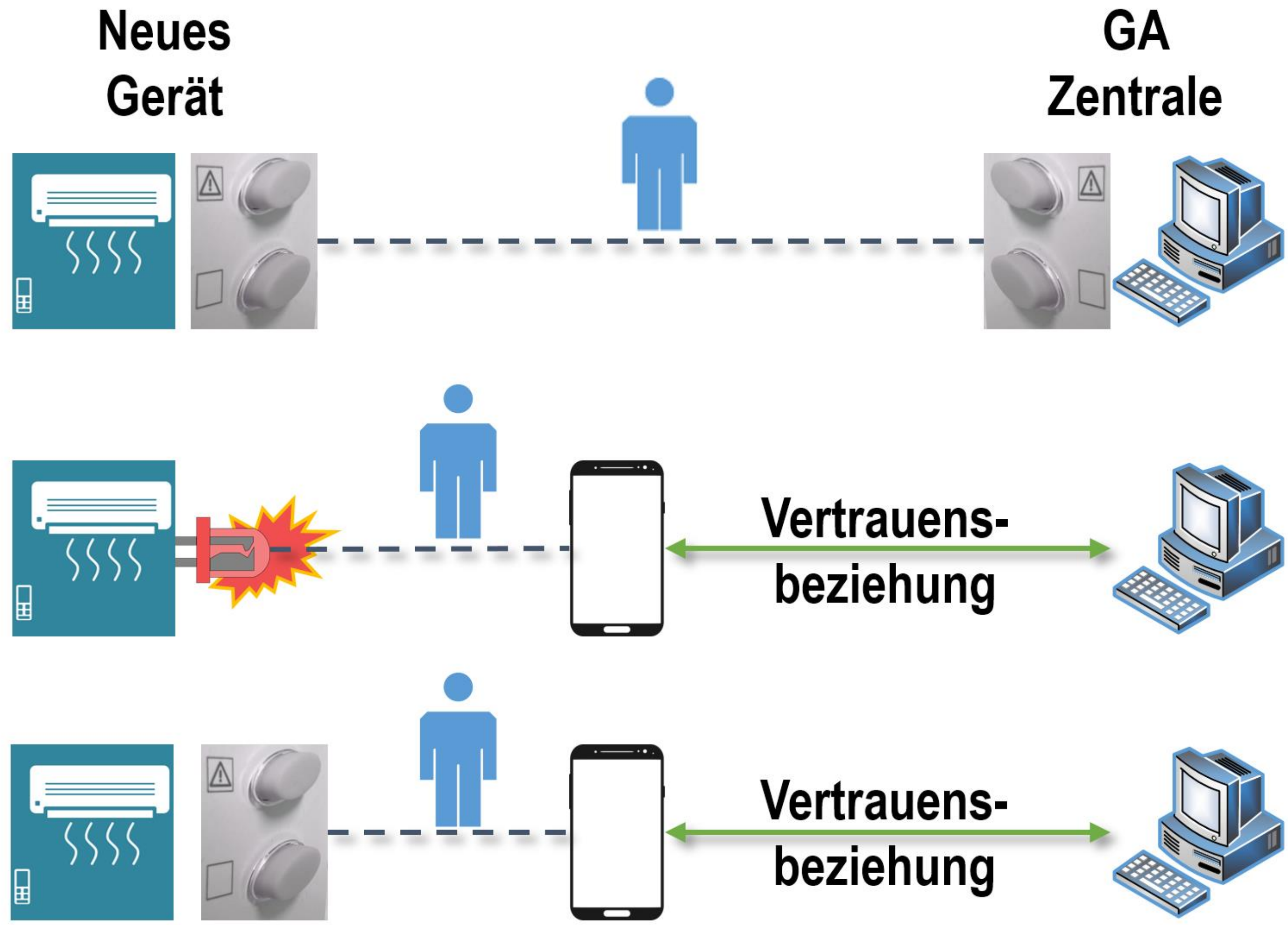

Bild 5: OutOfBand.png
Three possibilities for realizing out-of-band authentication