Abstract der fertigen Arbeit

The popularity of Smart Homes has been increasing over the last few years and this trend still carries on. They offer great comfort while causing less struggle. This concurrence is definitely a treat for homeowners. The budget-friendly Internet of Things (IoT) offers a lot of devices which are commonly used in Smart Homes. Time and again, they do not provide a decent security level. This is the point where the problems might start off. Unnoticed by the homeowner, hackers might compromise the network; in the end things can even get worse and the homeowner finds himself being held to ransom.

Although, the number one risk associated with Smart Homes are hacker attacks, only few IT security mechanisms are applied to protect the Smart Home. In this thesis an experimental setup is established to test a simple and effective security mechanism, impressively preventing hacker attacks. This experiment can probably raise the aware- ness of hacker attacks. The sheer number of failed attacks happening during the experiment period of time will alert homeowners; in the event that a hacker attack still turns out successful, the homeowner gets immediately informed, which raises the overall security enormously. The mechanism that can effectively boost the network security is called "Honeypot". The aim of a honeypot is to reroute the attackers from their original target and monitor the attackers' actions. Subsequently, this information is used to redesign the security concept of the Smart Home. This rerouting is performed with simulated vulnerabilities which are easy to exploit.

This thesis evaluates the different design approaches of honeypots and analyses potential attack vectors for Smart Homes. The knowledge gained from the proof-of-concept implementation is then used for further improvements of the honeypot, so that the Smart Home Honeypot is capable of protecting a variety of different Smart Homes against a variety of attackers.

In the end the evaluation of the design concepts and the results from the experimental implementation together led to a design guideline for Smart Home Honeypots. The gained knowledge should be used to create a whole range of different honeypots that are able to protect all kinds of Smart Homes. At the same time, the setup and the maintenance should be kept simple and affordable. This way, a budget-friendly and effective security mechanism is created which can be installed by any Smart Home owner. If all precautions explained in this Master Thesis are adopted appropriate honeypots can effectively protect a Smart Home against virtually all kinds of possible attackers.