"What if someone steals it?" Hands-on evaluation of the software security work of a networked embedded system

Adina Borg
ad4600bo-s@student.lu.se
Hedda Klintskog
he4125kl-s@student.lu.se

June 2022

Popular Science Summary

Today, information technology (IT) is constantly growing and our society becomes increasingly dependent on IT solutions. Some systems are negligible while others are very critical and their loss of data or downtime can be devastating. While IT grows so does the criminal activity in the cyber-world. Hackers have been around for as long as computers have been but the view of a "hacker" has changed. A lot of people associate the term "hacker" with teenagers, hoodies, basements and possibly with the hacking organisation *Anonymous*. These are relevant associations, however, a big part of hacking today is done by people who have it as their profession. Hacking is performed by criminal organisations as well as by Nation States and federal organisations. It can also be performed under the term "ethical hacking" which is when hacking is used legally to find and mitigate security vulnerabilities.

It is common for companies and other organisations to hire *Penetration testers* to try and hack their systems. A penetration tester is an ethical hacker who has permission to hack a system as a criminal hacker would do. The penetration tester report all security vulnerabilities found to the hiring organisation which they can then mitigate, making it more difficult for a criminal attacker to find vulnerabilities.

In this thesis, a penetration test is performed on a horn speaker, a speaker used in places such as airports and building sites. The penetration testing is partly performed to find possible security vulnerabilities. It is also performed as a way to evaluate different methods and tools used during penetration testing. It is studied how easy it is to find and use different methods and tools. Further, an evaluation is also done of the process which has been performed by the developers to make threat models and construct a speaker with as few vulnerabilities as possible.

To be able to understand the motivation behind attacking this type of speaker, different main goals an attacker could have were mapped out before starting the penetration testing. One goal could e.g. be to steal sensitive data while another one could be to play your own audio from the speaker and all speakers connected to it on the network. When the penetration testing began it started out from a *Black Box* perspective since we had no previous knowledge about the speaker. A system is seen as a Black Box if no knowledge exists of how the system works. During the penetration testing we used methods and tools which were recommended by experienced penetration testers and when their recommendations were not enough other popular options were looked for, compared and tested. It was shown that having good methods to follow is important to keep penetration testing structured. It was also shown that using existing tools can be both positive and negative since it can ease the work but it is also a risk of missing vulnerabilities if the penetration tester does not understand how the tools work.

After the different attacks were tried against the speaker it was possible to compare the approaches tried during the penetration testing with the threats in the threat models done by the company. Here we saw that threat modelling is a good method for finding many possible threats. The category captured by our penetration testing that was missing from the threat modelling was misuse of the system. This includes scenarios where an attacker intentionally uses the system wrong in order to hack into the system.