Smart Building Security
Nothing is as it seems

04.04.2019

from Hagen Lang

Security expert Prof. Dr. Hartmut Pohl from softScheck GmbH explains in an interview which security vulnerabilities they regularly identify in IoT devices. His presentation at the Smart Building Summit on 2 May in Dresden together with Wilfried Kirsch gives developers important ideas for their design and development process.

QUESTION: Mr. Pohl, you and your colleague Wilfried Kirsch will give a lecture on "Hardware-based attacks using smart cameras as an example" at the Smart Building Summit in Dresden on 2 May 2019. Why is this topic important?

PROF. DR. HARTMUT POHL: The topic concerns manufacturers of smart devices for Smart Home and Smart Building, of course the users of these devices and the operators of networks to which these devices are connected, e.g. house and building automation networks. The security of the properties themselves could also be compromised if physical access were gained by means of these devices.

QUESTION: Let's stick with the user, what should he have to fear today, after years of reporting about security on all channels? Isn't the technology mature today?

PROF. DR. HARTMUT POHL: There is a lot of talking and reporting — the practice looks completely different: My colleagues have taken an example of a product from a European company that is known and active worldwide in the smart building sector — a company that very successfully sells functionally excellent cameras, thermostats and weather stations worldwide. They stand out due to their ease of use and the cameras in particular are advertised with the sales argument "additional security against burglary" etc. Such a camera, the currently available model, we have just hacked.

QUESTION: What does that mean exactly?

PROF. DR. HARTMUT POHL: We have identified a security vulnerability that allows an attacker to connect his account to a camera he has previously been able to access. For example, if the camera was ordered in an online shop and returned within the legal deadlines. He can then spy on the owner or even exclude the owner from accessing his own camera. What we have done technically can be read online. We have informed the manufacturer about this and the vulnerability was fixed in February 2019. You can read about this vulnerability here.

QUESTION: Then everything is fine.

PROF. DR. HARTMUT POHL: Well. First of all, the camera was at a relatively good security level. On the other hand, it shows that even market leaders are not protected against security bugs. In addition, the error was structured in such a way that a victim (user) could not prevent unauthorized access to his camera. All he could do was to send the device back and buy a new one.

The second problem, however, is that — regardless of security gaps — you can do mischief with such cameras. The camera's "Revolutionary Face Recognition Technology"

improves security, according to advertisements, because it immediately sends alarms to the mobile phone when it detects an intruder's unknown face.

So at softScheck we photographed our faces and printed them out on A4 paper. We finally managed to get the camera to think of such an expression as a familiar, "allowed" face. So an intruder can trick the system with a well-made facial expression of a "allowed" inhabitant, it may then not trigger an alarm and send no notification to the inhabitant's mobile phone, even though strangers are turning his apartment upside down. The camera works, there is no software error, but you can outsmart it.

QUESTION: In your presentation at the Smart Building Summit on May 2nd in Dresden, you will not describe how to make A4 copies of faces.

PROF. DR. HARTMUT POHL: No, we use an IoT Smart Camera to show how it can be hacked using inexpensive methods that are comprehensible to everyone. We just solder a USB to RS232 adapter to the camera to connect it to a computer. We disturb the boot process with the Pin2Pwn method. Here, a needle is used to bridge one of the channels of the flash device, which means that the requested file cannot be read. This error causes the bootloader shell to start, in which we execute a manipulated boot image that gives us root privileges. What can be done after a successful rooting of the device and how manufacturers can make attacks of this kind more difficult, we explain in the presentation.

QUESTION: Can manufacturers have their products tested by you?

PROF. DR. HARTMUT POHL: Of course, but there are relatively simple methods with which developers can make it very difficult for hackers. All you have to do is apply it. We will discuss this in our lecture. Developers of IoT-Devices get important ideas for their design and development process in Dresden.

Secondly, we offer the very successful Security Testing Process developed by us, in which we use 6 methods — starting with the requirements, through the design, the source code to the machine executable code — to successfully examine each step for security gaps using a (different) method. We therefore take over the entire security engineering support of the development process of hardware and software, firmware, mobile apps and also check servers and networks.