DeepSec 2017 Workshop: Smart Lockpicking – Hands-on Exploiting Contemporary Locks and Access Control Systems – Slawomir Jasek

Posted on **October 31,2017** by **sanna**

You can, quite reasonably, expect smart locks and access control systems to be free from alarming security vulnerabilities - such a common issue for an average IoT device. Well, this training will prove you wrong. After performing multiple hands-on exercises with a dozen of real devices and various technologies, you will never look at the devices the same way. Smart lockpicking is something to scare you, not just on Halloween.

https://www.youtube.com/watch?v=YU5g-Wy_5e0 We asked Slawomir a few questions about his training:
Please tell us the top 5 facts about your workshop.

- Focused on hands-on, practical exercises with real devices
- Lots of various topics and technologies covered
- Regardless if you are a beginner or a skilled pentester, you will learn something new and have a good time
- Many exercises designed as “homework”, possible to repeat later at home
- Includes hardware pack (about 100€ value) for each student, consisting of Raspberry Pi, NFC board, and Bluetooth Low Energy sniffer. The hardware will allow you to crack and clone NFC cards, sniff and analyse Bluetooth Low Energy connections

Image not found
http://blog.deepsec.net/wp-content/uploads/2017/10/hardware-e1509444195664.jpeg

How did you come up with it? Was there something like an initial spark that set your mind on creating this Workshop?

I wanted to focus on devices everyone can encounter, yet common sense is that we can trust their security. Practical exercises debunking your „comfort zone“, performed hands-on yourself, are in my opinion one of best ways to effectively learn a given topic. Also, once you master assessment of the ones supposed to be most secure, other IoT devices will seem to you even more giant „jar of bugs”.

So, smart locks, electronic safety and access control systems were the natural choice here. Vendors' claims on the security rendered them even more attractive for the task. And it soon turned out that in so many cases „the king is naked”. A significant number of such devices have serious security flaws that can be exploited even by non-highly skilled intruder. And as a result cause serious loss.

Why do you think this is an important topic?

I think a quick scroll through the recent headlines will do as an sufficient answer. Of course the media often overestimate the real risk, but you just can’t ignore the fact anymore that the smart devices are increasingly surrounding us, and their security level is usually still far from acceptable.

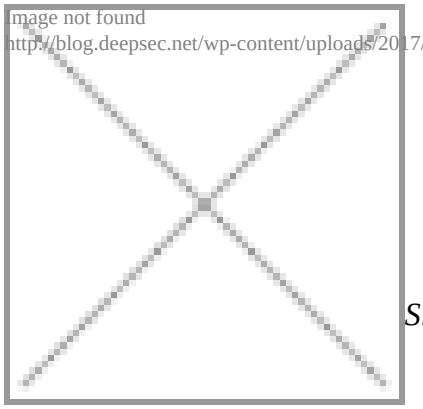
I am very enthusiastic about new technologies, but on the other hand I think before entrusting our lives to them, we should first understand and mitigate the associated risks.

Is there something you want everybody to know – some good advice for our readers maybe?

Did I mention the free Raspberry and other goodies - for NFC card cloning and BLE sniffing already?

A prediction for the future – what do you think will be the next innovations or future downfalls when it comes to particularly your field of expertise / the topic of your training?

The digital revolution will not stop. And unless you hide in a cave, you will encounter the new smart devices responsible for your safety. Don't let them catch you by surprise.



Slawomir is an IT security consultant with over 10 years of experience. He participated in many assessments of systems' and applications' security for leading financial companies and public institutions across the world, including a few dozen e-banking systems. Also he developed secure embedded systems certified for use by national agencies. Slawomir has an MSc in automation&robotics and loves to hack various devices, gadgets, home automation and industrial systems. Beside current research (BLE, HCE), he focuses on consulting secure solutions for various software and hardware projects. Speaker at BlackHat USA (new Bluetooth Smart Man-in-the-middle proxy tool), Appsec EU (insecurity of proprietary network protocols), HITB (HCE contactless payments), Confidence (IoT), Devoxx and other conferences for

developers (SDLC, mobile application security). Trainer at Deepsec, Appsec EU, HackInParis, HackInTheBox, Confidence.

Posted in:Conference,Training | Tagged:Access Control,DeepSec,Hacking,Infrastructure,IoT,IoT Devices,Smart Lockpicking,Training | With 0 comments