Security Divas 2017
Reflection Report

Tetiana Yarygina

Department of Informatics, University of Bergen

Abstract

NorSIS Security Divas is an annual security conference for female professionals held in Gjøvik, Norway. This report reflects on the talks given during NorSIS Security Divas 2017 with emphasis on the topics of my personal interest. General conference experience is also briefly described. Attendance of the even was funded by COINS Research School.

1 Sikkerhet i min personlige kritiske infrastruktur by Marie Moe

Implantable medical devices (IMDs) such as implantable cardioverter defibrillators and pacemakers are designed to monitor and sustain regular heart rhythms. These are small battery-powered devices placed under the skin. The latest generation of IMDs support wireless communication. Base stations installed in the patients' home collect data from such IMDs and send it to the hospital. Additionally, IMDs can be remotely reprogrammed by health care professionals with specializes equipment. Such functionality exposes greater attack surface compared to less "smart" devices. Other medical devices with similar capabilities are insulin pumps.

Unauthorized remote access to such life critical devices is a serious and real threat. Security of IMDs is an important question that will gain even more attention when IMDs become readily available for general public world-wide. The title of the talk reflects the fact that the speaker herself has a pacemaker and was involved in a security analyses of such type of devices.

The manufacturers of IMDs often follow security-by-obscurity principle. The communication protocols used by IMDs and corresponding programming devices are proprietary and closed-source. Reverse-engineering is the only way to analyse them.

Many of the modern IMDs were shown to be insecure. Demonstrated attacks include reply, DoS, spoofing and MITM attacks that can result in significant reduce of IMDs battery life, patient's privacy violation, and even lead to lethal consequences. Many reverse-engineered protocols were shown to lack such essential security features as message integrity and authenticity.

2 The Role of EC3 in Combating Cybercrime by Aglika Klayn

Europol is the European Union law enforcement agency. The talk was centered around Europol European Cybercrime Centre (EC3), which the speaker represents, and the units main activities. EC3 was established by Europol in 2013 to strengthen the law enforcement response to cybercrime such as online fraud, child sexual exploitation, and different cyber attacks. An important and unique aspect of EC3 is its ability to fight crime across countries borders.

No More Ransom (`https://www.nomoreransom.org/`) is an initiative to fight ransomware in which Europol participates together with Dutch National Police, Intel Security, and Kaspersky Lab. Ransomware is a type of malware that either locks the device or encrypts electronic files on it. Ransomware demands a ransom payment to revert the changes or not publish the personal data. No More Ransom web-site increases general public awareness on the matter by providing ransomware prevention advice, as well as assists ransomware victims by releasing multiple tools to unlock/decrypt their devices. Additionally, the web-site provides links to report the criminal incident (ransomware attack).

Ransomware scams became increasingly common nowadays. They target not only individuals, but whole organizations including hospitals, police departments, and other critical governmental units. Another interesting trend is that ransomware started using more sophisticated encryption schemes with constantly increasing key length, and exists for almost any modern OS.

Secure Platform for Accredited Cybercrime Experts (SPACE) is a collaborative web platform for security specialists developed by Europol. It allows people from law enforcement areas, private sector and academia to share their knowledge and expertise on cybercrime. Although access to the expert community is granted by invitation only, SPACE still could be a useful resource for PhD students involved in security.

3 General conference experience

NorSIS Security Divas 2017 gathered over 160 participants from all around Norway, as well as other Scandinavian countries. Most of the talks were held in Norwegian. The conference was well organized. The participants were both from industry and academia, which is a nice mix. I had a chance to talk to many interesting people from such companies as Accenture, Nordea bank, Mnemonic, Finn, and some others. I would recommend attending Security Divas conference for COINS students in the future.