https://www.pressetext.com/news/20180821014

DeepSec Conference releases Schedule for 2018
Focusing on the Insecurity of Things and infrastructure

Vienna (pts014 / 21.08.2018 / 09:25) – This year's DeepSec In-Depth Security Conference will focus on the topic of Insecurity of Things (IoT) and components of everyday infrastructure. The ever-advancing networking opens up completely new ways for attackers – faster than developers and manufacturers can fix bugs. Instead of using secure design for products and code, machine learning and artificial intelligence are integrated – unfortunately, implemented using convenient statistics and the algorithm of the week from the daily menu of the development kit. The presentations at the DeepSec conference will therefore put the alleged technologies of the future to the test. Mobile networks, the Internet of Things, collaboration platforms in the cloud, customer relationship management systems and the human factor are in the cross-hairs.

Smart is the new Cyber

Information technology has a legitimate reputation for constantly inventing new terms and acronyms for make-believe solutions to technical problems. Mostly, this is a pure hide and seek game, very well illustrated by the keywords Cyber, Cloud and Virtual. Behind the scenes, some terms are justified, but hardly anyone checks up on what is really hidden behind a product. The best example for this right now is the trend to make everything smart, no matter if security was a design criterion or not in the first place. The power supply should become a smart grid, questionnaires should turn into Smart Assistants, etc.

A look inside reveals components that are often just somehow linked together, without any concept of security. The best examples are smartphones, which have mutated into an universal key. On a single device you have a variety of accesses that require specific apps. Thus, these items automatically become a sought-after target. The Mobile App Attacks 2.0 workshop will demonstrate how to use apps and the smartphone platform as a basis for successful attacks. Furthermore, a workshop on mobile security is also part of the conference programme. The coach David Burgess is a veteran in this field. In 2009, he'd already discovered and documented serious security vulnerabilities in mobile networks at DeepSec. This year he's back and can also tell us something about the new standards.

Uncertainty of Things everywhere

Vulnerabilities of devices from the Internet of Things (IoT) are also presented and analyzed in lectures and workshops. Johannes Pohl demonstrates in his training how to analyze the communication of IoT devices. This work serves as the basis for derived attacks. Few manufacturers are really able to design and implement secure communication as a protocol, regardless of whether the protocol is new or based on established standards.

In his talk, Werner Schober, security researcher of SEC Consult, presents weaknesses in "smart" sex toys. Unfortunately this is not a bad joke. All IoT devices of every industry are a danger. The original purpose of a device doesn't matter - Attackers have already broken into casinos utilizing a networked aquarium. In addition, especially for sex toys, the discipline for regular updating the firmware is certainly lower than for "smart" TVs. Thus, these items automatically become a risk to security and privacy at the same time. Countless other things of everyday life can be enumerated that can be used to attack information systems.

The Human Factor

No matter what technology you use, the human factor remains an important part of information security. The human body gets also networked. Ulrike Hugl from the University of Innsbruck discusses implanted RFID (radio-frequency identification) chips. With such foreign bodies oneself becomes part of the questions about data security and attacks by third parties, because RFID components carry data and can be read out. In her talk Ulrike Hugl will examine the distribution, the usage of and the ethical issues surrounding RFID.

Furthermore, there are talks on threat analysis, an important part of digital defense, often carried out by automated processes. The limits of the capabilities of human experts will be examined and how they can be supported by automated systems. In his presentation, Stefan Schumacher will highlight how the human brain can be manipulated and how social engineering attacks can be implemented using methods based on this knowledge. Most successful attacks always use a component that touches the human factor.

Interdisciplinary and in touch with Research

Today, information security is not just about technology. Security problems always have to be investigated and solved in an interdisciplinary team. The DeepSec In-

Depth Security Conference is meant for a spectrum of research, education, industry, government and business. Just like last year, visitors also have the opportunity to attend lectures at the parallel Reversing and Offensive-oriented Trends Symposium.

ROOTS is an academic workshop that takes place parallel to and at the same time as the DeepSec Conference. The aim is to show that the combination of science and information technology, and the combination of professional insider knowledge, academic research and practical approaches, can defend modern digital infrastructure better than ever before. Seize the opportunity.

Programme and Booking

The DeepSec conference takes place on the 29th and 30th of November.
The trainings will take place on the two preceding days, the 27th and 28th of November.

Training & Conference venue:
The Imperial Riding School Vienna – A Renaissance Hotel
Ungargasse 60
1030 Vienna

Current programme: https://deepsec.net/schedule.html
Tickets for the conference and trainings: https://deepsec.net/register.html

Sender: DeepSec GmbH
Contact: René Pfeiffer
Mobile: + 43-676-5626390
E-mail: deepsec@deepsec.net
Website: https://deepsec.net/