HackCon#11 conference is a good place for IT security society to come together to socialize and discuss about IT security. The conference gives a good overview about IT security challenges for some IT systems from attacking and defending perspectives. It also arises privacy concerns related to collected information by different enterprises and handling of these information.

The presenters in HackCon#11 were from different countries with different background in IT security, the things which enriches the conference output. This article gives a brief overview about discussed topics within the conference. Below each topic a brief description is given about discussed points within related topic:-

How to bypass your security with 30 dollar:-

This lecture discussed hardware-related IT security attacks, such as, ATM Skimming attack. Where it demonstrated the possibility of running hardware-related attacks using cheap hardware within short time. In addition, some suggestions were given to countermeasures these kinds of attacks.

Security implications of cybernetic implants:-

This lecture discussed security weaknesses of RFID cards and expected implications on IT security by implants techs, such as RFID implants. By the end, it went through attack scenario in which, attacker cloning card to implant it inside his/her body.

Protecting our people:-

This lecture discussed security enhancement through people. Where, it elaborated how security could be improved through improvement of people behaviours. By the end, a tool aims to improve human behaviour were presented

When Penguins Attack your highly valued asset

This lecture discussed the security attacks coming from Linux OS machine. The lecture gave some example for such attacks. It went also through some possible defensive techs, which could be used against these attacks.

Secure your organization from Phishing attacks

This lecture gave an overview about phishing attack types, being Phishing, spear phishing and whaling. It went also through followed steps by attacker to run possible phishing attack. By the end it recommended a set of defensive considerations, tools and techs, which should be used to protect system from phishing attack.

Wi-Fi IDS/Firewall

This lecture discussed the security challenges and attacks of Wi-Fi networks. At the beginning, it went through set of Wi-Fi popular attacks, such as, SSL MIMT, DNS hijack and traffic monitoring. Later, it described the scope of security requirements needed to handle by defensive techs. By the end, it gave an overview about open source tool, called Chellam (Wi-Fi IDS/Firewall) as possible defensive techs, which satisfy most of reported security requirements.

Smartwatch risks, the new security risk to your enterprise

This lecture discussed the security risks resulted from popular smartwatches, being (Apple Watch, Samsung Gear 2 Neo, Android Wear (Moto 360) and U8). At the beginning, the lecture went through popular smartwatch services. Later, it gave an overview about these smartwatches vulnerabilities and ran demonstrative demo for exploiting some vulnerabilities. It went also through possible risks resulted from smartwatch on the enterprise. By the end, it concluded the need to improve the security level of the smartwatches based on the current estimated level.

SMS and IMSI catchers

The lecture discussed possible attacks via SMS and IMSI on mobile device. It start with SMS-based attack, where, It identified a set of malicious activities that could be performed by these attacks, like listing on conversation. It claimed also, that available mobile anti-virus is not enough to assure the protection against these kind of attacks. Since, these anti-virus monitor main OS only. Second part of the lecture was mainly about IMSI attack, where an overview about this attack was given. By the end, secure mobile communication app was presented as possible countermeasure against SMS-based and IMSI attacks.

The age of Mobile App Insecurities

This lecture discussed security of mobile apps running on popular platform, such as IOS and Android. At the beginning, it gave an overview about current status of mobile apps security downloadable from different play stores. It went also through common mobile vulnerabilities, such as insecure data storage. By the end brief demonstrative demo was given about exploitability of described vulnerabilities.

Protect Yourself from Online Tracking & Surveillance

The lecture discussed the online tracking and surveillance applied on user by big enterprises, like google. At the beginning it went through the kinds of collected information about users, like, purchasing habit of user (amazon) and watch video (YouTube). By the end, it recommend a set of tools and techs to protect user from online tracking.

Reported by Seraj Fayyad, 26 Feb. 16