TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Practical Exploitation of IoT Networks and Ecosystems

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

Deep Armor is offering a hands-on training for pentesting and hardening Internet of Things (IoT) ecosystems, with special focus on popular communication protocols such as Zigbee, Bluetooth & BLE, as well as Device - Mobile - Cloud security topics. Students will learn to use specialized low-cost hardware (supplied to each student for the duration of the training) & software tools to perform live packet capture, manipulation and injection in wireless sensor networks and Bluetooth/BLE channels.

Students will learn about weaknesses in consumer IoT devices (wearables) paired with mobile ecosystems (Android & iOS) — how information theft is scarily easy, and what steps can be taken to harden these designs. Cloud is an essential part of IoT, and our course includes a case study of AWS IoT Core — how to securely deploy virtual “Things”, configure the rules, accesses and communication parameters. We conclude with defensive security best practices and next generation SDLC for the products of tomorrow.

ERNW Insight GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
BIC: GENODE61HD3

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
Ust-ID DE 304 445 827
IBAN: DE84 6729 0100 0067 1236 03

Managing Director:
Kerstin Schröter

The Internet of Things (IoT) market today is defined by product manufacturers pushing a broad spectrum of computing devices out to the hands of consumers at an ever-increasing pace and connecting them to the Internet. They are in a rush to hit the market shelves before their competitors and they often marginalize security, citing irrelevance and no return on investment. Consumers rarely prioritize security over cost, and this this often incentivizes vendors to ignore security.

An IoT product has no predefined form factor. It may be a smart fridge, a pacemaker, or a traffic light in a smart city. Makers of these classes of devices are often small/medium sized businesses who look for standards and reusable code for communication protocols, software stacks and libraries. But standards are few and are rarely one-size-fits-all in this space.

Most IoT architectures can broadly be broken up into three logical modules – the form factor device, mobile applications and cloud services. These three modules may usually be broken up into sub-modules that each have their own computing stack and communicate with each other, as well as the other components through a plethora of communication protocols.

Dozens of protocols and standards exist for IoT-class products. This situation poses a significant challenge for security teams tasked with ensuring that no design and implementation level weaknesses exist in such communication channels. Among the IoT hardware form factor devices, low power protocols such as ZigBee, 6LoWPAN, Z-Wave, Bluetooth, BLE, etc. are popular. Device manufacturers also frequently customize the base IEEE 802.15.4 specifications (ZigBee, for example, is built on top of this) to architect their own Wireless Sensor Networks (WSN) for communication between the IoT gateways and node devices. Such WSNs are popular in Industrial IoT (IIoT) products.

On the consumer IoT front (wearables, home gateways, etc.), Bluetooth and Bluetooth Low Energy (BLE) have been in use for years. While the Bluetooth specifications have gone through several revisions and have included security as part of the protocol, vendors often turn to minimal (or no) security for Bluetooth and BLE channels. Any kind of cryptographic operation on such small form factor devices, which are often powered by low performance micro-controllers running on low power batteries, can be very expensive.

Deep Armor offers a new, hands-on class on practical exploitation of IoT systems. Our program spans across the entire ecosystem — covering security for the hardware form factors, mobile/cloud components and communication protocols. We have four primary sections in our program:

- Attacking and Hardening a Zigbee-class IoT Network
- Practical Exploitation of Bluetooth - Mobile Channels, and BLE Security
- Next-generation cloud solutions for IoT products
- Secure by Design

Prerequisites

- Ability to understand and run simple commands on a Linux terminal;
- Basic programming skills (python is preferred, but familiarity with any programming language is sufficient to execute the tasks);
- Basic understanding of Android application model and logs;
- Familiarity with Wireshark;
- Basics of cryptography;
- Understanding of common network protocols and web applications.

Requirements

- A laptop running Kali Linux - Natively running Kali is strongly preferred. Kali Live on USB with Persistence also works when configured for USB passthrough;
- At least 8 GB RAM on the laptop;
- Laptops should be capable of plugging in two USB 2.0 devices (you should bring your own adapters, if required) ;
- Internet access is necessary, so students need to bring their own Wireless network adapters, if required;
- Trainers will share the list of open source software to be installed prior to the training date.

About the Trainer

Sumanth Naropanth is the Founder & CEO of Deep Armor, an internationally recognized security consulting firm. He is a business & technical expert in information security and has held security leadership positions in large corporations and startups. He has championed next-generation Security Development Life Cycle (SDLC) frameworks, architected secure solutions, and has managed global security assurance teams. Sumanth regularly speaks and conducts trainings at well-known security conferences, including at Black Hat, FIRST, Troopers, AppSec, and so on. Sumanth has a Master's degree in Computer Security from Columbia University.

Sunil Kumar is a Senior Security Analyst at Deep Armor. He has extensive experience in security research, product security assessment and SDLC methodologies. Sunil's areas of expertise include threat modeling, penetration testing of mobile & web applications and IoT products. He has advanced knowledge of AWS and has developed cloud security tools and applications using node.js and python. Sunil regularly speaks at local and international security conferences. Prior to his current role at Deep Armor, Sunil worked as a security engineer for Ola Cabs and Aricent Technologies.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com