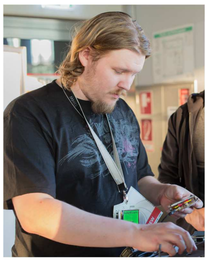
SyScan360 Seattle 2017 CFT Submission

Cellular Hacking

Section A

Trainer 1:



Brian Butterly

bbutterly@ernw.de - @BadgeWizard

ERNW GmbH, Heidelberg, Germany

Bio:

Brian is a security researcher, analyst and simply a hacker at Heidelberg (Germany) based ERNW GmbH. Coming from the field of electronic engineering he tends to choose alternate approaches when hitting new projects. He currently works on the intersection of embedded-, mobile and telco-security, with tasks and research ranging from evaluating apps and devices through to analyzing their transport networks and backend infrastructures. Resulting from the broad range of practical experience and natural curiosity he has developed a very diverse set of skills and knowledge. He enjoys cracking open black boxes and learning about their details down to the electronic circuits and creating the tools he needs on the way. He is always happy to share his knowledge and findings.

Trainer 2:

Hendrik Schmidt

hschmidt@ernw.de - @hendrks_

ERNW GmbH, Heidelberg, Germany

Bio:

Hendrik Schmidt is a seasoned security researcher with vast experiences in large and complex enterprise networks. He is a pentester at the German based ERNW GmbH with focus on telecommunication networks. Over the years he evaluated and reviewed all kinds of network protocols and applications. He loves to play with complex technologies and networks and demonstrated several implementation and design flaws. In this context he learned how to play around with core and backhaul networks, wrote protocol fuzzers and spoofers for testing implementations and security architecture. As his profession of pentester, security researcher and consultant he will happily share his knowledge with the audience.

Section B

Title: **Cellular Hacking**

Description:

What do a GPS tracker, a home alarm system and a small industrial control system have in common? They can all be remotely controlled via a cellular uplink. The same applies to various smart meters, cameras automotive components and many other modern devices for which usability and remote access are a core factor.

Mobile/cellular networks offer us many different services such as voice, text messages and internet access, which are utilized by evermore embedded devices. Still, even today, the cellular world is covered by a dense fog of RF mist. The workshop is aimed at lifting just this fog by teaching all skills necessary for setting up an individual cellular network for penetration testing and free research on various devices. The setup will enable the attendee to do actual phone calls, send text messages and use an actual internet uplink. Above this, being aimed and security, the setup exposes all interfaces and communication for injection and classical Man in the Middle attacks. Starting with basic attacks known from classical IP networks, the course will switch to cellular specific attacks, like text message/SMS fuzzing and the creation of custom OTA messages.

The course is oriented around a few common market devices: GPS trackers, automotive trackers with immobilizers, smart meters and small scale industrial control systems. While demonstrations will be performed on the actual devices, the attendees will work on cellular development boards which basically emulate the behavior identified on the practical device. To be able to use actual cellular communications basestations, custom SIM cards and basic VMs will be provided, together with a cable setup which offers a simple solution for circumventing potential legal issues.

The workshop is aimed at cellular enthusiasts and devs/techs working with cellular devices in general. There are no specific prerequisites, except for basic Linux and networking knowledge.

The following topics will be covered during the training

- Day 1
  - Introduction to cellular networks and their structure
  - Differences between 2G, 3G and 4G networks
  - Network setup and configuration including software and hardware
  - Open network vs. shield box vs. wired setup
  - Network assessment using OsmocomBB
  - SIM card configuration
- Day 2
  - IMSI Catcher / Stingray / Fake Basestation concepts
  - Running an own 2G network with SMS, Data and Voice
  - Forwarding calls to public networks via VoIP
  - Interception of voice calls
  - Introduction to APNs and Security Measures
  - Data interception, injection and MiTM
- Day 3
  - Forwarding text messages to public networks
  - Interception and Injection of text messages
  - Text message / SMS fuzzing
  - General device assessments, pentesting and practical attacks
  - Information on acquiring equipment

Pre-requisite of Training Class: Student / Hardware / Software

- Laptop, with current VirtualBox installation & host extensions
  - Preferably admin permissions on host system, just to be sure
- Basic Linux knowledge
- Basic networking knowledge

We will provide

- Prepared VM
- Basestations
- Cables for connecting devices and basestations
- Test phones
- SIM cards
- DevBoards with cellular connectivity and firmware for training
- Practical case studies