MOBINFSEC: 5G Mobile Networks, Technologies & Security

Kernkonzepte der mobilen Kommunikation

Dr. Florian Wamser, Hochschule Luzern

18. April 2024

5G Mobile Networks, Technologies & Security: Kernkonzepte der mobilen Kommunikation

Letzte Änderung: 18. April 2024

Begleitendes Kursmaterial des Moduls *5G Mobile Networks, Technologies & Security* im Frühlingssemester 2024 an der Hochschule Luzern. Kursmaterial für einen Semesterkurs mit 14 Wochenstunden.

⚠ *Dieses Skript wird während der Vorlesung angepasst und vervollständigt. Neue Kapitel kommen im Verlauf der Vorlesung hinzu.*

Autor: Dr. Florian Wamser, florian.wamser@hslu.ch

Ausgabe 2024

Erstmalige Durchführung im HS22 (2022).

Selbststudium

Ausflug: Mobile Protocol Stack - Was passiert, wenn ich mein Telefon einschalte?

2 Vorwort

Die folgende Einheit ist für das *Selbststudium* konzipiert. Sie lernen individuell und effizient nach Ihrem eigenen Zeitplan. Im Folgenden werden Ihnen Materialien zur Verfügung gestellt, die nach Anleitung durchgearbeitet werden müssen. Am Ende müssen Sie Fragen beantworten und auf die Lernplattform ILIAS hochladen. Nach dem Einreichen Ihrer Lösung erhalten Sie die Musterlösung zum Download.

2.1 Feedback

Mit Ihrer Mithilfe kann die Qualität des Kurses laufend den Bedürfnissen angepasst und verbessert werden.

Sollte etwas in diesem Kurs nicht wie beschrieben funktionieren, melden Sie dies bitte direkt dem Lehrpersonal oder per E-Mail an Florian Wamser (<florian.wamser@hslu.ch>).

2.2 Liste an Lernmaterialien

- Video-Link: Harald Welte - *What happens on a protocol level when I switch on my phone?* (CCC - `Easterhegg 2018`) → https://media.ccc.de/v/ARMP3D
- Gleiches Video als MP4-Download: https://elearning.hslu.ch/ilias/goto.php?target=file_6168388_download&client_id=hslu
- Diese Anleitung zum Selbststudium mit Hintergrundinformationen
- Wissensfragen, die dieser Anleitung am Ende beigefügt sind. Direkt in diesem PDF-Dokument auszufüllen.
- Abgabeformular: https://elearning.hslu.ch/ilias/goto.php?target=exc_6168392

Lesen Sie nun im folgenden die Hintergrundinformationen durch, schauen Sie sich das Video *What happens on a protocol level when I switch on my phone?* (CCC - Easterhegg 2018) von Harald Welte an und beantworten Sie die beigefügten Fragen.

3 Hintergrundinformationen

3.1 Easterhegg

Das Easterhegg (auch Easter(H)egg oder ./easter -h -egg oder EAST erh, egg - kurz einfach EH - genannt) ist eine jährliche internationale Veranstaltung des Chaos Computer Club. Sie findet seit 2001 während der Osterfeiertage statt. Das Easterhegg wendet sich an Hacker und Interessierte.

Die Teilnehmerzahl des Easterheggs beschränkt sich auf mehrere hundert Leute, im Gegensatz zu den grösseren Veranstaltungen des CCC (Chaos Communication Congress), zu denen mehrere tausend Besucher kommen. Auf dem Easterhegg werden Workshops und Vorträge angeboten. Ein Markenzeichen des Easterheggs ist das im Eintrittspreis enthaltene Frühstück bis zum Abend einschliesslich Kaffee-Flatrate, zu der jeder Teilnehmer eine persönliche Erinnerungs-Tasse erhält. Dies soll den gemütlich-kommunikativen Charakter der Veranstaltung betonen.

Im Jahr 2018 fand die Easterhegg (https://eh18.easterhegg.eu) in Würzburg in Deutschland statt. Unter anderem wurde über Themen im Mobilfunk diskutiert.

3.2 Video: *What happens on a protocol level when I switch on my phone?*

Harald Weltes Vortrag *What happens on a protocol level when I switch on my phone?* ist online frei verfügbar und zeigt sehr anschaulich, was passiert, wenn ein Handy eingeschaltet wird. Er zeigt, was tatsächlich auf den Protokollschichten von Mobilfunknetzen passiert, wenn ein (2G/3G)-Telefon eingeschaltet wird. Das Video trägt die folgende Beschreibung:

> *Die meisten Hacker haben im Allgemeinen eine ziemlich gute Vorstellung davon, was auf Netzwerkebene passiert, wenn TCP aufgebaut wird, wie ARP funktioniert und wie der Start einer HTTP-Verbindung aussieht. Aber wie steht es mit dem Verständnis über den Ablauf, wenn sich Ihr Mobiltelefon beim (2G/3G) Mobilfunknetz anmeldet? In diesem Vortrag erfahren Sie Schritt für Schritt, was Ihr Telefon tut.*
>
> *Um die Komplexität zu reduzieren, wird in diesem Vortrag nur 2G/3G vorgestellt, wobei 4G für eine spätere Inkarnation übrig bleibt.*
>
> *Dies ist ein ziemlich technischer Vortrag, aber er richtet sich an Personen ohne oder mit geringem Hintergrundwissen über Mobilfunksysteme oder -protokolle.*

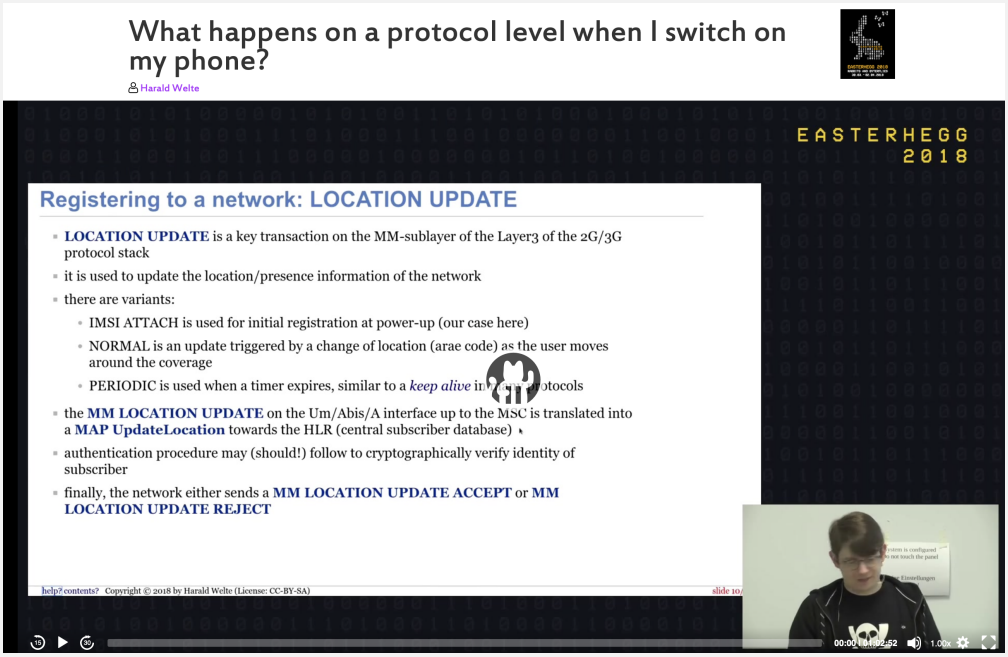

Abbildung 1: Screenshot des Videos *What happens on a protocol level when I switch on my phone?* . Quelle CCC.

Dauer: 62 min
Veröffentlichung: 2018-04-01
URL: https://media.ccc.de/v/ARMP3D

Weitere interessante Videos von Harald Welte finden Sie unter https://media.ccc.de/search?p=Harald+Welte.

4 Wissensfragen

Um die Fragen zu beantworten, schauen Sie sich das Video an und studieren Sie den Inhalt. Ich verweise auf das Internet und die Vorlesungsunterlagen für weitere Informationen. Zum Schluss laden Sie bitte diese Dokument in ILIAS im Abgabeordner hoch, damit Sie die Musterlösung abrufen können.

1. Die Spezifikationen für die verschiedenen Mobilfunkgenerationen sind im Internet frei verfügbar. Release 99 ist beispielsweise die initiale Spezifikation für den UMTS-Mobilfunk.

Wo im Internet kann man die Spezifikation der Mobilfunk-Generationen einsehen?
Tipp: Die Standardisierungsorganisation ist die 3GPP.

2. Die erste Aktion, die ein Smartphone durchführt sobald es eingeschaltet wurde, ist die Zell- und Netzwerkwahl. Beschreiben Sie den Vorgang `Network Selection (2G)` bis das Smartphone die Zelle kennt.

3. Machen Sie sich im Internet auf Wikipedia schlau: Welchen Mobile Country Code (MCC) senden und benutzen alle Mobilfunk-Zellen in der Schweiz? Wie lautet der Mobile Network Code (MNC) für den Schweizer Provider `Salt`?

   MCC Schweiz: _____

   MNC Salt: _____

4. Wie kann ein Telefon feststellen, dass es im Home-Netzwerk eingebucht ist?

5. Welche Funktion hat das `Location Update`?

6. Wie heisst das Pendant der 2G-Einbuchung-Prozedur `IMSI Attach` einer Simkarte bei GPRS, um Daten versenden zu können?

7. Wie lautet der Befehl im 2G-Mobilfunknetz, um den Tunnel aufzubauen, der zwischen Smartphone und GGSN (= Kernnetzelement, das den Zugang zum Internet verwaltet) aufgebaut wird, um Daten zu senden?