

Security of Wireless Networks HS2022

Srdjan Čapkun

Course Info

ML H 44,

Exam:

- 20% exercises and related reports
- 80% final written exam

- You can expect one question / problem per Topic.
- Questions might come from lab sessions.

Course Content

Topic 1. Introduction to Physical Layer of Wireless Networks

Topic 2. Physical Layer Based Security

Topic 3. GNSS (GPS/Gallileo) Security

Topic 4. Cellular Network Security (1-5G)

Topic 5. Security of Distance Measurement (and Positioning)

Topic 6. Jamming and Jamming Resilient Communication

Topic 7. WiFi and Bluetooth Security

+ bonus research topics (if time)

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

Patrick Leu^{1*}, Giovanni Camurati^{1*}, Alexander Heinrich², Marc Roeschlin¹, Claudio Anliker¹, Matthias Hollick², Srdjan Capkun¹, and Jiska Classen²

¹ETH Zurich and ²TU Darmstadt *Contributed equally



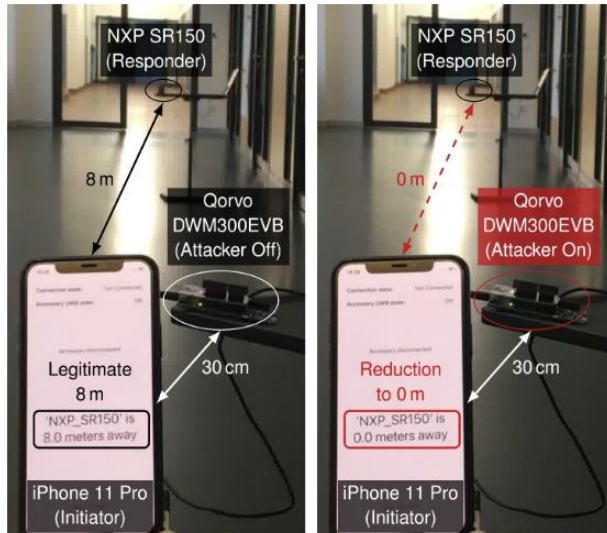
Ghost Peak in a nutshell

Ghost Peak is the first practical distance-reduction attack on IEEE 802.15.4z High-Rate Pulse Repetition (HRP) Ultra-Wide-Band (UWB). With Ghost Peak, an over-the-air attacker can reduce measured distances from a pair of Apple U1 chips (deployed in iPhones, AirTags, and HomePods) by several meters (e.g., 12m to 0m). The same is possible when a U1 chip interoperates with NXP (SR40/150) and Qorvo (DWM3000) chips. Ghost Peak does not leverage any knowledge about cryptographic material, it can be implemented with a 65 USD off-the-shelf device. Ghost Peak brings into question the use of HRP UWB for access control (e.g., car entry and start), mobile payments, and other security-critical applications.

[USENIX Security 2022 Paper](#)

[ESCAR 2021 Slides](#)

[CANS 2021 Keynote](#)



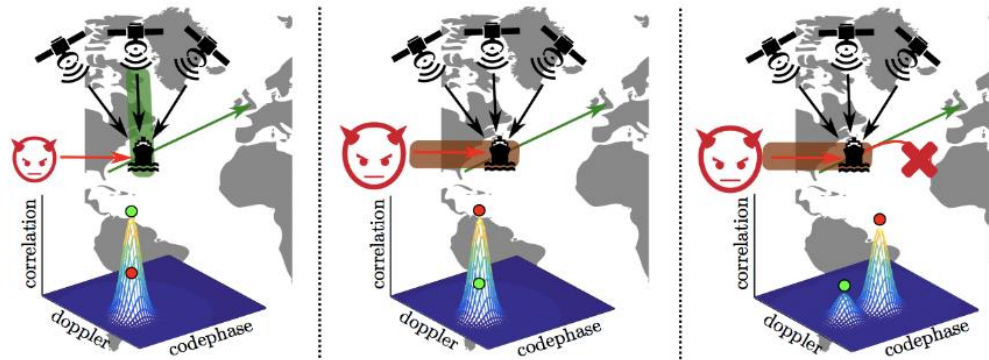
Security of Global Navigation Satellite Systems

The Problem

Today, it is possible to spoof a GPS receiver to any arbitrary location. Check out the video we created to demonstrate how trivial it is to spoof GPS signals today! The increasing availability of low-cost radio hardware platforms make it feasible to execute such attacks with less than few hundred dollars worth of hardware equipment.

Selected Projects






SPREE: A Spoofing Resistant GPS Receiver



Global Positioning System (GPS) is used ubiquitously in a wide variety of applications ranging from navigation and tracking to modern smart grids and communication networks. However, it has been demonstrated that modern GPS receivers are vulnerable to signal spoofing attacks. For example, today it is possible to change the course of a ship or force a

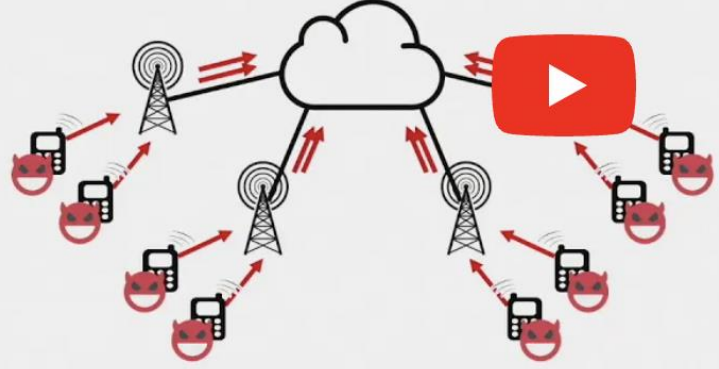
“...the GPS receiver is vulnerable to signal spoofing attacks. For example, today it is possible to change the course of a ship or force a

Presentation Video


USENIX Security '19 - Hiding in Plain Signal: Physical Signal Ov...Watch onShareTHE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Signaling Storm

- Using a botnet in general



26 / 36



Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Authors:

Hoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim, KAIST

Abstract:

Long-Term Evolution (LTE) communication is based on an open medium; thus, a legitimate signal can potentially be counterfeited by a malicious signal. Although most LTE signaling messages are protected from modification using cryptographic primitives, broadcast messages in LTE have never been integrity protected. In this paper, for the first time, we present a signal injection attack that exploits the fundamental weaknesses of broadcast messages in LTE and modifies a transmitted signal over the air. This attack, which is referred to as signal overshadowing (named *sigover*) has several advantages and differences when compared with existing attacks using a fake base station. For example, with a 3 dB power difference from a legitimate signal, the *sigover* demonstrated a 98% success rate when compared with the 80% success rate of attacks achieved using a fake base station, even with a 35 dB power difference. Given that the *sigover* is a novel primitive attack, it yields five new attack scenarios and implications. Finally, a discussion on two potential countermeasures leaves practical and robust defense mechanism as a future work.

Labs - Content

The labs comprise the following topics:

- Lab 1: Introduction to Software Defined Radios (SDRs)
- Lab 2: Jamming-Resistant Communication
- Lab 3: Global Positioning System (GPS) Spoofing
- Lab 4: Signal Overshadowing in Cellular Networks

We strongly encourage you to read the lab instructions published on Moodle before the sessions.

Labs - Schedule / Administration

The labs will be completed in groups of two

- Groups are going to be created on Moodle
- You can team up on your own. If you don't find a partner, let us know.
- We will inform you once you can register for your favorite session.
- The registration window for the lab sessions will open after the second lecture (27.09.2022). Information regarding the registration will be published on Moodle beforehand.

Labs - Schedule / Administration

The lab sessions are going to be held **bi-weekly on Fridays starting from 07.10.2022 and 15.10.2022**, respectively, in up to eight sessions. There is a limit of 6 groups (12 students) per session.

Session	Start Date	Time
Lab Session A	07.10.2022	08:15-10:00
Lab Session B	07.10.2022	10:15-12:00
Lab Session C	07.10.2022	13:15-15:00
Lab Session D	07.10.2022	15:15-17:00
Lab Session E	15.10.2022	08:15-10:00
Lab Session F	15.10.2022	10:15-12:00
Lab Session G	15.10.2022	13:15-15:00
Lab Session H	15.10.2022	15:15-17:00

Lab - Exercises

For every lab, there are going to be questions on Moodle that you have to answer.

- It is sufficient if one of the two students submits their answers.
- They will be graded and account for 20% of your final mark.
- Questions will mostly be open text: Try to answer them thoroughly but concisely.
- We encourage you to discuss the labs with your fellow students, but you must not share complete solutions.