Simple Replay Attack Demo with GNU Radio

Murat Sever
GRCon'25

N-Ways to Perform an RF Replay Attack

Murat Sever
GRCon'25

Outline

- Who am I?
- Replay Attacks
- Notebook
- Resources

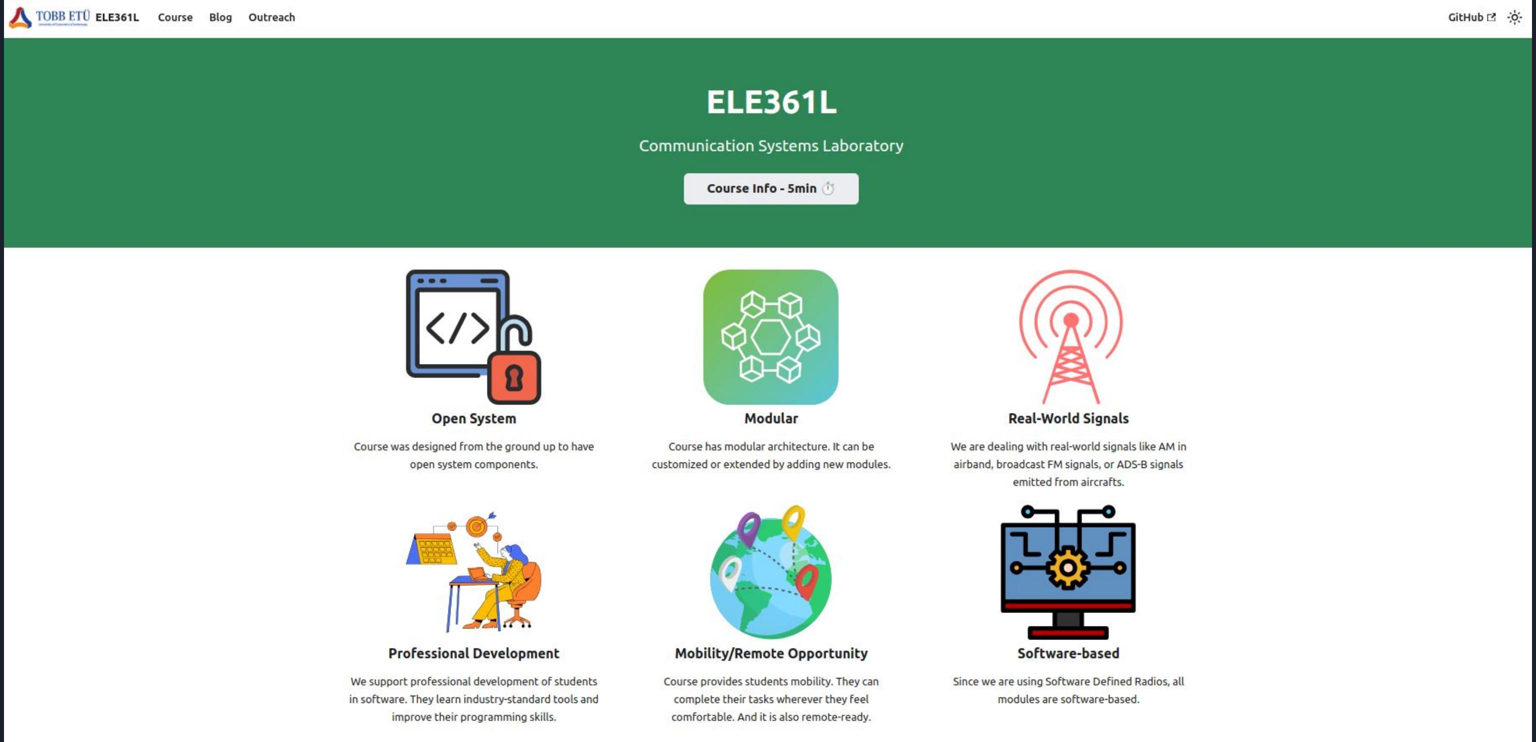
TOBB ETU, Ankara, Turkey

Lecturer @

TOBB ETÜ

Ekonomi ve Teknoloji Üniversitesi

ELE361L: ele361l.github.io



ELE361L

Communication Systems Laboratory

Course Info - 5min

Open System

Course was designed from the ground up to have open system components.

Modular

Course has modular architecture. It can be customized or extended by adding new modules.

Real-World Signals

We are dealing with real-world signals like AM in airband, broadcast FM signals, or ADS-B signals emitted from aircrafts.

Professional Development

We support professional development of students in software. They learn industry-standard tools and improve their programming skills.

Mobility/Remote Opportunity

Course provides students mobility. They can complete their tasks wherever they feel comfortable. And it is also remote-ready.

Software-based

Since we are using Software Defined Radios, all modules are software-based.

Events: GNU Radio Conference 2023

GRCon23
TEMPE, ARIZONA

5-9 September 2023

Talk & Workshop

Outreach Program

My Sponsors

ARDC

AMATEUR RADIO DIGITAL COMMUNICATIONS

GREAT SCOTT GADGETS

Replay Attack

- Definition: previously captured RF signal is retransmitted to trigger the same action

Setup

- HackRF
- Remote
- LED

Steps

1. Monitor
2. Capture
3. Check
4. Replay

1. Monitor

- Understand where the communication takes place

2. Capture

- Instead of live transmission
- Save the signal onto disk

3. Check

- Inspect your capture

4. Replay

- You need a transmit-capable SDR to replay
- Simple
  - GNU Radio
  - hackrf_transfer
  - Flipper Zero
  - URH
- Advanced
  - rtl_433 / inspectrum / URH for decoding
  - GNU Radio

Notebook Time!

- Interactive
- Step-by-step instructions
- Solutions
- Capture or use the record supplied

Links

SDR General

- Software Defined Radio with HackRF - 11 Lessons

Replay Attacks

- Studying radio communications with GNURadio and SDR
- Impersonating a remote using SDR and GNURadio
- Black Hat Arsenal Lab – Tire Pressure Sensors!

Teşekkürler!
Thanks!

Murat Sever

TOBB ETU

ytregitim@gmail.com

Find me on LinkedIn