FURKAN GÖKSEL

furkan.goksel27@gmail.com
github.com/frkngksl ◇ linkedin.com/in/frkngksl/ ◇ exploit-db.com/?author=10891

EDUCATION

Middle East Technical University, Ankara *2016 - 2021*
Department of Computer Engineering CGPA: 3.88 (2nd Top Student in the Department)

PROJECTS

Process Tracer
The project aims to monitor and manipulate the system calls made by a Linux Process through a browser-based interface. With such a manipulation option, the project provides researchers to ease analyzing the system calls of the suspicious programs. The project is fully written in C language.

AgriLoRa: A Smart Agriculture Framework (published by Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications's next volume)
This project aims to develop a complete cost-effective Smart Agriculture Solution. In this project, I'm responsible for establishing Wireless Sensor Network using LoRa modules. More specifically, I am trying to add new Ad-Hoc routing protocols for communication between LoRa gateways. The novelty is standard LoRaWAN protocol uses star topology, but AgriLoRa uses mesh topology to eliminate Internet connection necessity.

On the Safety Implications of Misordered Events and Commands in IoT Systems (published by SafeThings 2021: IEEE Workshop on the Internet of Safe Things)
This project aims to solve ordering problems in IoT systems components, espacially for Smart Home environments. It was my summer internship research project in Purdue University under the advisorship of Asst. Prof. Z. Berkay Celik.

Web Application Firewall Administration Tool (WAFADM)
This project aims to ease the usage of ModSecurity Web Application Firewall by implementing rule compilers, generators, access zones and new functionalities. This is my graduation project under the advisorship of Dr. Onur Tolga Şehitoğlu. It is the winner of METU CENG Demo Day 2021.

Shoggoth
This project aims to evade static check of security solutions against different file types. I presented this tool in the BlackHat Europe 2022 Arsenal.

TECHNICAL STRENGTHS

Simulation OmNet++
Languages C, C++, Python, MySQL, PIC Assembly, x86 Assembly, Java, Lua, Nim

WORK EXPERIENCE

Picus Security, Ankara January 2023 - Present
Senior Red Team Engineer

· Working on CTI Validation, Lateral Movement Simulations, Windows and MacOS Endpoint Attacks.

Picus Security, Ankara March 2021 - January 2023
Red Team Engineer

· Working as a part of Red Team, specifically for endpoint attacks.

Asst. Prof. Z. Berkay Çelik, Purdue University July 2020 - October 2020
Undergraduate Student Researcher

· I had been doing a research about IoT systems and their security.

Secrove Information Security Consulting, Istanbul Mar 2020 - September 2020
Security Researcher

· Working in an EDR project of the company and researching new security areas.

Secrove Information Security Consulting, Istanbul Mar 2019 - September 2019
Intern

· During my internship, I performed penetration tests for mobile and web applications. Also, I developed Process Tracer here.

PRESENTATIONS / TALKS

A New Approach to Dynamic Analysis: Process Tracer
BSCon2020

· I have made a presentation about system calls, manipulation of them and an analysis tool, that is written by me, Process Tracer.

On the Safety Implications of Misordered Events and Commands in IoT Systems
SafeThings2021

· I have made a presentation about our findings on the simulation environment. I generally summarized the paper.

Shoggoth: Asmjit Based Polymorphic Encryptor
BlackHat Europe 2022 Arsenal

· I have made a presentation about my new research tool and polymorphic approach to static control bypasses.

PUBLICATIONS

AgriLoRa

· Pelin Angin, Mohammad Hossein Anisi, **Furkan Göksel**, Ceren Gürsoy,and Asaf Büyükgülcü. Agrilora: A digital twin framework for smartagriculture.Journal of Wireless Mobile Networks, Ubiquitous Computing,and Dependable Applications (JoWUA), 11(4):77–96, December 2020.

On the Safety Implications of Misordered Events and Commands in IoT Systems

· **Furkan Goksel**, M. Ozgur Ozmen, Michael Reeves, Basavesh Shivakumar and Z. Berkay Celik. IEEE Workshop on the Internet of Safe Things, 2021

CERTIFICATES

- Certified Red Team Professional (CRTP) - February 2022
- OffSec Certified Professional (OSCP) - March 2023

- Certified Red Team Operator (CRTO) - August 2023

AWARDS / HONORS

- GUIDED2020: 2nd Guided Research Symposium 1st place with project AgriLoRa
- ICS & IoT Cyber Security Bootcamp CTF: Blackout 1st place with team KöpükRF
- METU CENG Demo Day 2020 1st place with project WAFADM

CVES

- CVE-2020-35597: Multiple SQL Injections on Victor CMS
- CVE-2021-30461: VoIPmonitor UnAuth RCE
- CVE-2022-31464: Adaware Protect Local Privilege Escalation
- CVE-2022–34008: Comodo Antivirus Local Privilege Escalation Through Insecure File Move