

Emre Süren

✉ E-mail | 🔗 LinkedIn | 🐙 GitHub | 🎓 Scholar | 📁 Portfolio | 📍 Stockholm, Sweden

RESEARCH INTERESTS

Vulnerability discovery, Exploit development, Digital forensics, IoT, AI-based cybersecurity applications, open-source, and Capture the Flag (CTF).

EDUCATION

- Ph.D. in Information Systems (Cybersecurity)** 2014 – 2019
Middle East Technical University 🌐 📍 Ankara, Turkey
A novel and efficient detection technique for zero-day web-based exploit kit families
- Master's in Information Systems (Cybersecurity)** 2014 – 2019
Middle East Technical University 🌐 📍 Ankara, Turkey
Detection of malicious web pages
- Bachelor in Computer Engineering** 2012 – 2014
Hacettepe University 🌐 📍 Ankara, Turkey

EMPLOYMENT

- Postdoctoral Researcher** 2020 – 2023
KTH Royal Institute of Technology 🌐 📍 Stockholm, Sweden
School of Electrical Engineering and Computer Science
- Principal Lecturer** 2017 – 2020
Hacker School & Freelance 🌐 📍 Turkey
- Senior Engineer (Incident Response & Threat Intelligence Analyst)** 2013 – 2017
HAVELSAN 🌐 📍 Ankara, Turkey
Turkish Air Force Cyber Defense Command
- Researcher (Penetration Tester)** 2007 – 2013
TUBITAK 🌐 📍 Ankara, Turkey
National Cybersecurity Institute

PUBLICATIONS

Journals

- [5] F. Heiding, **E. Suren**, J. Olegård, R. Lagerström. *Penetration testing of connected households*. Computers & Security, 126:103067, February 2023
- [4] **E. Suren**, F. Heiding, J. Olegård, R. Lagerström. *PatIoT: Practical and agile threat research for IoT*. International Journal of Information Security (IJIS'22), 213–233, December 2022
- [3] **E. Suren**. *ZEKI: Unsupervised Zero-day Exploit Kit Intelligence*. Turkish Journal of Electrical Engineering & Computer Sciences (TJEECS'20), 28(5):1859-1870, March 2020
- [2] **E. Suren**, P. Angin, N. Baykal. *I see EK: A Lightweight Technique to Reveal Exploit Kit family by Overall URL Patterns of Infection Chains*. Turkish Journal of Electrical Engineering & Computer Sciences (TJEECS'19), 27(5):3713-3728, September 2019
- [1] **E. Suren** and P. Angin. *Know Your EK: A Content and Workflow Analysis Approach for Exploit Kits*. Journal of Internet Services and Information Security (JISIS'19), 9(1):24–47, February 2019

Conference Proceedings

[1] Ciklabakkal, Ege and Donmez, Ataberk and Erdemir, Mert and **Suren, Emre** and Yilmaz, Mert Kaan and Angin, Pelin. *ARTEMIS: An intrusion detection system for MQTT attacks in Internet of Things*. 38th Symposium on Reliable Distributed Systems (SRDS'19), 369-3692, *October 2019*

FUNDING

DFIRent - Next-generation AI-assisted Digital Forensics Tools		<i>2024 – 2029</i>
Agency	European Union - DIGITAL Europe ☞	
Fund	6M € in total / 1.5M € our share In preparation	
PIs	Emre Süren, to be determined	
Role	Task leader	
Objective	AI-based digital forensics on current operating systems, memory, and IoT devices	
AI²IoT – AI-based IoT Vulnerability Exploitation		<i>2024 – 2029</i>
Agency	European Research Council - Starting Grant ☞	
Fund	1.5M € In preparation	
PIs	Emre Süren	
Role	Project leader	
Objective	Developing AI-based methods and tools for IoT vulnerability discovery	
IoT VR – Vulnerability Research on Consumer IoT Devices		<i>2024 – 2026</i>
Agency	Swedish Research Council – Cyber and Information Security ☞	
Fund	1.4M SEK (~0.14K €) Pending	
PIs	Emre Süren	
Role	Project leader	
Objective	Vulnerability research on current IoT hardware, firmware, and radio protocols	
EnergyShield – Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring, and Protection of Critical Energy Infrastructures		<i>2019 – 2022</i>
Agency	European Union – Horizon 2020 ☞	
Fund	8M € in total / ~0.6M € our share EU funding	
PIs	Robert Lagerström (PostDoc supervisor)	
Role	Senior researcher & Task leader	
Objective	Vulnerability research on European energy utilities	
VASA – Viable cities and Attack Simulation & threAt modeling		<i>2020 – 2022</i>
Agency	Swedish Energy Agency – Viable Cities Program ☞	
Fund	6M SEK (~0.6M €) National funding	
PIs	Robert Lagerström (PostDoc supervisor)	
Role	Senior researcher & Project leader	
Objective	Vulnerability research on smart building devices	

TEACHING

KTH Royal Institute of Technology

- [EP2780 - Graduate] Digital Forensics and Incident Response ☞ *2022*

Hacker School & Freelance

- Digital Forensics and Incident Response *2017 – 2020*
- Web Application Hacking *2017 – 2020*
- Ethical Hacking (Penetration Testing) *2017 – 2020*

Graduate | 🔗

- | | |
|---|-------------|
| [7] Exploiting memory corruption bugs for remote code execution on IoT firmware
<i>Erik Mickols, KTH</i> | 2023 – 2023 |
| [6] Penetration testing smart thermostats
<i>Adam Lindberg, KTH</i> | 2023 – 2023 |
| [5] Nationwide password patterns of Swedish people
<i>Daniel Gustafsson, KTH</i> | 2022 – 2022 |
| [4] Automated security analysis of firmware
<i>Farrokh Bolandi, KTH</i> | 2022 – 2022 |
| [3] (Classified) Hacking the airport X-ray machine
<i>Felix Zuber, KTH</i> | 2022 – 2022 |
| [2] Threat modeling and penetration testing of an IoT product. Yanzi IoT network
<i>Diyala Isabar, KTH</i> | 2021 – 2021 |
| [1] Security analysis of a Beckhoff CX-9020 programmable logic controller
<i>Liam Carter, KTH</i> | 2021 – 2021 |

Undergraduate

- | | |
|--|-------------|
| [3] Penetration testing of ten popular Swedish Android applications
<i>Alexander Astély & Johan Ekroth, KTH</i> | 2022 – 2022 |
| [2] Security evaluation of ten Swedish mobile applications
<i>Jens Ekenblad & Stefan Andres Garrido Valenzuela, KTH</i> | 2022 – 2022 |
| [1] Trends and scientometrics in cyber security research
<i>Jesper Slagarp & Elvira Häggström, KTH</i> | 2021 – 2022 |

ACADEMIC SERVICE

Technical Program Committee

- | | |
|--|-------------|
| • International Symposium on Networks, Computers and Communications (ICNCC) 🔗
<i>Member</i> | 2023 |
| • DFIR Review (DFIRR) 🔗
<i>Member</i> | 2023 |
| • ADFSL Conference on Digital Forensics, Security and Law 🔗
<i>Member</i> | 2022 – 2023 |
| • Swedish National Computer Networking Workshop (SNCNW) 🔗
<i>Co-chair</i> | 2022 |

Reviewer

- | | |
|--|-------------|
| • IEEE Security & Privacy (S&P) 🔗 | 2023 |
| • Information Security Journal: A global perspective (ISJGP) 🔗 | 2023 |
| • Computer Science Review (CSR) 🔗 | 2022 – 2023 |

- International Journal of Critical Infrastructure Protection (IJCIP) ☞ 2022
- Business & Information Systems Engineering (BISE) ☞ 2022
- Practice of Enterprise Modelling Conference (PoEM) ☞ 2022
- IEEE Int. Enterprise Distributed Object Computing Conference (EDOC) ☞ 2022
- IEEE Wireless Communications and Networking Conference (WCNC) ☞ 2022

Administrative Service & Membership

- European Union Agency for Cybersecurity (ENISA) ☞ 2023 – current
CEI Listed expert
- KTH NSE Cybersecurity lab ☞ 2020 – 2023
Member & Author
- Turkish Criminal Courts ☞ 2014 – 2019
Authorized digital forensics specialist

INVITED TALKS & PANELS

- CTF Competitions for Cybersecurity Education 2022
Education Track - KTH EECS Summer Event 2022

EVENTS ORGANIZED

- EU Cyber Attaché Exercise 2023
KTH - CDIS Cyber range Stockholm
- Turkish National Cybershield Exercise 2017
Hacker School Ankara
- Turkish Military Cybershield Exercise 2015
HAVELSAN Ankara
- Turkish National Cybershield Exercise 2013
TUBITAK Ankara

PERSONAL DEVELOPMENT

Private Training


- Burp Suite Certified Practitioner 2021
PortSwigger Online
- Advanced Web Attacks and Exploitation (OSWE) 2021
OffSec Online
- Penetration Testing with Kali Linux (OSCP) 2019
OffSec Online
- Reverse Engineering Malware 2016
SANS Las Vegas
- Customized Malware Analysis 2016
Mandiant Ankara

- Enterprise Incident Response 2015
Mandiant Ankara
- Network Penetration Testing and Ethical Hacking 2013
SANS Bootcamp
- Web App PenTesting and Ethical Hacking 2012
SANS Washington DC
- Security Essentials 2011
SANS Bootcamp


Certificates (GIAC profile | Acclaim profile)

- Certified Ethical Hacker (CEH) v10 2018
- GIAC Reverse Engineering Malware (GREM) 2016
- TSE Certified Penetration Test Expert – Network & System 2015
- TSE Certified Penetration Test Expert – Web & Database 2015
- GIAC Penetration Tester Certification (GPEN) 2013
- GIAC Web Application Penetration Tester (GWAPT) 2012
- GIAC Security Essentials (GSEC) 2011
- Certified Ethical Hacker (CEH) v7 2011




Discovered vulnerabilities

- TwinCAT OPC UA Server  2021
CVE-2021-34594 - Unauthenticated any file manipulation through relative path traversal

Exploit development

- Ruckus IoT Controller (Ruckus vRIoT) 1.5.1.0.21  2020
Remote Code Execution

Open-source security research tools

- **Memopsy.** Memory forensics tool.  2023
Owner
- **PatrIoT.** IoT vulnerability research methodology.  2021
Owner
- **Grauditi.** Offensive source code review tool.  2020
Contributor