

EVANGELOS BITSIKAS

Boston, United States of America

(+1)8573812731 ◊ vaggelisbtk@gmail.com, bitsikas.e@northeastern.edu

SUMMARY

Cybersecurity researcher and PhD Fellow at Northeastern University, specializing in wireless network security, drone/robotic communications, and machine learning in security. Demonstrated impact through real-world vulnerability disclosures, peer-reviewed publications, and patent-level innovation.

WORK EXPERIENCE

Doctoral Researcher, Northeastern University *Sep. 2022 - Present*

- Conducting advanced research on Cellular/Mobile Networks and Security within the Signal Intelligence Lab.
- Developed and implemented novel network attack vectors (e.g., SMS privacy attacks) and corresponding defense mechanisms. Extensive use of Machine Learning techniques offensively and defensively.
- Designed dynamic cellular networks for M2M missions and operations.
- Created security over-the-air testing frameworks to identify 5G vulnerabilities in mobile devices.

Research Assistant, New York University (Abu Dhabi) *Aug. 2019 - Aug. 2022*

- Conducted in-depth research on Cellular, Mobile, and Aviation Security as a full-time member of the CSP-Lab (supervised by Christina Pöpper).
- Led projects focusing on LTE/5G security, identifying and mitigating unique attacks and vulnerabilities.
- Investigated ADS-B and jamming incidents, contributing to enhancements in aviation security.

Research Assistant, Athens University of Economics and Business *Mar. 2017 - Aug. 2019*

- Engaged in security research in the AUEB Infosec Labs, focusing on Industrial Control Systems and malware detection.
- Developed Machine Learning-based Intrusion Detection Systems (IDS) to identify malicious network traffic.
- Conducted side-channel attacks against Modbus systems to evaluate privacy leakage and system vulnerabilities.

EDUCATION

Northeastern University *Sep. 2022 - Present*

Ph.D. in Cybersecurity

— Advisor: Aanjhan Ranganathan

M.S. in Cybersecurity

Dec. 2024

King's College London

PG.Cert. in Advanced Cybersecurity

Jul. 2021 - Apr. 2022

Athens University of Economics and Business

B.Sc. in Computer Science

— Thesis: Side channel attacks on network traffic on ICS/SCADA systems for privacy leakage

— Advisors: George Stergiopoulos & Dimitris Gritzalis

Sep. 2013 - Nov. 2018

CORE SKILLS

Programming Languages: C/C++, Python, Assembly X86, Java

Wireless Security: Cellular Networks (LTE, 5G), Aviation Security, WiFi 802.11

Selected Tools: Wireshark, Aircrack-ng, CoWPAtty, srsRAN, OpenAirInterface, Amarisoft, Open5GS, Kismet

Network Security & Penetration Testing: Vulnerability Discovery and Exploitation with Kali Linux

Selected Tools: Nmap, Burp Suite, Metasploit Framework, Nessus, Wireshark, OpenVAS, Hydra, John the Ripper

Software Exploitation: Reverse Engineering, Software Vulnerabilities (e.g., Buffer Overflows), Exploitation and Fuzzing
Selected Tools: GDB, Ghidra, IDA Pro, AFL, OllyDbg, Valgrind

Artificial Intelligence & Machine Learning: Machine Learning in Cybersecurity Aspects
Selected Tools: Keras, Scikit-learn, TensorFlow, PyTorch

Soft Skills: Problem-solving, Critical Thinking, Effective Communication, Teamwork, Leadership, Adaptability

PUBLISHED WORKS

[1] **Amplifying Threats: The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks.** Bitsikas E., Schnitzler T., Pöpper C., Ranganathan A., USENIX WOOT Conference on Offensive Technologies, Philadelphia PA USA, August 2024 [🔗](#)

[2] **ASTRA-5G: Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices.** Khandker S., Guerra M., Bitsikas E., Jover Piqueras R., Ranganathan A., and Pöpper C., Security and Privacy in Wireless and Mobile Networks (WiSec), Seoul Korea, May 2024 [🔗](#)

[3] **Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings.** Bitsikas E., Schnitzler T., Pöpper C., Ranganathan A., USENIX Security Symposium, Anaheim CA USA, August 2023 [🔗](#)

[4] **UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework.** Bitsikas E., Khandker S., Salous A., Ranganathan A., Jover Piqueras R., and Pöpper C., Security and Privacy in Wireless and Mobile Networks (WiSec), Guildford Surrey UK, May-June 2023 [🔗](#)

[5] **Hope of Delivery: Extracting User Locations From Mobile Instant Messengers.** Schnitzler T., Kohls K., Bitsikas E., and Pöpper C., Network and Distributed System Security Symposium (NDSS), San Diego CA USA, February 2023 [🔗](#)

[6] **You have been warned: Abusing 5G's Warning and Emergency Systems.** Bitsikas E., and Pöpper C., Annual Computer Security Applications Conference (ACSAC), Austin TX USA, December 2022 [🔗](#)

[7] **Don't hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications.** Bitsikas E., and Pöpper C., Annual Computer Security Applications Conference (ACSAC), Virtual USA, December 2021 [🔗](#)

[8] **On ADS-B Sensor Placement for Secure Wide Area Multilateration.** Darabseh A., Bitsikas E., Tedongmo B. and Pöpper C., 8th OpenSky Symposium, Belgium 2020 [🔗](#)

[9] **Detecting GPS Jamming Incidents in OpenSky Data.** Darabseh A., Bitsikas E., and Tedongmo B., In Proceedings of the 7th OpenSky Workshop, vol. 67, pp. 97-108. Switzerland 2019 [🔗](#)

[10] **Using side channel TCP features for real-time detection of malware connections.** Stergiopoulos G., Chronopoulou G., Bitsikas E., Tsalis N. and Gritzalis D., Journal of Computer Security, Vol. 27, no. 5, pp. 507-520, 2019 [🔗](#)

[11] **Automatic Detection of Various Malicious Traffic Using Side Channel Features on TCP Packets.** Stergiopoulos G., Talavari A., Bitsikas E., Gritzalis D., European Symposium on Research in Computer Security (ESORICS), Spain 2018 [🔗](#)

[12] **Side Channel Attacks over Encrypted TCP/IP Modbus Reveal Functionality Leaks.** Tsalis N., Stergiopoulos G., Bitsikas E., Gritzalis D. and Apostolopoulos T., Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, 2018 [🔗](#)

PRE-PRINT WORKS

[1] **Security Analysis of 5G NR Device-to-Device Sidelink Communications.** Bitsikas E., Ranganathan A., Arxiv Version 2025 [🔗](#)

[2] **Dyna-5G: A Dynamic, Flexible, and Self-Organizing 5G Network for M2M Ecosystems.** Bitsikas E., Belfki A., Ranganathan A., Arxiv Version 2024 [🔗](#)

PATENTS

Cellular User Localization System: SMS Side-Channel Timing Analysis Method And Apparatus

US Patent No: US-20250063327-A1 [↗](#)

Publication Date: 2/20/2025

Description: This patent establishes an innovative approach for an authentication-localization mechanism using SMS timing analysis.

CERTIFICATIONS

The Fundamentals of Software Exploitation, RET2 Systems

Certificate ID: 110A21CDC348AF8CA41303BC68C2308E

Stanford Advanced Cybersecurity Certificate, Stanford University

Network Defense Professional (eNDP), eLearnSecurity

Certificate ID: 9369766

VHL Certificate of Completion, Virtual Hacking Labs

Certificate ID: 2085933024

SWSE, WiFi security and pentesting, Pentester Academy

Certificate ID: SWSE-10327

Advanced Infrastructure Hacking, NotSoSecure, Black Hat Training 2016

PROFESSIONAL TRAININGS

OffSec Proving Grounds: Virtual Pentesting Labs

Currently: 47 Hashes, 29 Hosts, 334 Points.

ACSAC 2024: TracerFIRE (Forensic and Incident Response Exercise)

RET2 Systems: WarGames

Completed 40+ binary challenges on software exploitation.

Hack-the-Box: Penetration Testing

Main: 64 root-compromised, and 2 user-compromised machines

Academy: HTB Certified Penetration Testing Specialist Path (CPTS)

Academy: Introduction to Binary Fuzzing

Academy: Stack-Based Buffer Overflows on Linux x86

Academy: Stack-Based Buffer Overflows on Windows x86

INE: Malware Analysis

Zero2Automated: Advanced Malware Analysis

HONORS, AWARDS & GRANTS

Research Grants

[1] Google PhD Fellowship Program

Awarded by Google, 2024

Recognition for outstanding research in Security and Networking [↗](#)

[2] Android Security and Privacy Research (ASPIRE)

Awarded by Google, 2021

Development of a security testing platform for 5G devices.

Role: Co-author & Implementation Leader [↗](#)

Honors and Awards

[1] GSMA Mobile Security Research Acknowledgements

Recognition for significant contribution in mobile industry: CVD-2024-0098

[2] ACSAC 2024 Conferenceship Award

Award of \$2, 350 for selected candidates

[3] EB NIW (National Interest Waiver) Approval

Recognition by the United States Citizenship and Immigration Services (USCIS) of the academic profile as part of the green card process

[4] NDSS 2024 Student Support Award

Award of \$2, 000 for selected candidates

[5] Cyber Security Awareness Week 2023 (CSAW'23)North America *Finalist* in the Applied Research Competition (6.2% Acceptance Rate)**[6] GSMA Mobile Security Research Acknowledgements**

Recognition for significant contribution in mobile industry: GSMA-2023-0072

[7] AERPAW Community Workshop 2023 Award

Selected and NSF-funded for training

[8] Cyber Security Awareness Week 2021 (CSAW'21)MENA *Finalist* in the Applied Research Competition**SERVICES**

Paper Peer Reviewer

MDPI Journal of Mathematics	<i>2025</i>
IEEE Transactions on Information Forensics & Security	<i>2024</i>
External – ACM Conference on Computer and Communications Security (CCS)	<i>2024</i>
IEEE Transactions on Information Forensics & Security	<i>2023</i>
ACM Transactions on Privacy and Security	<i>2023</i>
IEEE/ACM Transactions on Networking	<i>2023</i>

Committees

USENIX Security Artifact Evaluation Program Committee	<i>2025</i>
NDSS Artifact Evaluation Program Committee	<i>2025</i>
Northeastern University PhD Admission Committee	<i>2023-2024</i>
Northeastern University Tenure Track Hiring Committee	<i>2023-2024</i>
USENIX Security Artifact Evaluation Program Committee	<i>2024</i>

Teaching

TA – CS 4760/6760 Security of Wireless and Mobile Systems, Northeastern University	<i>Fall 2024</i>
TA – CS 4760/6760 Wireless and Mobile Network Security, Northeastern University	<i>Spring 2024</i>
TA – CS-UH 3210 Computer Security, New York University (Abu Dhabi)	<i>Fall 2019</i>

Conference Organization

Technical Session Coordinator – Security and Privacy in Wireless and Mobile Networks (WiSec)	<i>2021</i>
--	-------------

Memberships

USENIX Association member

TALKS & PRESENTATIONS

Past, Current and Future Works in Wireless and Cellular Security

Verizon-Northeastern Co-Op Program 2023, Boston MA, USA

Extracting User Locations by Analyzing SMS Timings

NYU CSAW 2023, New York NY, USA

USENIX 2023, Anaheim CA, USA

UE Security Reloaded

ACM WiSec 2023, Guildford, UK

Security in Cellular Networks

ACW 2023, NC State University, USA

Security of 5G Emergency Systems

ACSAC 2022, Austin, TX

Vulnerabilities in the Handover Procedure of Cellular Telecommunications

NYU CSAW MENA 2021, Virtual

ACSAC 2021, Virtual

On ADS-B Sensor Placement for Secure Wide Area Multilateration

8th OpenSky Symposium 2020, Belgium

VULNERABILITY DISCLOSURES

Multiple Vulnerabilities in 5G NR Sidelink.

Research Work: Security Analysis of 5G NR Device-to-Device Sidelink Communications

Procedure: GSMA Coordinated Vulnerability Disclosure

Disclosure: CVD-2024-0098 [↗](#)

SMS Timing Attacks on Mobile Networks for Location Identification.

Research Work: Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings

Procedure: GSMA Coordinated Vulnerability Disclosure

Disclosure: CVD-2023-0072 [↗](#)

Attacks and Vulnerabilities of 5G's Emergency Systems.

Research Work: You have been warned: Abusing 5G's Warning and Emergency Systems

Procedure: Federal Communications Commission (FCC)

Disclosure: "FCC Acts to Strengthen the Security of Nation's Alerting Systems" (11/27/2022) [↗](#)

SELECTED PRESS ATTENTION

The Hacker News

New Mobile Network Vulnerabilities Affect All Cellular Generations Since 2G [↗](#)

Google Security Blog

Android 14 introduces first-of-its-kind cellular connectivity security features [↗](#)

The Economic Times

New smartphone vulnerability could let hackers track your location [↗](#)

Restore Privacy

Timing Attacks on WhatsApp, Signal, and Threema can reveal user location [↗](#)

Northeastern Global News

Northeastern doctoral student studying cybersecurity and wireless networks awarded prestigious Google Fellowship [↗](#)

LANGUAGES

Greek (Native), **English** (Full Professional Proficiency), **German** (Intermediate), **Latin** (Intermediate),
Russian (Elementary)

SOCIAL MEDIA

Personal Website  **LinkedIn**  **Github**  **Google Scholar** 