EVANGELOS BITSIKAS

Boston, United States of America
(+1)8573812731, (+30)6975578449 ⋄ vaggelisbtks@gmail.com, bitsikas.e@northeastern.edu

WORK EXPERIENCE

Research Assistant, New York University (Abu Dhabi) ***Aug. 2019 - Aug. 2022***
Conducted comprehensive research in *Cellular, Mobile, and Aviation Security* as a full-time member of the CSP-Lab (Center for Cyber Security). Lead projects on LTE/5G security related to novel attacks and defenses resulting in publications. Worked also on ADS-B and jamming incidents for aviation.

Research Assistant, Athens University of Economics and Business ***Mar. 2017 - Aug. 2019***
Engaged in security research focusing on *Industrial Control Systems*, *Computer Networks*, and *Malware* detection using *Machine Learning* within the AUEB Infosec Labs. Worked on ML-based Intrusion Detection Systems (IDS) to uncover malicious network traffic, and on side-channel attacks against Modbus.

EDUCATION

Northeastern University ***Sep. 2022 - Present***
Ph.D in Cyber Security
Thesis: –
GPA: 3.96/4.0

Northeastern University ***Sep. 2022 - Present***
M.Sc. in Cyber Security (Part of Ph.D)
GPA: 3.96/4.0

King's College London ***Jul. 2021 - Apr. 2022***
PG.Cert. in Advanced Cyber Security
Coursework: Security Engineering, Network Security, Security Management, Cryptography
GPA: 73/100 (First-Class Honours)

Athens University of Economics and Business ***Sep. 2013 - Nov. 2018***
B.Sc. in Computer Science
Thesis: Side channel attacks on network traffic on ICS/SCADA systems for privacy leakage
GPA: 7.26/10 (Very Good - 82th Percentile)

CORE SKILLS

Programming Languages: Proficient in *Java*, *C/C++*, *Python*, *Assembly X86*. Developed security-related custom frameworks, tools, and scripts.

Wireless Security: In-depth knowledge of Cellular Networks (e.g., LTE, 5G), Aviation, and WiFi 802.11. Experienced with frameworks and tools such as *Wireshark*, *Aircrack-ng*, *CoWPAtty*, *srsRAN*, *OpenAirInterface*, *Amarisoft*, and *Open5GS*. Utilized and customized frameworks and tools for wireless security experiments.

Network Security & Penetration Testing: Highly skilled in *Kali Linux*, with extensive use of tools like *Nmap*, *Burp Suite*, *Metasploit Framework*, and *Nessus*. Conducted network security evaluations in research projects and training environments (e.g., Hack The Box).

Software Exploitation: Expertise in software exploitation techniques, including reverse engineering, and memory corruption vulnerabilities (e.g., buffer overflows). Proficient with tools such as *GDB*, and *IDA Pro*, for debugging, disassembly, and exploitation scripting. Experience in developing custom exploits and payloads for complex systems and environments.

Artificial Intelligence & Machine Learning: Proficient in leveraging Machine Learning (*Keras*, *Scikit*, etc.) in Cybersecurity, for offensive and defensive purposes. Published research and completed innovative projects in this area.

Soft Skills: Strong problem-solving abilities, critical thinking, effective communication, teamwork and leadership skills, strong analytical mindset, adaptive and attention to detail.

PUBLICATIONS

[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 Security Symposium, Philadelphia PA USA, August 2024 (To Appear)

[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 (To Appear)

[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 2020, 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

PATENTS

Cellular User Localization System: SMS Side-Channel Timing Analysis Method And Apparatus
Provisional Patent Application No: 63531433
Date Filed: August 2023
Description: This provisional patent application proposes an innovative approach for an authentication-localization mechanism using SMS timing analysis.

RESEARCH FUNDINGS & GRANTS

Multi-Modal Security Testing Platform for 5G User Equipment ***2021 - 2022***
Google's Android Security and PrIvacy REsearch (ASPIRE)
Role: Co-authorship & Leading Implementation

CERTIFICATIONS

Stanford Advanced Cybersecurity Certificate, Stanford University — ***Jan. - May 2021***

Network Defense Professional (eNDP), eLearnSecurity — ***Dec. 2020***
Certificate ID: 9369766

VHL certificate of completion, Virtual Hacking Labs — ***Apr. 2020***
Certificate ID: 2085933024

SWSE, WiFi security and pentesting, Pentester Academy — ***Nov. 2019***
Certificate ID: SWSE-10327

Advanced Infrastructure Hacking, NotSoSecure, Black Hat Europe — ***Nov. 2016***

PROFESSIONAL TRAININGS

RET2 Systems: WarGames
20+ binaries for reverse engineering, and memory exploitation

Hack-the-Box: Penetration testing (Academy)
HTB Certified Penetration Testing Specialist (CPTS) Path

INE: Malware Analysis
Reverse engineering, static and dynamic analysis techniques.

Zero2Automated: Advanced Malware Analysis
Reverse engineering, evasion, exploitation, decompilation, and shellcoding techniques.

Hack-the-Box: Penetration testing (Main)
64 root-compromised, and 2 user-compromised machines

HONORS & AWARDS

NDSS 2024 Student Support Grant
An award of $\$2,000$ for selected candidates

Cyber Security Awareness Week 2023 (CSAW'23)
North America *Finalist* in the Applied Research Competition (6.2% Acceptance Rate)

GSMA Mobile Security Research Acknowledgements
Recognition for significant contribution in mobile industry: GSMA-2023-0072

AERPAW Community Workshop 2023
Selected and NSF-funded for training

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

SERVICES

Reviewer

External, ACM Conference on Computer and Communications Security (CCS) — ***2024***
IEEE Transactions on Information Forensics & Security — ***2024***
ACM Transactions on Privacy and Security — ***2023***
IEEE/ACM Transactions on Networking — ***2023***

Committees

Northeastern University PhD Admission Committee — ***2023-2024***
Northeastern University Tenure Track Hiring Committee — ***2023-2024***
USENIX Security Artifact Evaluation Program Committee — ***2023-2024***

Teaching
TA, CS 4760/6760 Wireless and Mobile Network Security, Northeastern University ***Spring 2024***
TA, CS-UH 3210 Computer Security, New York University ***Fall 2019***

Memberships
USENIX Association member

SECURITY DISCLOSURES

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: GSMA-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

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

EVENT TALKS

5G Research Directions, Verizon ***Sep. 2023***

Cellular Network Security, AERPAW Community Workshop ***May 2023***

LANGUAGE CERTIFICATIONS

C2 Certificate of Proficiency in English, University of Michigan ***Nov. 2014***

B1 Sprachdiplom (German Language), Goethe Institute ***Aug. 2012***

SOCIAL MEDIA

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