Billy Tsouvalas
Research Assistant & PhD Candidate at SUNY Stony Brook
Electrical & Computer Engineer BSc, MSc
IBM & Google Cybersecurity Professional Certifications
[Website](), [LinkedIn](), [Google Scholar]()

Stony Brook, NY
+1 (804)-980-1233
vtsouvalas@cs.stonybrook.edu

Education

Stony Brook University (SBU)	2022-Present
Computer Science PhD	
Virginia Commonwealth University (VCU)	2021-2022
Computer Science Graduate Studies	
University of Patras	2014-2020
BSc, MSc in Electrical and Computer Engineering	
Master's Thesis: Malware Classification Methodologies	

Work Experience

Research Scientist Intern — Summer 2024
Cloudflare
Bot & Fraud Research and Development

Research Assistant — 2023-Present
Stony Brook University, Stony Brook, NY
Web Security, Deception-based Defenses
Bot Management and Mitigation

System Administrator — 2023-Present
Stony Brook University, Stony Brook, Stony Brook, NY
Computer Science Dept PragSec Lab Network & Server administrator

Teaching Assistant — 2022-2023
Stony Brook University, NY
Computer Networks course

Research Assistant — 2021-2022
Virginia Commonwealth University, Richmond, VA
Network Intrusion Detection and Prevention Systems
Critical Infrastructure Cybersecurity: Energy Sector (Solar, Wind)

Publicity and Media Administrator — 2021-2022
Virginia Commonwealth University Cybersecurity Center, Richmond, VA
Publicity, Social Media Marketing, and Digital Presence

Research Intern — 2019-2020
University of Patras, Greece
Static and Dynamic Malware Analysis and Detection
Online Misinformation Propagation

Freelance Web Developer — 2018-2020
Web Design, Full-Stack Web Development
Business-oriented Web Applications
Social Media and Digital Marketing Strategy

Research

SBU PragSec Lab — 2022-Present
Web Application Security, Honeypots, Bot behavior
Active Defenses and Deception-based Security

VCU Modern Heuristics Research Group — 2021-2022
Critical Infrastructure and Network Security, Cyber-Physical Systems
Anomaly Detection for IDS (Collaboration with DoE)

University of Patras Malware Analysis Team	2019-2020

Development of Static and Dynamic Malware Detection Tools
Online Rumor Propagation and Misinformation Detection Framework

Publications

2024

Knocking on Admin's Door: Protecting Critical Web Applications with Deception
Billy Tsouvalas, *Nick Nikiforakis*
International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2024)

2023

Efficient Graph-Based Malware Detection Using Minimized Kernel and SVM
Billy Tsouvalas, *Dimitrios Serpanos*
Cyber Malware: Offensive and Defensive Systems

[PATENT] Methods and systems for surgical training
*Lauren Siff, Milos Manic, Lewis Franklin Bost, **Vasileios Tsouvalas***
Patent number: WO2023215822A2, Application number: PCT/US2023/066595

Surgical teaching of the retropubic midurethral sling: a virtual reality training system
*Lauren Siff, **Vasileios Tsouvalas**, Lewis F Bost, Milos Manic*
International Urogynecology Journal - **AWARD: Best Video Presentation at AUGS/IUGA**

2022

Location and Language Independent Fake Rumor Detection through Epidemiological and Structural Graph Analysis of Social Connections
*Dimitrios Serpanos, Georgios Xenos, **Billy Tsouvalas***
Frontiers in Artificial Intelligence

2021

Data-driven correlation of cyber and physical anomalies for holistic system health monitoring
*Daniel L Marino, Chathurika S Wickramasinghe, **Billy Tsouvalas**, Craig Rieger, Milos Manic*
IEEE Access

CyStAR: Cyber-Physical Threat Detection and Asset Monitoring
*Craig Rieger, Jacob P Lehmer, Daniel Marino Lizarazo, Chathurika S Wickramasinghe, **Billy Tsouvalas**, Milos Manic*
Idaho National Laboratory Software

2020

Malware classification methodologies.(link)
B. Tsouvalas
University of Patras, Greece MSc Thesis

Academic Service - Volunteering

Web Security Session Chair Information Security Conference 2024	2024
Publicity Chair Information Security Conference 2024	2024
USENIX WOOT Conference on Offensive Technologies 2024 Artifact Evaluation Committee	2024
ACM CCS 2024 Artifact Evaluation Committee	2024
USENIX 2024 Artifact Evaluation Committee	2024
Instructor for *Women in Science and Engineering (WSE)* Rotation Web Security and Network Intrusion Course	Spring 2024
Instructor for *Women in Science and Engineering (WSE)* Rotation Web Security and Network Intrusion Course	Fall 2023
Publicity Chair IEEE EuroS&P Workshop Active Defense & Deception Workshop	2022, 2023
Reviewer for IEEE Transactions on Industrial Informatics	2022

Awards - Grants

Distinguished Artifact Reviewer ACM CCS 2024	2024
Best Video Abstract Presentation at AUGS/IUGA 2022 Virtual Reality Training Model for Retropubic Sling Surgery American Urogynecologic Society (AUGS) and International Urogynecological Association (IUGA) 2022	2022
NSF Student Travel Grant for 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS'2020) Award Abstract # 2014439	2021

Certifications & Courses

INFOSEC Advanced Python Scripting for Cybersecurity Specialization Course duration: 1 month	Obtained: Sep. 2023
INFOSEC OWASP Top 10 Specialization Course duration: 1 month	Obtained: Sep. 2023
INFOSEC Privacy Fundamentals Specialization Course duration: 1 month	Obtained: Aug. 2023
Google Cybersecurity Professional Certificate Course duration: 6 months	Obtained: Aug. 2023
Palo Alto Networks Cybersecurity Prof. Cert. Course duration: 1 month	Obtained: June 2023
CISCO Network Automation Engineering Fundamentals Specialization Course duration: 3 months	Obtained: June 2023
(ISC)^2 Certified in Cybersecurity Specialization (CC) Course duration: 1 month	Obtained: June 2023
INFOSEC JavaScript Security Specialization Course duration: 1 month	Obtained: June 2023
EC-Council Cybersecurity Attack and Defense Fundamentals Course duration: 5 months	Obtained: June 2023
Google IT Automation w/ Python Professional Certificate Course duration: 8 months	Obtained: Oct. 2021
INFOSEC Cyber Incident Response Specialization Course duration: 4 months	Obtained: Aug. 2021
IBM Cybersecurity Analyst Professional Certificate Course duration: 8 months	Obtained: Dec. 2020
Homeland Security and Cybersecurity Specialization University of Colorado, Colorado Springs Course duration: 4 months	Obtained: Dec. 2020

Professional Skills

Network & Systems

Nginx, Apache, Mitmproxy, Openresty, Lua, Docker, Hydra, Wpscan, Honeypot Deployment, Bot Behavior Analysis

Network Security

IDS/IPS, Wireshark, Zeek, Suricata, Snort, Stratosphere IPS, Anomaly Detection, Intrusion Detection Datasets

Penetration Testing and Forensics

OWASP, Burp Suite, Metasploit, NMAP, Hashcat, Aircrack-ng, Volatility

Malware Analysis

NSA Ghidra, Hex Rays IDA Pro, Radare, gdb, Malware Reverse Engineering, Control Flow & API Call Graphs

Machine Learning and Data Mining

Binary Decision Trees, Random Forest, SVM, Neural Networks, Markov Chains, BERT

Programming and Scripting

Python, C, C++, DSP Assembly, Java, Javascript, Git, Matlab

Languages

English[1] ●●●●●

French[2] ●●●●●

Greek (Native) ●●●●●

German ●●○○○

[1]ETS TOEFL
[2]DALF C1 CERF

Soft Skills

Fast Learner   Responsible   Performance Under Pressure   Team Work

Multitasking   Stamina   Verbal Communication   Public Speaking

Misc

Military Service Obligations Fulfilled   2018-2019
Hellenic Navy