Abbas Acar

Security and Privacy Researcher

Email: abbasacar@gmail.com - Website: abbasacar.github.io - Linkedin: linkedin.com/in/abbas-acar/

SUMMARY

- Actively conducting system security research for 8+ years with a particular focus on practical and impactful perspectives.
- Impact & Recognition: Authored 20 (5 journals, 15 conference) papers, and 1 patent, over 1800 citations to date.
- Interests: IoT/Mobile/Web/System Security, Privacy-Preserving Technologies, Modern Authentication Methods
- Building Blocks: Machine Learning (ML) and Cryptography

EDUCATION

Florida International University (FIU) *Miami, FL* July 2020
PhD in Electrical and Computer Engineering
Florida International University (FIU) *Miami, FL* April 2019
MSc in Electrical and Computer Engineering,
Middle East Technical University (METU) *Ankara, Turkey* June 2015
BSc in Electrical and Electronics Engineering
Minor in Mathematics

EXPERIENCE

Postdoctoral Associate | Florida International University 2020 - Present

- Research: Research novel projects in computer science and cybersecurity such as IoT/mobile/web security/privacy, AI/ML security, and blockchain/bitcoin security.
- Mentoring: Mentorship to 9+ graduate and 20+ undergraduate students.
- Service: Serving as a program committee member and reviewer for top-tier security conferences/journals.
- Writing: Writing grant proposals and research articles.

Graduate Research Assistant | Florida International University 2015 - 2020

- Research: Worked on a wide range of cybersecurity projects such as biometric user authentication, IoT security/privacy, advanced threat intelligence, and secure data exchange methods.
- Teaching: Handled class activities such as the design of the classes, being a substitute, and grading the homework and exams for Internet of Things (IoT) and Network Security classes.

Research Internships| Northeastern University & University of Padua

- Summer research visit to the group led by Prof. Engin Kirda at Northeastern University, MA, USA. 2018
- Summer research visit to the SPRITZ group led by Prof. Mauro Conti at the University of Padua, Italy. 2017

SKILLS

- Programming Languages: Python, C/C++, Java/Kotlin for Android, Solidity (Ethereum), Rust, Verilog
- Security Tools: WireShark, Nmap, JtR, Aircrack, OpenVPN, killerbee, Scapy, HackRF One, Metasploit, Burp Suite
- Reverse-engineering: IDA Pro, OllyDbg, Netcat, Procmon, ApateDNS
- ML/DL Frameworks: Scikit-learn, PyTorch, Keras, TensorFlow, Anaconda
- Blockchain: Ethereum in Google BigQuery, web3.py, Metamask Software
- Cryptography: NTL, HELib, SEAL
- Web: Node.js, PHP, WebAssembly (Wasm), HTML, CSS, JSON
- Virtualization: Oracle VM VirtualBox, VMware, Docker
- Data Analysis and Visualization: Pandas, Numpy, SciPy, SQL, Sqlite3, Matplotlib, Plotly
- Software Engineering: MagicDraw, Draw.io, Visual paradigm, GIT

PROJECTS

Biometric User Authentication: Designed a biometric user authentication/identification system with sensor data from smartwatches while the user is typing. Also designed a privacy-preserving protocol for biometric user authentication systems.
Tools and Skills: 1) Developed an Android app in Java/Kotlin for sensor data capture and feature extraction from smartwatches. 2) Applied machine learning and distance metrics for user identification/classification using Matlab and Python. 3) Integrated cryptography libraries written in C/C++ to Android app for feature calculation through the Java Native Interface (JNI).
Role: Primary researcher from the idea creation and system engineering to prototype development as well as an active contributor in the writing of the proposal.
Impact: Awarded by the National Science Foundation (NSF); $357k (FIU) + $143k (FAU). 1 conference, 2 journals, 1 patent based on the research findings.

Mobile Device Security: Analyzed Android security updates for the timeliness and availability of security updates by OEMs.
Role: Primary researcher and contributed to the writing of the proposal.
Tools and Skills: Implemented crawler scripts to collect 360k Android security updates from OEM websites. Since it is mostly large structured and unstructured data, we used data analysis tools such as Pandas and Numpy, and visualization tools such as Matplotlib and Plotly Express modules in Python for statistical trend analysis and gathering information from the data.
Impact: Awarded as part of Google's ASPIRE Research award with a fund of $112k. 1 top-tier (NDSS) publications.

Machine Learning Security:

- Obfuscated Malicious WebAssembly Modules Detection: Proposed a threat detection system for malicious obfuscated WebAssembly samples using adversarial training that empowers the web.
  Tools and Skills: 1) Used Javascript and WebAssembly to obfuscate malicious samples. 2) Implemented a Convolutional Neural Network (CNN) for a supervised binary image classification task in TensorFlow via the Keras API.
- On-device Machine Learning for IoT Intrusion Detection: Compared on-device ML algorithms regarding energy consumption for IoT intrusion detection and anomaly detection applications.
  Tools and Skills: Implemented and ran various machine learning and TinyML algorithms on microcontroller units (MCUs), edge devices (e.g., Raspberry Pi), and cloud servers. Used the MicroMLgen module for converting Sklearn models to C++ for TinyML.
- Adversarial ML against Malware Detection Models: Designed and tested semantic-preserving adversarial samples against state-of-the-art malware detection systems.
  Tools and Skills: Implemented a Convolutional Neural Network (CNN) for malware detection and tested with adversarial samples.

IoT Security and Privacy:

- IoT-Smart Home Security and Privacy: Designed a novel multi-stage privacy attack by utilizing machine learning for detecting and identifying the types of IoT devices, their states, and ongoing user activities.
  Tools and Skills: 1) Captured network traffic using tools Wireshark, scapy, and killerbee from 20+ IoT devices. 2) Used the scikit-learn module for machine learning tasks such as device identification, user activity detection, and classification.
- IoT Cryptojacking Malware Detection: Developed models for anomaly detection in network traffic and IoT devices, which can detect both in-browser and host-based cryptojacking malware.
  Tools and Skills: 1) Wireshark for network traffic capture. 2) Scikit-learn to classify the malware samples in various attack configurations and network settings. 3) Tsfresh to calculate a large number of time series features.

Web Security:

- Ransomware over Browser: Demonstrated novel browser-based ransomware called RøB as a malicious web app/threat that encrypts the user's files from the browser and implemented three defense solutions against this new attack vector.
  Tools and Skills: 1) JavaScript and WebAssembly to implement the proof-of-concept ransomware on the browser 2) Implemented the defense based on the malicious modification identification using ML algorithm via scikit-learn module.
- (In)Security of Modern Web Applications: Investigated Unrestricted File Upload (UFU) vulnerabilities in the Node.js ecosystem.
  Tools and Skills: 1) JavaScript and Python to create malicious payloads and upload it to the test web applications. Uncovered vulnerabilities in open-source Node.js applications affecting over 2 million web applications and resulting in 19 high-severity CVEs.

Blockchain Security:

- Malicious Smart Contracts and Crypto Scams: Proposed a user activity simulation-based scam/phishing detection mechanism for phishing websites involving fraudulent activities involving cryptocurrencies such as drainers.
  Tools and Skills: 1) Implemented a tool for phishing websites allowing them to simulate the user interaction before the actual connection using Chrome developer tools such as Selenium, Puppeteer, and Metamask. 2) We used BigQuery to query the relevant smart contracts written in Solidity.

SELECTED PUBLICATIONS

- **[NDSS '24]** "50 Shades of Support: A Device-Centric Analysis of Android Security Updates". Abbas Acar, Guliz Seray Tuncay, Esteban Luques, Harun Oz, Ahmet Aris, and Selcuk Uluagac. Network and Distributed System Security Symposium, 2024.
- **[USENIX Security '23]** "RøB: Ransomware over Modern Web Browsers". Harun Oz, Ahmet Aris, Abbas Acar, Guliz Seray Tuncay, Leonardo Babun, and Selcuk Uluagac. In the 32nd USENIX Security Symposium, 2023.
- **[NDSS '22]** "A Lightweight IoT Cryptojacking Detection Mechanism in Heterogeneous Smart Home Networks". Ege Tekiner*, Abbas Acar*, and Selcuk Uluagac. (*equal contribution). Network and Distributed System Security Symposium, 2022.
- **[NDSS '22]** "The Truth Shall Set Thee Free: Enabling Practical Forensic Capabilities in Smart Environments". Leonardo Babun, Amit Kumar Sikder, Abbas Acar, and A. Selcuk Uluagac. Network and Distributed System Security Symposium, 2022.
- **[ACM CSUR '18]** "A survey on homomorphic encryption schemes: Theory and implementation". Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. ACM Computing Surveys (CSUR), 2018.