Erkam Uzun

Georgia Institute of Technology, Atlanta, GA.
euzun@gatech.edu /erkamuzun /euzun https://sites.gatech.edu/euzun

I have research and hands-on development experience in secure multi-party computation, Open ID Connect, zero-knowledge proof and post-quantum cryptography schemes for private privacy-preserving Deep Learning, private biometric authentication/surveillance, encrypted fuzzy database query systems.
Looking for full-time software engineering positions.

Education

Georgia Institute of Technology
Ph.D. in CS (3.65/4) • Thesis: *Security and Privacy in Biometrics-Based Systems.* (2015 – 2021)

TOBB University of Economics and Technology
M.Sc. in Comp. Eng. (3.79/4) • Thesis: *Analysis and Tamper Detection of Audio Evidence.* (2012 – 2014)
B.Sc. in Comp. Eng. and EEE (3.47/4) • Senior Proj.: *Fast Detection of Audio Tampering.* (2006 – 2011)

Skills

Coding: Java (10+ years), C/C++ (3+ years), Python (5+ years), Matlab (10+ years), C# (5+ years), Android (5+ years), NodeJS (2+ years), GAMS (3 years), TensorFlow (3+ years), PyTorch (2+ years).

Cryptography: Hands on experience on • Microsoft SEAL and EMP toolkits • homomorphic encryption, secure multi-party computation, zero-knowledge proof, secure secret sharing, fuzzy extractors, locality sensitive hashing, Open ID Connect, SAML SSO schemes.

Experience and Projects

Georgia Institute of Technology, US

Postdoctoral Fellow (8/2021 – · · ·) Graduate Research Assistant (8/2015 – 8/2021).

- **Privacy-Preserving Fuzzy Database Search:** Designed an encrypted fuzzy (e.g., biometrics, medical images) database query protocol upon deep learning and homomorphic encryption.
- **Privacy-Preserving Remote Biometric Authentication System:** Designed an encrypted biometric verification system upon zero-knowledge-proof protocol, by transforming DL inferences to cryptographic hashes, and a Style-GAN-based entropy measurement mechanism. • Implemented the system with Android and NodeJS-based front-ends and an OIDC compatible identity provider server.
- **Live Biometric Verification for MLaaS:** Proved vulnerability of the major MLaaS systems (e.g., Azure Cognitive Services), then designed and implemented a liveness detection protocol.
- **Automating Stock Market Manipulation** Contributed on measuring the feasibility of using a botnet to automate stock market manipulation, incorporating with U.S. SEC files and dark web marketplace.

Published PPML'21, USENIX'21, IEEE S&P'21 Magazine, AsiaCCS'21, ACSAC'20, NDSS'18 papers, and three USPTO patents. Funded by Cisco Systems, Office of Naval Research, and DARPA.

Check my website (`/euzun/projects`) for details, demo, and implementation.

VMware, US

Research Engineering Intern (Summer, 2017).

- **Mobile Device Tracking System:** Developed a large-scale ML model to fingerprint device-specific acoustic and camera sensors for mobile device tracking and de-anonymization.

Published two USPTO patents.

New York University Abu Dhabi, UAE

Visiting Researcher (Summer, 2016) Research Engineer (10/2013 – 9/2015).

- **Social Media Crawler:** Developed an image crawler that collects millions of publicly shared images from social media (e.g., Flickr) and analyzes their ExIF headers to profile non-doctored image parameters.

Experience and Projects (continued)

- **Encoded JPEG Data Discriminator:** Developed an encoded JPEG data discriminator by leveraging from the JPEG standards, ExIF tags, and Huffman coding properties.
- **Orphaned JPEG Fragment Recovery:** Designed a novel JPEG decoder to recover and assemble any arbitrarily given encoded data without the existence of decoding and assembling parameters (metadata).

Published IEEE TIFS'15, WIFS'17, and TIFS'19 papers.

Check my repo (/euzun/jpgscraper) for the tools.

TOBB University of Economics and Technology, Turkey

Graduate Research Assistant (9/2011 – 10/2013).

- **Speech Activity, Audio Compression History and Tamper Detection:** Developed a system upon SVM with acoustic features of speech signals to discriminate them against non-speech audio, then verified non-tampered speech signals by detecting transcoded audio and cut-paste-swap forgeries.
- **Lifetime Optimization of Sensor Networks:** Designed and analyzed different WSN models by using (mixed-) integer programming to optimize their lifetime considering the i) transmission power control strategies between sensor nodes, ii) attacks to the critical nodes, and iii) scalable routing scenarios.

Published in IEEE TC'13, IEEE ICCSPA'13, Speech Comm'14, Ad Hoc Networks'14 and IEEE SAS'15.

Check my repo (`/euzun/SensorNetworks`) for mathematical optimization models..

Selected Publications

Citations: 238 – **h-index:** 8. Check my Google Scholar for the full list.

- **E. Uzun**, S. Chung, V. Kolesnikov, A. Boldyreva, W. Lee, "*Fuzzy Labeled Private Set Intersection with Applications to Private Real-Time Biometric Search.*", USENIX Security Symposium, 2021.
- C. Yagemann, S. Chung, **E. Uzun**, S. Ragam, B. Saltaformaggio and W. Lee. *"Modeling Large-Scale Manipulation in Open Stock Markets."*, IEEE Security & Privacy Magazine, 2021.
- **E. Uzun**, C. Yagemann, S. Chung, V. Kolesnikov, W. Lee, "*Cryptographic Key Derivation from Biometric Inferences for Remote Authentication.*", AsiaCCS, 2021.
- C. Yagemann, S. Chung, **E. Uzun**, S. Ragam, B. Saltaformaggio and W. Lee. *"On the Feasibility of Automating Stock Market Manipulation."*, ACSAC, 2020.
- **E. Uzun** and H. T. Sencar,"*JpgScraper: An Advanced Carver for JPEG Files*", IEEE Transactions on Information Forensics and Security, 2019.
- **E. Uzun**, S. Chung, I. Essa, W. Lee, "*rtCaptcha: A Real-Time Captcha Based Liveness Detection System*", NDSS 2018
- **E. Uzun** and H. T. Sencar, "*Carving Orphaned JPEG File Fragments*", IEEE Transactions on Information Forensics and Security, 2015.
- **E. Uzun** and H. T. Sencar, "*A Preliminary Examination Technique for Audio Evidence to Distinguish Speech from Non-Speech Using Objective Speech Quality Measures*", Speech Communication, Elsevier, 2014.
- **E. Uzun**, B. Tavli, K. Bicakci, D. Incebacak, "*The Impact of Scalable Routing on Lifetime of Smart Grid Communication Networks*", Ad Hoc Networks, Elsevier, 2014.
- K. Bicakci, H. Cotuk, B. Tavli, **E. Uzun**, "*The Impact of Transmission Power Control Strategies on Lifetime of Wireless Sensor Networks*", IEEE Transactions on Computers, 2013.

Miscellaneous Experience

Honors and Awards: Demo Day People's Choice and Create-X Startup Launch Awards by IISP, 2020 (5,000$) • RSA Security Travel Award by VentureLab, 2020 (4,000$) • Cybersecurity Summit Experts Award by IISP, 2019 (1,000$) • Startup Seed Funding by Ministry of Industry and Technology of Turkey, 2012 (60,000$).

Selected Reviewer: CCS (2018 - 2020) • IEEE S&P (2018 - 2020) • USENIX Security (2016 - 2021) • NDSS (2017) • RAID (2017) • IEEE TMC (2021) • IEEE TDSC (2021) • IEEE TIFS (2018 - 2020)

Membership: Subject Matter Expert for The Homeland Defense and Security Inf. Analysis Center.

Press: TechCrunch • MIT Technology Review • governmentCIO • ScienceDaily • Security Advisor ME.