Berk Gulmezoglu

Research Assistant

Atwater Kent Lab. ECE Department, WPI, Worcester, MA 01609

bgulmezoglu@wpi.edu

5086853882

WORK EXPERIENCE

Research Assistant Worcester Polytechnic Institute

08/2014 – Present

Achievements/Tasks

- Hardware Security on the Cloud
- Cryptographic Implementation Security
- Machine Learning and Artificial Intelligence

Visitor Researcher, Fraunhofer AISEC Munich/Germany

10/2017 – 12/2017

Achievements/Tasks

- worked on mobile phone hardware security and web security
- showed through my research that the privacy in mobile phones can be violated by other applications
- developed an application, which can detect whether a person has visited a whistleblowing website. This detection technique even works in dark web, where the identity of the person is not revealed to other people.
- presented a paper on this in ESORICS 2017
- wrote a book chapter on side-channel attacks in IoT devices to address possible future flaws in the IoT hardware

Summer Intern, VMware Inc. Palo Alto, CA

05/2017 – 08/2017

Achievements/Tasks

- worked on Translation Lookaside Buffer side-channel attacks in VMware products
- reported two security flaws in their public cloud system to VMware security team, which could be exploited by attackers in the future
- presented my studies in a poster session to VMware employees

Teaching Assistant Worcester Polytechnic Institute

01/2015 – 01/2017

Achievements/Tasks

- Introduction to Cryptology
- Computer & Network Security
- Machine Learning in Cybersecurity

SKILLS

C/C++ | C# | Java | Python | Matlab | OpenGL | Git | GNU GCC | Microsoft Visual Studio

EDUCATION

Worcester Polytechnic Institute, Ph.D. Candidate in ECE (08/2014 – Present)

- working on cache side-channel attacks on the public clouds
- working on Artificial Intelligence algorithms to increase the efficiency of micro-architectural attacks
- focus on RNN based countermeasures against up-to-date side-channel attacks on servers and mobile phones

Bilkent University, Turkey M.S. in Electrical and Electronics Engineering (09/2012 – 08/2014)

Bilkent University, Turkey B.S. in Electrical and Electronics Engineering (09/2007 – 06/2012)

AWARDS

2nd Best Poster Award in Data Science, Cybersecurity and Computer Science (04/2018)

Research Assistantship from WPI ECE Department for Ph.D. (08/2014 – Present)

Global Research Fellowship from WPI (2017)

Full Scholarship from TUBITAK research center for Master of Science (2012 – 2014)

Full Merit Scholarship from Ihsan Dogramaci Bilkent University (2007 – 2012)

LANGUAGES

English | Turkish

WORK EXPERIENCE

Research Assistant
Bilkent University
08/2012 – 08/2014

Achievements/Tasks
- worked on “Indoor Multi-person Tracking via Ultra-wideband Radars”
- developed an algorithm, which can track the movements of many people in an environment
- results were presented in IEEE Sensors journal in 2015

Summer Intern, Savronik Electronic Industry and Commerce Inc.
Eskisehir/Turkey
07/2011 – 08/2011

Achievements/Tasks
- worked on “Image Processing for Handwriting Recognition”
- developed a tool to detect the handwriting characters, which helped handwritten documents to be converted to a word file easily
- presented my results at the end of the internship

Summer Intern, ASELSAN Communication and Information Technologies Inc.
Ankara/Turkey
07/2010 – 08/2010

Achievements/Tasks
- did research on “Friend and Foe Target Detection by Satellites”
- literature research on how other countries establish the difference between friend and foe targets
- presented my results at the end of the internship

BOOK CHAPTERS

Side-Channel Attacks in the Internet of Things: Threats and Challenges (2018)
- Zankl, A., Seuschek, H., Irazoqui, G. & Gulmezoglu B.
- Solutions for Cyber-Physical Systems Ubiquity, 325-357

PUBLICATIONS

FortuneTeller: Predicting Microarchitectural Attacks via Unsupervised Deep Learning
Gulmezoglu, B., Moghimi, A., Eisenbarth, T., & Sunar, B. arXiv preprint arXiv:1907.03651 (2019)

SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks
Islam, S., Moghimi, A., Bruhns, I., Krebbel, M., Gulmezoglu, B., Eisenbarth, T., & Sunar, B. USENIX 2019, Santa Clara, CA

Undermining User Privacy on Mobile Devices Using AI
Gulmezoglu, B., Zankl A., Tol, M. C., Islam, S., Eisenbarth, T., & Sunar, B. ASIACCS 2019, Auckland, New Zealand

PerfWeb: How to Violate Web Privacy with Hardware Performance Events
Gulmezoglu, B., Zankl A., Eisenbarth, T., & Sunar, B. ESORICS 2017, Norway, Oslo

Cache-based Application Detection in the Cloud Using Machine Learning
Gulmezoglu, B., Eisenbarth, T., & Sunar, B. ASIACCS 2017, Abu-Dhabi, UAE

Cache Attacks Enable Bulk Key Recovery on the Cloud
Inci, M. S., Gulmezoglu, B., Irazoqui, G., Eisenbarth, T., & Sunar, B CHES 2016, Santa Barbara, CA

Co-location detection on the Cloud
Inci, M. S., Gulmezoglu, B., Eisenbarth, T., & Sunar, B. COSADE 2016, Graz, Austria

A Faster and More Realistic Flush + Reload Attack on AES
Gülmezoglu, B., Inci, M. S., Irazoqui, G., Eisenbarth, T., & Sunar, B. COSADE 2015, Berlin, Germany

Seriously, get off mycloud! Cross-VM RSA Key Recovery in a Public Cloud
Inci, M. S., Gulmezoglu, B., Irazoqui, G., Eisenbarth, T., & Sunar, B. (2015) IACR Cryptology ePrint Archive http://eprint.iacr.org/2015/898.pdf

JOURNALS

Cross-VM Cache Attacks on AES (2015)
Gulmezoglu, B., Inci, M. S., Irazoqui, G., Eisenbarth, T., & Sunar, B. IEEE on Multi-Scale Computing Systems, PP(99), 2332-2345

Multi-person Tracking With a Network of Ultra-wideband Radar Sensors Based on Gaussian Mixture PHD Filters (2015)

Gulmezoglu, B., M.B., & Gezici, S. IEEE Sensors