BERK GULMEZOGLU

Assistant Professor of Electrical and Computer Engineering, Iowa State University
613 Morill Rd. Ames, IA, 50011, USA bgulmez@iastate.edu (515) 294-1404

Updated: Jul 11, 2023

EDUCATION

2014 - 2020	**Worcester Polytechnic Institute**, Ph.D. in Electrical and Computer Engineering
2012 - 2014	**Bilkent University**, M.S. in Electrical and Electronics Engineering
2007 - 2012	**Bilkent University**, B.S. in Electrical and Electronics Engineering

ACADEMIC AND RESEARCH APPOINTMENTS

Iowa State University, Electrical and Computer Engineering	Ames, IA, USA
Assistant Professor	Aug 2020–present
Worcester Polytechnic Institute, Vernam Lab.	Worcester, MA, USA
Graduate Research Assistant	Aug 2014–Jul 2020
Bilkent University, Wireless Communications Lab	Ankara, TURKEY
Graduate Research Assistant	Jan 2010–Aug 2011

INDUSTRIAL EXPERIENCE

Fraunhofer AISEC, Hardware Security Team	Munich, GERMANY
Visitor Researcher, Mentored by Andreas Zankl	Oct 2017–Dec 2017
VMware Inc., Cloud Security Team	Palo Alto, CA, USA
Research Intern, Mentored by Fred Jacobs	May 2017–Aug 2017
Aselsan Inc., National Defense Team	Ankara, TURKEY
Research Intern, Mentored by Dilek Afyonluoglu	May 2010–Aug 2010

AWARDS AND HONORS

Internal to ISU

- Exploratory Research Projects: Automated Hardware Hardening Against Transient Execution Attacks, Spring 2023, Reward Amount: **$25,000**
- ECpE FutURE: Funding the Undergraduate Research Experience, Fall 2021, Reward Amount: **$4,000**

External to ISU

- 2nd Best Poster Award in Data Science, Cybersecurity and Computer Science, 2018
- Research Assistantship, WPI ECE Department, 2014 – 2020
- Global Research Fellowship, WPI, 2017
- Full Scholarship, TUBITAK Research Center, 2012 – 2014

REFEREED PUBLICATIONS

Book Chapters

[B1]. Andreas Zankl, Hermann Seuschek, Gorka Irazoqui, and Berk Gulmezoglu, **Side-channel Attacks in the Internet of Things: Threats and Challenges**, Research Anthology on Artificial Intelligence Applications in Security, 2021

Journal Articles

[J4]. Debopriya Roy Dipta, Berk Gulmezoglu, *MAD-EN: Microarchitectural Attack Detection through System-wide Energy Consumption*, IEEE Transactions on Information Forensics and Security (IEEE TIFS), 2023 (IF=7.2)

[J3]. Berk Gulmezoglu, *XAI-based Microarchitectural Side-channel Analysis for Website Fingerprinting Attacks and Defenses*, IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 2021 (IF=6.8)

[J2]. Berk Gulmezoglu, M. Sinan Inci, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, *Cross-VM Cache Attacks on AES*, IEEE Transactions on Multi-Scale Computing Systems, 2015 (IF=2.06)

[J1]. Berk Gulmezoglu, M. Burak Guldogan, Sinan Gezici, *Multi-person Tracking with a Network of Ultra-Wideband Radar Sensors based on Gaussian Mixture PHD Filters*, IEEE Sensors, 2015 (IF=4.3)

Peer-reviewed Conference Publications

[C10]. Claudius Pott, Berk Gulmezoglu and Thomas Eisenbarth, ***Overcoming the Pitfalls of HPC-based Cryptojacking Detection in Presence of GPUs*** ACM Conference on Data and Application Security and Privacy, 2023 (AR: 18%)

[C9]. Debopriya R. Dipta and Berk Gulmezoglu, ***DF-SCA: Dynamic Frequency Side Channel Attacks are Practical,*** Annual Computer and Security Conference (ACSAC), 2022 (AR: 21%)

[C8]. M. Caner Tol, Koray Yurtseven, Berk Gulmezoglu, and Berk Sunar, ***FastSpec: Scalable Generation and Detection of Spectre Gadgets Using Neural Embeddings,*** IEEE European Symposium on Security and Privacy (Euro S&P), 2021 (AR: 25%)

[C7]. Saad Islam, Ahmad Moghimi, Ida Bruhns, Mortiz Krebbel, Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar, ***SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks***, USENIX, 2019 (AR: 15.5%)

[C6]. Berk Gulmezoglu, Andreas Zankl, M. Caner Tol, Saad Islam, Thomas Eisenbarth, and Berk Sunar, ***Undermining User Privacy on Mobile Devices Using AI***, ASIACCS, 2019 (AR: 17%)

[C5]. Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth, and Berk Sunar, ***PerfWeb: How to Violate Web Privacy with Hardware Performance Events***, ESORICS, 2017 (AR: 16%)

[C4]. Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar, ***Cache-based Application Detection in the Cloud Using Machine Learning***, ASIACCS, 2017 (AR: 18.7%)

[C3]. M. Sinan Inci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, ***Cache Attacks Enable Bulk Key Recovery on the Cloud,*** CHES, 2016 (AR: 20.3%)

[C2]. M. Sinan Inci, Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar, ***Co-location Detection on the Cloud***, COSADE, 2016 (AR: 30.3%)

[C1]. Berk Gulmezoglu, M. Sinan Inci, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, ***A Faster and More Realistic Flush+Reload Attack on AES,*** COSADE, 2015 (AR: 34.2%)

Arxiv/Preprint Publications

[A2]. Berk Gulmezoglu, Ahmad Moghimi, Thomas Eisenbarth, and Berk Sunar, ***Fortuneteller: Predicting Microarchitectural Attacks via Unsupervised Deep Learning***, Preprint arXiv:1907.03651, 2019

[A1]. M. Sinan Inci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, ***Seriously, Get off My Cloud! Cross-VM RSA Key Recovery in a Public Cloud***, IACR Cryptology ePrint Archive, 2015

Thesis

[T2]. Berk Gulmezoglu, ***Towards Automated Analysis of Microarchitectural Attacks using Machine Learning***, PhD Thesis, Worcester Polytechnic Institute, July 2020

[T1]. Berk Gulmezoglu, ***Indoor Multi-person Tracking via Ultra-wideband Radars***, Master Thesis, Bilkent University, August 2014

PROFESSIONAL LEADERSHIP AND SERVICE

Editorial Board

- 2021-2022, MDPI Information Special Issue on “Side-channel Attacks and Defenses on Cryptography”

Program Committee

- 2023, CCS, Euro S&P
- 2022-2023, ESORICS
- 2021-2022, CRISIS

Journal and External Reviewer

- 2021, Samsung Ho-Am Prize
- 2021-2022, IEEE Transactions on Information Forensics and Security
- 2021, MDPI Cryptography
- 2021, MDPI Information

STUDENT ADVISING

Current PhD Students

Debopriya Roy Dipta	Fall 2021
Seonghun Son	Summer 2022

Current MS Students

Nayra Lujano	Spring 2022
Evan Helman	Spring 2023

Current BS Students

Anuraag Pujari	Fall 2021

TEACHING EXPERIENCE

Iowa State University

- Spring 2022, 2023: CPRE 538: Reverse Engineering and Security Testing
- Fall 2021, 2022: CPRE 381: Computer Organization and Assembly Level Programming
- Spring 2021: CPRE 681: Advanced Computer Architecture

Guest lecturer

- CPRE 581: Computer Systems Architecture (Fall 2020, Fall 2021, Fall 2022)
- CPRE 482X: Hardware Design for Machine Learning (Fall 2020)

Worcester Polytechnic Institute (During Ph.D.)

Guest lecturer

- ECE 4801: Computer Architecture (Spring 2020)
- ECE 579M ST: Machine Learning in Cybersecurity (Spring 2019)

ENGAGEMENT AND SERVICE

- Served as a volunteer judge at Science Bound “Nothing Less Than Success” Science Fairs! (2022)