Daniel Moghimi

Computer Security and Privacy, Ph.D

1775 Diamond Street - Unit 1-210, San Diego, CA, USA, 92109

+1 (774) 810 6466 danielm@ucsd.edu moghimi.org danielmgmi danielmgmi

Research Interests

System Security, Hardware Security, Applied Cryptography, Side Channels, Microarchitectural Attacks, Trusted Computing, Machine Learning and Security, , Vulnerability Fuzzing, Binary Analysis, Reverse Engineering

Research/Work Experience

Postdoctoral Fellow **Jan. 2021 - Current**
UCSD, San Diego, CA
`Mentors: Dr. Nadia Heninger and Dr. Deian Stefan`
- Research on hardware-software co-design for enforcing speculative memory safety and secure/trusted isolation.

Interim Engineering Intern **Sep. 2020 - Dec. 2020**
Qualcomm - Product Security, (Remote) Holden, MA
`Manager: Dr. Can Acar, Mentor: Dr. David Hartley`
- Security evaluation of PCIe susbystem within the system on a chips (SoC).
- Prototyping a trusted encryption protocol using TPM.

Research Assistant **Sep. 2016 - Sep. 2020**
Worcester Polytechnic Institute, Worcester, MA
`Advisors: Dr. Berk Sunar and Dr. Thomas Eisenbarth`
- Research on microarchitectural security, side channels, trusted execution environment (TEE), side-channel cryptanalysis.
- Coordinated disclosure of critical hardware/firmware vulnerabilities.
- Research was funded by the National Science Foundation grant CNS-1618837 and CNS-1814406, Intel Side-Channel Academic Program (SCAP), and Cloudflare $\$30,000$ research gift.

Graduate Student Visitor **Nov. 2019 - Dec. 2019**
University of California, San Diego, CA
`Host: Dr. Nadia Heninger`
- Study of lattice-based attacks and algorithmic techniques for side-Channel cryptanalysis.

College Intern PhD Cross Functional – Application Security **Jun. 2016 - Aug. 2016**
Cisco Talos, Austin, TX
`Supervisors: Richard Johnson, Dr. Yves Younan`
- Customizing the AFL fuzzing tool to work with Intel Processor Trace for binary instrumentation and tracing.
- Developing the FuzzFlow vulnerability discovery framework.

Senior Web Developer – Full Stack Developer **Nov. 2014 - Jul. 2015**
Ganj Afzar, Tehran, IR
- RESTful API services in NODE.JS and 3rd party API Integration (Payment, Ticketing, Logging, Amazon AWS).
- Front-end development in bootstrap and angular.js.

Computer Security and Software Development **Jun. 2010 - May 2014**
'Freelance, Self-employed', Tehran, IR
- Binary analysis, Reverse engineering, win32 programming, Application security.

Education

Ph.D in Electrical & Computer Engineering **May 2017 - Dec. 2020**
Worcester Polytechnic Institute, Worcester, MA
Doctoral Dissertation: "Revisiting Isolated and Trusted Execution via Microarchitectural Cryptanalysis"

M.S in Computer Science **Jan. 2016 - May 2017**
Worcester Polytechnic Institute, Worcester, MA
Master Thesis: "Side-Channel Attacks on Intel SGX: How SGX Amplifies the Power of Cache Attacks"

B.Eng. in Computer Engineering **Sep. 2008 - Jul. 2012**
IAU, Tehran, Iran
Final Project: "Survey on Reverse Engineering OOP Binaries"

Teaching Experience

Teaching Assistant **Jan. 2016 - May. 2017**
Worcester Polytechnic Institute, Worcester, MA (3 Semesters)
Advanced Computer Networks (CS 4516), Techniques of Programming Language Translation (CS 4533), Webware (CS 4241), Operating System (CS 3013), Machine Organization and Assembly Language (CS 2011), Software Security Engineering (CS 4401).

Teaching Assistant **Sep. 2015 - Dec 2015**
Wayne State University, Detroit, MI (1 Semester)
Computer Science I (CSC 2110)

Publications

A. Refereed

Swivel: Hardening WebAssembly against Spectre **2021**
S Narayan, C Disselkoen, D Moghimi, S Cauligi, E Johnson, Zhao Gang, A Vahldiek-Oberwagner, R Sahita, H Shacham, D Tullsen, Deian Stefan
The 29th Usenix Security (SEC 2021).

CopyCat: Controlled Instruction-Level Attacks on Enclaves **2020**
D Moghimi, J Van Bulck, N Heninger, F Piessens, B Sunar
The 29th Usenix Security (SEC 2020).

Medusa: Microarchitectural Data Leakage via Automated Attack Synthesis **2020**
D Moghimi, M Lipp, B Sunar, M Schwarz
The 29th Usenix Security (SEC 2020).

TPM-Fail: TPM meets Timing and Lattice Attacks **2020**
D Moghimi, B Sunar, T Eisenbarth, N Heninger
The 29th Usenix Security (SEC 2020).

LVI: Hijacking Transient Execution through Microarchitectural Fault Injection **2020**
J. Van Bulck, D. Moghimi, M. Schwarz, M. Lipp, M. Minkin, D. Genkin, Y. Yarom, S. Berk, D. Gruss, F. Piessens
The 41st IEEE Symposium on Security and Privacy (S&P 2020).

JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms **2020**
Z Weissman, T Tiemann, D Moghimi, E Custodio, T Eisenbarth and Berk Sunar
Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2020).

Fallout: Reading Kernel Writes From User Space **2019**
M Minkin, D Moghimi, M Lipp, M Schwarz, J Van Bulck, D Genkin, D Gruss, F Piessens, B Sunar, Y Yarom
merged with Store-to-Leak (arXiv:1905.05725), under Canella et al. "Fallout: Leaking Data on Meltdown-resistant CPUs"
The 26th ACM Conference on Computer and Communications Security (CCS 2019 - AR %15.7).

ZombieLoad: Cross-Privilege-Boundary Data Sampling **2019**
M Schwarz, M Lipp, D Moghimi, J Van Bulck, J Stecklina, T Prescher, D Gruss
The 26th ACM Conference on Computer and Communications Security (CCS 2019 - AR %15.7).

Spoiler: Speculative Load Hazards Boost Rowhammer and Cache Attacks **2019**
S Islam, A Moghimi, I Bruhns, M Krebbel, B Gulmezoglu, T Eisenbarth, B Sunar
The 28th Usenix Security (SEC 2019 - AR %15.27).

MemJam: A False Dependency Attack against Constant-Time Crypto Implementations **2019**
A Moghimi, J Wichelmann, T Eisenbarth, B Sunar
International Journal of Parallel Programming (IJPP 2019).

MicroWalk: A Framework for Finding Side Channels in Binaries **2018**
J Wichelmann, A Moghimi, T Eisenbarth, B Sunar
Annual Computer Security Applications Conference (ACSAC 2018 - AR %20.00).

CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks **2018**
F Dall, G De Micheli, T Eisenbarth, D Genkin, N Heninger, A Moghimi, Y Yarom
Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2018 - %28.65)).

MemJam: A False Dependency Attack against Constant-Time Crypto Implementations in SGX **2018**
A Moghimi, T Eisenbarth, B Sunar
The Cryptographers' Track at the RSA Conference (CT-RSA 2018 - AR %32.91).

CacheZoom: How SGX Amplifies The Power of Cache Attacks **2017**
A Moghimi, G Irazoqui, T Eisenbarth
Cryptographic Hardware and Embedded Systems (CHES 2017 - AR %25.38).

B. Preprints

SoK: Practical Foundations for Spectre Defenses **2019**
S Cauligi, C Disselkoen, D Moghimi, G Barthe, D Stefan
under submission, arXiv preprint is available (arXiv:2105.05801).

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

C. Posters/Short Papers

SCREAM: Sensory Channel Remote Execution Attack Methods (Poster) **2016**
N Brown, N Patel, P Plenefisch, A Moghimi, T Eisenbarth, C Shue, and K Venkatasubramanian
Usenix Poster Session (Usenix 2016).

Abstract Runtime Structure for Reasoning about Security (Usenix Paper) **2016**
M Abi-Antoun, E Khalaj, RaduVanciu, and A Moghimi
The Symposium and Bootcamp on the Science of Security (HotSoS 2016).

Talks

JackHammer: Rowhammer and Cache Attacks on Heterogeneous FPGA-CPU Platforms **Oct. 2020**
Conference talk at hardwear.io Netherlands 2020

CopyCat: Controlled Instruction-Level Attacks on Enclaves **Sep. 2020**
Invited talk at Intel Labs

TPM-Fail: TPM meets Timing and Lattice Attacks **Aug. 2020**
Invited talk at Workshop on attack in Cryptography 2020.

TPM-Fail: TPM meets Timing and Lattice Attacks **Aug. 2020**
Conference talk at Usenix Security 2020.

Medusa: Microarchitectural Data Leakage via Automated Attack Synthesis **Aug. 2020**
Conference talk at Usenix Security 2020.

CopyCat: Controlled Instruction-Level Attacks on Enclaves **Aug. 2020**
Conference talk at Usenix Security 2020.

Remote Timing Attacks on TPMs, AKA TPM-Fail **Aug. 2020**
Conference talk at Black Hat USA 2020.

Breaking Deployed Crypto: The Side Channel Analyst's Ways **April. 2020**
Conference talk at Hardwear.io Virtual Con 2020.

LVI: Hijacking Transient Execution with Load Value Injection **April. 2020**
Conference talk at Hardwear.io Virtual Con 2020.

Exploiting Microarchitectural Flaws in the Heart of the Memory Subsystem **Feb. 2020**
Invited talk at Columbia University, New York City, NY.

TPM-Fail: TPM meets Timing and Lattice Attacks **Jan. 2020**
Conference talk at Real World Crypto 2020, New York City, NY.

ZombieLoad: Leaking Data on Intel CPUs **Nov. 2019**
Conference talk at ToorCon 21 (2019), San Diego, CA.

SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks **Aug. 2019**
Conference talk at Usenix Security 2019, Santa Clara, CA.

Microarchitectural Attacks and Cloud Accelerators **Jun. 2019**
Guest talk at Intel SCAP Conference 2019, Intel, Hillsboro, OR.

Microarchitectural Attacks: Protecting Cloud Accelerators **Mar. 2019**
Guest talk at Intel SCAP Meeting 2019, University of Florida, Gainesville, FL.

MemJam: A False Dependency Attack against Constant-Time Crypto Implementations **Apr. 2018**
Conference talk at RSA Conference 2018 (CT-RSA 2018), San Francisco, CA.

Side-channel Attacks on SGX Enclaves **Sep. 2017**
Conference talk at New England Security Day (NESD 2017), Northeastern, Boston, MA.

Professional Skills

Programming: *C, C++, x86/x64 Assembly, Python, PHP, Lua, JavaScript, Java, C#, Perl, R, Matlab, SQL/NoSQL*

Tools/Platforms: *Pintools, IDA Pro, WinDebug, GDB, Immunity Debugger, Wireshark, LateX, Linux Kernel, Windows WDK/SDK, SageMath, SGX SDK*

Honors/Awards

Pwnie Awards *Nominee for Best Cryptographic Attack* **Dec. 2020**
for "TPM-Fail: TPM meets Timing and Lattice Attacks"

CSAW Applied Security Research Competition (Europe) *Top 10 Finalists* **Nov. 2020**
for "LVI: Hijacking Transient Execution through Microarchitectural Fault Injection"

CSAW Applied Security Research Competition (US-Canada) *Top 10 Finalists* **Nov. 2020**
for "TPM-Fail: TPM meets Timing and Lattice Attacks" development

Postdoctoral Fellowship *UCSD Computer Science and Engineering Fellowship* **Aug. 2020**
60,000-65,000$ per year fellowship

Student Conference Travel Awards *TCHES 2019, Real World Crypto 2019 and 2020, NDSS 2020*

Professional Service

Program Committee: Usenix Security 2022, IACR CHES 2022, SPACE 2021, ASHES 2020

Shadow Program Committee: IEEE S&P 2019 and 2017

Journal/External Reviews: ACM CSUR 2021, ACM CCS 2021, IEEE TDSC 2020, ACM DTRAP 2020, IEEE TIFS 2020, ACM JETC 2020, IACR Eurocrypt 2020, IJIS 2019, DATE 2019, IACR Kangacrypt 2018, IEEE TIFS 2018, IACR TCHES 2018, IACR Asiacrypt 2017, IFIP/IEEE VLSI-SoC 2017

Open-source Projects

VirusBattle IDA Plugin
Integration of Virus Battle API to the IDA Pro disassembler
In collaboration with `Dr. Arun Lakhotia`, *University of Louisiana*
https://github.com/danielmgmi/virusbattle-ida-plugin.

***lodash* library for Lua**
Functional programming library for Lua inspired by the lodash.js
https://github.com/danielmgmi/lodash.lua.