Daniel Moghimi

Computer Security Researcher, Ph.D Candidate

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

Research Interests

System Security, Hardware Security, Applied Cryptography, Trusted Computing, Machine Learning and Security

Recent Experience

Postdoctoral Fellow **Jan. 2021 - Current**
UCSD, San Diego, CA
Mentors: Dr. Nadia Heninger and Dr. Deian Stefan

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 **May. 2017 - 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.

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.

Education

Ph.D in Electrical & Computer Engineering **May 2017 - Dec. 2020**
Worcester Polytechnic Institute, Worcester, MA

M.S in Computer Science **Jan. 2016 - May 2017**
Worcester Polytechnic Institute, Worcester, MA

B.Eng. in Computer Engineering **Sep. 2008 - Jul. 2012**
IAU, Tehran, Iran

Selected Publications

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).

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).

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).

Selected Talks

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

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

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.

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"

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

Professional Service

Program Committee: Workshop on Attacks and Solutions in Hardware Security (ASHES 2020)

Shadow Program Committee: IEEE S&P 2017 and 2019

Individual Reviews: IFIP/IEEE VLSI-SoC 2017, IACR Asiacrypt 2017, IACR TCHES 2018, IEEE TIFS 2018, IACR Kangacrypt 2018, DATE 2019, IJIS 2019, IACR Eurocrypt 2020, ACM JETC 2020, IEEE TIFS 2020 (2 reviews), ACM DTRAP 2020, IEEE TDSC 2020