MICHAEL DORAN

Atlanta, GA | 231.571.8689 | doranm09@gmail.com | U.S. Citizen | Active TS/SCI | CI Polygraph

PROFESSIONAL SUMMARY

Senior Embedded Systems Engineer, cybersecurity researcher, and U.S. Army Reserve Cyber Warfare Officer with 13+ years of experience in defense R&D and high-assurance embedded systems. Technical lead and Principal Investigator for Department of War programs spanning seL4 virtualization, ARM/RISC-V platforms, AMD Versal/Zynq, secure boot, hardware roots of trust, cyber-physical security, and autonomous systems. Georgia Tech Ph.D. researcher with peer-reviewed publications and operational technology cybersecurity intellectual property.

CORE QUALIFICATIONS

High assurance: seL4, secure virtualization, zero trust, secure boot, hardware roots of trust, remote attestation

Platforms: ARM, RISC-V, x86, AMD Versal/Zynq, FPGA/SoC, embedded Linux, BSP and device-driver development

Cyber / R&D: cyber-physical security, malware reverse engineering, digital forensics, SBIR, C/C++, Python, Rust, MATLAB, React, Electron, Vivado, Vitis

RELEVANT EXPERIENCE

DornerWorks | Grand Rapids, MI

Senior Embedded Systems Engineer | Aug 2017-Present | 40 hrs/week

- Lead technical execution across an approximately $10M defense R&D portfolio, directing multidisciplinary teams of 8-12 engineers across embedded software, FPGA/SoC, secure virtualization, networking, and cybersecurity.
- Develop high-assurance computing platforms based on the formally verified seL4 microkernel, including virtual machine monitor infrastructure, board support packages, device drivers, and hardware abstraction for ARM, RISC-V, AMD Zynq UltraScale+, and AMD Versal systems.
- Support Cyber-Hardened Satellite Software (CHSS) and Magnetite transition efforts by porting secure virtualization to AMD Versal and developing VM Composer, an Electron-based tool for rapid configuration of embedded virtualization architectures.
- Serve as Principal Investigator and technical/program lead for Department of War SBIR efforts, translating government objectives into architectures, experiments, demonstrations, schedules, success criteria, and engineering deliverables.
- Design cyber-resilient and zero trust architectures using least privilege, capability-based access control, workload isolation, secure boot, attestation, hardware roots of trust, and protected device interfaces.
- Support space, autonomous, and ground vehicle programs and integrate heterogeneous AI workloads, including YOLOv8 deployment to AMD neural processing hardware; perform integration, verification, requirements traceability, technical writing, and customer briefings.

U.S. Army Reserve | Augusta, GA / Atlanta, GA

Cyber Warfare Officer, Captain | Jun 2020-Present | Reserve service; hours vary by duty status

- Lead defensive cyberspace operations, technical teams, mission planning, readiness, and operational execution for Department of War networks and systems; translate commander intent into executable technical and operational activities.
- Led a 39-member team of cybersecurity specialists and partner organizations supporting collective defense and visibility into network and host metrics using approved cyber defense capabilities.
- Progressed through team lead, mission element lead, and operations officer responsibilities; earned four consecutive top-block Officer Evaluation Reports and was selected for HHC company command beginning June 2027.
- Awards include the Army Commendation Medal (ARCOM) and Army Reserve Components Achievement Medal (ARCAM).

Twisthink | Holland, MI
Embedded Software Engineer | May 2013-Aug 2017 | 40 hrs/week

- Led embedded development for a nationwide industrial IoT control system managing more than 10,000 end nodes using Microchip platforms and Zigbee; developed device software, gateways, backend/frontend components, and system integration capabilities.
- Ported the wolfSSL encryption stack to enable TLS 1.2 communications and developed symmetric encryption mechanisms protecting node-to-gateway traffic; contributed .NET, Java, and JavaScript software across the connected product stack.

RESEARCH EXPERIENCE

Georgia Institute of Technology - iFAN Laboratory | Atlanta, GA
Doctoral Researcher | Ph.D. in progress; expected May 2028

- Research cybersecurity of cyber-physical and operational technology systems, including probabilistic risk assessment, dynamic Bayesian networks, network digital twins, vulnerability management, and resource-constrained cyber defense decision support.
- Develop experimental environments integrating network emulation, containerized cyber defense services, operational technology components, and tools including Zeek, Suricata, OpenVAS, Wazuh, MISP, OpenCTI, Trivy, and Grype; contributed ARM and RISC-V firmware orchestration support for Sandia National Laboratories minimega.
- Conducted proof-of-concept research on cybersecurity of radiation detection devices and secure data workflows, including secure boot, XML digital signatures, and encryption; work resulted in peer-reviewed Nuclear Technology publications.

CERTIFICATIONS

- GIAC Reverse Engineering Malware (GREM)
- GIAC Certified Forensic Analyst (GCFA)

EDUCATION

Georgia Institute of Technology, Atlanta, GA - Ph.D., Electrical & Computer Engineering, expected May 2028
Grand Valley State University, Allendale, MI - M.S., Computer Engineering, May 2023; Outstanding Thesis Award
Grand Valley State University, Allendale, MI - B.S., Computer Engineering, May 2017; Minor in Mathematics

SELECTED PUBLICATIONS & INTELLECTUAL PROPERTY

- Doran, Zebrowitz, and Zhang. “Development of a Vulnerability Management Tool for Advanced Reactors.” Nuclear Technology, 2026.
- Doran, Mukhopadhyay, and Zhang. “Cybersecurity of Radiation Detection Devices: A Proof-of-Concept Attack.” Nuclear Technology, 2026.
- Doran and Kandalaft. “Embedded Virtualization on RISC-V with seL4.” IEEE UEMCON, 2023, pp. 736-740.
- Doran, Russell, and Elliott. “Deterministic & Modular Architecture for Embedded Vehicle Systems.” GVSETS, 2023.
- Co-Inventor, U.S. Provisional Patent Application 64/008,551, “Cyber Physical Risk Assessment and Management Tool for OT System,” filed Mar. 17, 2026.

TEACHING & PROFESSIONAL LEADERSHIP

Cornerstone University | Adjunct Professor | Jan 2021-May 2023

- Developed and taught lecture and laboratory curriculum in ARM Cortex-M embedded systems for classes averaging 15 students; instructed C/C++, GPIO, serial/Bluetooth communications, RTOS concepts, PWM, ADC/DAC, digital design, and circuit analysis.

IEEE MILCOM 2026 | Panel Moderator

- Selected to moderate “High Assurance Hardware and Software Co-Design for Resilient System Security,” guiding discussion on assurance evidence, system boundaries, hardware/software interfaces, and resilient defense communications.