Matthew Weeks

(262) 672-0834 matthew.t.weeks@gmail.com San Antonio, Texas

An experienced cyber security expert with deep technical, leadership, and communication skills and an extensive and recognized record of accomplishment in the areas of reverse engineering, vulnerability discovery and exploitation, cyber security software development, cryptology, and cyber blue and red operations and leading successful security research and engineering teams.

Skills include developing in and reverse engineering C++, Rust, Java, C, C#, Python, x86 and x64 assembly, Ruby, JavaScript, and PHP; intrusion response; exploit development; speaking and writing skills; mentoring, team building, and team leadership

Department of Defense Top Secret/Sensitive Compartmented Information (TS/SCI) clearance (SSBI/SBPR).

Employment History

05/22-present **Aurora** Remote, San Antonio, TX

Staff Security Engineer

- Led security assessment program to threat model, identify components, determine attack surface, and identify vulnerabilities and architectural risks
- Coordinated with engineering organizations to identify novel, effective, and achievable risk mitigation strategies to prevent classes of attacks and fix code vulnerabilities
- Technologies and protocols assessed include CAN, CAN-FD, secure boot, C/C++ code in ARM and x86-64, Go code, power distribution, UART, JTAG, chip and board schematics, NTP, TLS, HSM's, TPM's, control systems for steering, braking, engine, transmission, and lighting, and CI/CD involving Github, Buildkite, AWS, and more
- Evaluation of security initiatives against safety case and standards such as ISO 21434

01/21-05/22 **Deloitte** Remote, San Antonio, TX

Technology Fellow

- One of the most senior, preeminent staff-level technology leaders sought after to pioneer the most challenging solutions and architectures
- Cyber Detect & Response Research and Development lead
- Led several Industrial Control System (ICS) Security initiatives
- Let AI/ML initiatives for the application of machine learning techniques to solving challenging security problems, bridging disparate cross-functional teams
- Cloud security technical lead for Deloitte's MXDR offering
- Built eminence through research, conference presentations, successful CTF team leadership, open-source code release
- Pioneered resilient, decentralized, secure, and performant communications networks

06/14-01/21 **R9B (root9B)** San Antonio, TX

Senior Research and Development Scientist

- Led root9B's R&D arm; tacking today's hardest technical problems and establishing a vision for the future
- Application security and vulnerability analysis, exploit development, cryptanalysis, hunting, malware reverse engineering
- Discovered many serious vulnerabilities in applications and cryptocurrency protocols

- Anonymity networks, highly autonomous systems, operational techniques, policy analysis, cloud security

Director, Emerging Technologies

- Built a small team focused on rapid capability development, grew to support operations & product development
- Pioneered memory-resident malware and credential assessment research, created unparalleled Orkos software

05/10-06/14 **United States Air Force – AFCERT** San Antonio, TX

- Created 15 new tactics and techniques for combating network intrusions
- Wrote numerous tools to identify, track, manipulate, and remove custom malware and targeted attackers
- Planned and led Defensive Cyber Operations; led the establishment of the USAF's enterprise-wide hunt team; directed investigations tracking down network intrusions

Officer-In-Charge, Intrusion Forensics, 33rd Network Warfare Squadron

- Reverse-engineered over 70 malicious samples, including Java, PDF, and browser exploits and malware
- Distinguished Graduate of Undergraduate Cyber Training and Intermediate Network Warfare Training
- Proposed and implemented numerous security improvements USAF-wide

06/10-06/14 **Metasploit Project**

Open-Source Security Software and Exploit Developer

- Writing client-side and privilege escalation exploits, persistence tools, and code injection techniques
- Attacks targeting Mozilla Firefox, Microsoft Office, Windows, McAfee, and Metasploit counterattacks
- Writing shellcode, payloads, DHCP and PXE servers, monitoring capabilities, and graphical user interface
- Maintaining Remote Procedure Call and GUI interfaces

06/08-08/08 **National Security Agency**

Web Development and Visualization

- Created a design and software interfaces for the display of geographic site information in Google Earth and Google Maps, displaying an overview of active topics and the NSA's use of its resources to respond to them
- AJAX programming with multiple databases and dynamic handling of large amounts of content
- Also created student website and improved the intern program website in style, ease of use, and readability

05/07-08/07 **Air Force Institute of Technology** Dayton, OH

Network Protocol Research

- Proposing and implementing protocol enhancements improving TCP performance in hostile environments

- Analyzing, testing, and rewriting existing research models
- Optimizing loss detection/recovery with existing congestion control algorithms

07/06-08/06 **SC Johnson & Son, Inc.** Racine, WI

Database Programming

- Developed database organization and user interface to meet department needs
- Wrote program to automatically handle data conversion and import
- Wrote code to perform detailed searches and handle different outputs and program flow
- Created complete documentation of database for users, administrators, and developers
- Enabled tracking of product registration and regulatory approval across many countries

Honors, External, and Volunteer Experiences

Selected Publications and Conference Presentations

- Presented "Internal Affairs: Hacking File System Access from the Web" at Black Hat (Las Vegas, US)
- Presented "Counterattack" at Black Hat (DC, US)
- Presented "Network Nightmare" at DEFCON (Las Vegas, US) and HackCon (Oslo, Norway)
- Presented "Mapping Privilege Escalation at Scale" at CanSecWest (Vancouver, Canada)
- Presented "Supply Chainsaw" at OPCDE (Dubai, UAE)
- Presented "Ambush" at BSides (Las Vegas, US) and DerbyCon (Louisville, US)
- Presented "Beyond E2E – Breaking and Remaking Modern Secure Communications" at Texas Cyber Summit
- Published "Chaos, Cryptology, and the Coupled Map Lattice" at Cedarville University

Collegiate Cyber Defense Competition Red Team

- Led the overall Southwest Regional CCDC Red Team (2012-2016)
- Core team member for CCDC National Finals Red Team (2015-present)

Educational and Training Honors

- Valedictorian, USAF Undergraduate Cyber Training
- Valedictorian, USAF Advanced Course in Engineering Cyber Security
- 1st, 1st, 2nd, and 2nd place annual Cedarville University Programming Competition
- Led top team in state, 3rd school in the US in the ACM International Collegiate Programming Contest-East Central region
- National Merit Finalist

Education

2006- 2010 **Cedarville University** Cedarville, OH

- Bachelor of Science in Mathematics and Computer Science (double-major), Bible minor
- GPA: 3.9

2005-2006 **University of Wisconsin-Parkside** Kenosha, WI

- 32 credit hours course work in Mathematics, Computer Science, and German
- GPA: 4.0