Andrew Kramer

509 N Blanche Ave, Madison SD, 57042
Personal: (530) 598-5619 | andrew@jmpesp.org
Work: (605) 256-5838 | andrew.kramer@dsu.edu

Education

PhD, Computer Science (IN PROGRESS) – Dakota State University – *Madison, SD* Aug 2021 – Present

MS, Applied Computer Science – Dakota State University – *Madison, SD* Aug 2015 – May 2017

BS, Cyber Operations – Dakota State University – *Madison, SD* Aug 2013 – May 2015

AA, Liberal Arts and Sciences – College of the Redwoods – *Eureka CA* Aug 2009 – May 2011

Work Experience

Assistant Professor of Cyber Operations – Dakota State University – *Madison, SD* Aug 2022 – Present

- CSC-432: Reverse Engineering
- CSC-748: Software Exploitation
- CSC-848: Advanced Software Exploitation

Instructor of Computer Science – Dakota State University – *Madison, SD* Aug 2017 – Aug 2022

- CSC-150: Computer Science I
- CSC-245: Information Security Fundamentals
- CSC-314: Assembly Language Programming
- CSC-431: Linux Administration

Deep Red Lab Director – Madison Cyber Labs (Madlabs) – *Madison, SD* June 2018 – Aug 2021

- Perform penetration tests and red team assessments for public and private sector partners.
- Research and develop novel tools tactics, techniques, and procedures (TTP's).
- Manage a small group of students working in the lab.

Cyber Security Internship – Johns Hopkins Applied Physics Lab – *Laurel, MD* May 2016 – Aug 2016

- Implemented "reverse execution" functionality in VM record-and-replay tool. (2016) May 2015 – Aug 2015
- Wrote test cases for much of the CWE dataset for use in a vulnerability discovery tool. (2016)
- Set up and managed a small cluster for distributed computing. (2015)
- Built an internet-connected vehicle capable of video streaming and gas-detection. (2015)

Penetration Test Engineer – Secure Banking Solutions – *Madison, SD* Feb 2014 – Sept 2014

- Located vulnerabilities in networks and systems belonging to financial institutions.
- Developed custom code to exploit complex security flaws.
- Performed social engineering tests on financial institutions, including pretext-calling and phishing.

Additional Activities

- **CyberCorps Scholarship for Service Co-PI**
  - Serve as a co-PI on DSU's CyberCorps Scholarship for Service grant from the National Science Foundation.
- **CAE Faculty Professional Development Trainer**
  - Teach summer crash-courses for other CAE university faculty, including topics such as stack and heap overflow exploitation, ROP, ALSR bypasses, browser exploitation, kernel exploitation, debugging and fuzzing.
- **GenCyber Camp Staff**
  - Regularly assist with summer GenCyber camps at DSU, including GenCyber Coed, GenCyber Girls, and GenCyber Teachers camps. Teach a variety of topics, including networking, wireless security, C programming, and electronics.

Projects, Research, and Achievements

- **DEFCON OpenSOC CTF 2020 - 1st Place Team**
  - https://dsu.edu/news/2020/08/team-takes-first-at-defcon.html
- **Wild West Hackin' Fest CTF 2019 - 1st Place Team**
  - https://mobile.twitter.com/n1ghthawk1/status/1187894127897260033
- **Slack Remote Code Execution via *[redacted until patched]***
  - https://hackerone.com/reports/922557
- **Fuzzing PHP with Domato**
  - https://blog.jmpesp.org/2020/01/fuzzing-php-with-domato.html
  - https://bugs.php.net/bug.php?id=79029
- **PHP Format String Exploitation**
  - https://blog.jmpesp.org/2016/07/exploiting-php-format-string-bugs-easy.html
  - https://www.exploit-db.com/exploits/39645
  - https://www.exploit-db.com/exploits/39082
- **Perl Leaks Memory by Design**
  - https://blog.jmpesp.org/2016/08/perl-leaks-memory-by-design.html
- **Linksys E-Series Remote Code Execution**
  - https://www.exploit-db.com/exploits/31683
- **CTF Writeups**
  - https://github.com/kernelpoppers/ctf_writeups/tree/master/TokyoWesterns2019/nothing_more_to_say
  - https://blog.jmpesp.org/2017/04/dakotacon-2017-ctf-write-ups.html
- **x86 Assembly Emulator**
  - https://github.com/Rewzilla/asemu
- **Distributed File-Format Fuzzer Using OpenMPI**
  - https://github.com/Rewzilla/distfuzz
- **Codegolf Competition Platform**
  - https://github.com/Rewzilla/codegolf-platform

Competencies

- **Languages:** C, x86 Assembly, Bash, Python, PHP, SQL.
- **Operating Environments:** Extensive Linux knowledge.
- **Reverse Engineering:** IDA Pro, Hopper, Ghidra, Olly, Immunity Debugger, objdump, GDB, Radare2.
- **Binary Exploitation:** Stack/heap exploitation, ASLR/DEP circumvention, pwntools, Chrome/V8, Linux kernel.