William Owen Redwood

CONTACT INFORMATION

Department of Computer Science
The Florida State University
Tallahassee, FL 32303

Mobile: +1-404-993-7677
E-mail: redwood@cs.fsu.edu

RESEARCH INTERESTS

Offensive security, cyber operations, 0day weaponization, insider threats, counterintelligence & fog computing, malware analysis & reverse engineering, and cyber-physical systems.

EDUCATION

Florida State University, Tallahassee, Florida USA

Ph.D Computer Science. Tentatively: May 2013 (**Current GPA 3.67**).

- Dissertation Topic: *Automating Counterintelligence for Insider Threats in National Security Systems*
- Area of Study: Fog Computing

M.S., Computer Science. April 30, 2011 (**GPA: 3.62**).

- Thesis Topic: *Proactive Network Defenses*
- Area of Study: Trust Management

Georgia Institute of Technology, Atlanta, Georgia USA

B.S., Computer Science. July 2008.

PROFESSIONAL EXPERIENCE

Sandia National Labs,
Livermore, CA USA
Center for Cyber Defenders Intern **May 2012 to Current**

- Project F.I.R.E.A.X.E.: Piloted DHS funded (blue + red team) hacking competiton involving voting machines.
- Project F.A.R.M.: Planning & development of next-gen cloud based malware analysis environment.
- Briefed POTUS advisor, congressmen, and other VIPs on projects
- Invited to participate in thinktank workshop for developing national cybersecurity policy

Florida State University,
Tallahassee, FL USA
Lead Instructor for "Offensive Security" **Jan 2013 to Current**

- New gradaute course that goes into hands-on depth with penetration testing and incident response techniques
- Designed and organized all the course material, and video taping every lecture (see URL below).
- 0day for anti-reverse engineering used against students in homework.
- Topics taught: x86 reverse engineering, exploitation development (windows and linux), shellcode development, polymorphic shellcode, network hacking, web application hacking, post exploitation, metasploit, and more
- http://www.cs.fsu.edu/~redwood/OffensiveSecurity/

Florida State University,
Tallahassee, FL USA
System Adminstrator for CS Department **Aug 2008 to May 2012**

- Assisted with the adminstration of Linux, Solaris, and Windows networks for the FSU CS Department.

Racetrac Petroleum HQ,
Atlanta, Georgia USA
Information Systems Intern **May 2007 to July 2007**

- Constructed an information map that details how the company earned all of its income.
- Established the documentation prototype standard and instruction manual to be used for all future process documentation.
- Won 1st place in the Intern competition project, by providing the standardized organizational plan for them to solve the back room clutter mess existing in every store.

Publications

Burmester, M., and W.O. Redwood. Dynamic Trust Management: Network Profiling for High Assurance Resilience. *MITACS Springer Volume on Advances in Network Analysis*. Book chapter in Springer Mathematics in Industry Series. Summer 2012.

Burmester, M., and W.O. Redwood. Markov anomaly modeling for Trust Management in variable threat environments. In: *Proceedings of the ACM:SE 2010*, April 17-20, 2010. Extended Abstract Talk.

Redwood, W.O. APECS: A Dynamic Framework for Preventing and Mitigating Theft, Loss, and Leakage of Mission Critical Information in Trust Management Networks. *Florida State University Master's Thesis*. May 2011.

Academic Appointments

SAIT Research Lab Director **October 2011 to present** Department of Computer Science,
The Florida State University

- Established a wide involvement among faculty and students in cyber security.
- Assisted and facilitated security research for SFS students.
- Promoted the learning of offensive security techniques for faculty and students.

Service

The Association for Computing Machinery (Student Chapter),
The Florida State University,
Office of Vice President **Fall 2011–Current**

- Successfully launched the first hacking competition @ FSU, titled "ACM D-FENSE", and was so succesfull it has continuted since.
- Introduced bi-weekly educational lecture seminars for students and faculty to teach vital programming tools such as Emacs, vi/vim, git/mecurial, gdb, and IDApro.

N0L3ptr *(A Cyber-Security focused student organization)*
The Florida State University,
Co-Founder & Leader **Fall 2011–Current**

- Participation in worldwide hacking competitions (aka CTF's). Recently placed in the **top 13% in the world** in largest hacking competition in history (CSAW 2012)
- Provides a safe environment for learning offensive security techniques for academic research.
- Hosts weekly workshops covering penetration testing / hacking techniques such as SQLi, shellcode, exploit development, and cyber warfare.

Conference Activity

1st place team for both competitions at the Los Alamos/Sandia National Labs **TracerFIRE 2011** Cyber Forensics Workshop (Dec, 2011).

Only team to hack the cyber physical system (a custom coffee machine). **TracerFIRE 2012** Cyber Forensics Workshop (Dec, 2012).

Conference Service

Volunteer organizer for: "NSF CyberTrust 2007", 14th NSF Conference on Cyber Security, Atlanta, GA, 2007.

Reviewer for The IEEE Journal on Selected Areas in Communications Special Issue on Advances in Digital Forensics for Communications and Networking (2010).

Reviewer for Oak Ridge National Labs Cyber Security and Information Intelligence Research Workshop (October 12-14, 2011).

Invited to review for the International Journal of Information Security (2012).

Skillset

Computer Programming:

- x86, C, C++, Java, JavaScript, Python, PHP, UNIX shell scripting (including POSIX.2), GNU make, SQL, MySQL.

Exploitation Technology:

- Metasploit, IDA pro, GDB, Wireshark, netcat.
- Fuzzing, x86 reverse engineering, (polymorphic) shellcode development, stack & heap exploitation, return-to-lib-c, and Return Oriented Programming (ROP).
- Bypassing DEP, ASLR, SAFE SEH, SEHOP, /GS Stack Cookies.
- SQLi, Cross Site Scriping (XSS), and XSS variants, malicious javascript.

Information/Internet Technology:

- Networking (UDP, TCP, ARP, DNS, Dynamic routing), Services (Apache, SQL, POP, IMAP, SMTP, application-specific daemon design), Cloud services (Openstack)
- Wireless networking transmission hardware and protocol simulation (GNURadio). Wireless waveform encoding, security, modulation, and transmission.

Operating Systems:

- Microsoft Windows family, Linux, BSD, Solaris, and other UNIX variants
- Windows and Linux administration, exploitation, post-exploitation, and rootkit design

Mathematics:

- Applied Mathematics, Applied Statistical Modeling, Real and Complex Analysis, Combinatorics, Markov Chains.