Zachary Cutlip

zachary.cutlip at gmail.com

Senior Vulnerability Researcher

Software security researcher with expertise in embedded device exploitation, software reverse engineering and vulnerability research.

Honors & Awards

Speaker:

- Black Hat USA 2012 [1]
- DEF CON 20 [2]
- University of Wisconsin "Lockdown 2013"
- 44CON 2013
- BayThreat 4

Projects & Publications:

- Bowcaster Exploit Development Framework [3]
- From SQL Injection to MIPS Overflows: Rooting SOHO Routers [4]
- Reverse Engineering and Exploiting the BT HomeHub 3.0b [5]

Education

- Johns Hopkins University
  - Master of Science in Computer Science
- Texas A&M University
  - Bachelor of Business Administration in Information Operations Management

Experience

- **Tactical Network Solutions, LLC**

  Senior Vulnerability Researcher, October 2011 – Present

  - Developed tools and techniques for research and exploitation of embedded systems
  - Reverse engineered proprietary networking API for a managed switch
    - Gained ability to write raw VLAN-tagged ethernet frames to the wire
  - Reverse engineered, binary patched BT modem's UPnP stack to run in emulation
    - Developed proof-of-concept exploit entirely in emulation
  - Implemented covert communications between cooperative processes embedded in traffic destined to a non-cooperating SSH server
  - Reverse engineered SOHO router vendor's UPnP stack
    - Identified and exploited partially implemented functionality for remote firmware upload
  - Co-instructed Introduction to Embedded Device Exploitation course
  - Helped develop Advanced Embedded Device Exploitation course
  - Developed surreptitious embedded device firmware, enabling encrypted, remotely triggered connection to a target behind a well-defended boundary

    - Developed a surreptitious implant capability tailored for a specific vendor's network infrastructure equipment
    - Developed a method of accepting incoming TCP connections undetectable by traditional port scanning tools
- **Raytheon Applied Signal Technology (formerly Seismic, LLC)**

  Senior Security Engineer, November 2009 – October 2011

    - Security tool development for the National Security Agency
    - Added custom capability to an open-source penetration testing framework
    - Developed tool-chain for decrypting, analyzing, & manipulating proprietary Remote Desktop Protocol data
    - Developed parser for Windows PE executable files and DLLs
- **Tresys Technology, LLC**

  Senior Software Engineer, March 2007 – November 2009

    - Developed (JMS) guarding appliance developing in pure C on Linux
    - Led vulnerability assessment of distributed intrusion detection system, uncovering multiple vulnerabilities through software reverse engineering and architecture review
    - Developed SELinux Mandatory Access Control Policy
- **National Security Agency/USAF**

  Operating System Vulnerability Analyst, May 2004 – June 2006

  Officer-in-Charge, ISSE Guards, March 2003 – March 2004

- **12th Air Force Network Operations Security Center**

  Crew Commander, August 2001 – March 2003

- **612th Air Communications Squadron**

  Communications Plans Officer, July 2000 – August 2001

---

[1] https://vimeo.com/64809593

[2] https://vimeo.com/64809592

[3] https://github.com/zcutlip/bowcaster

[4] http://tinyurl.com/agjr6bm [pdf]

[5] http://tinyurl.com/n9wnemp [pdf]

Resume Source: http://github.com/zcutlip/resume