# Zachary Cutlip

zachary[dot]cutlip[at]gmail.com

### Senior Security Researcher

### Summary

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

### Highlights

* March 2013: Created open source Bowcaster exploit development framework [1]
* October 2012: Published remote root exploit for BT HomeHub
* July 2012: Black Hat USA Presenter [2]
* July 2012: DEF CON 20 Presenter [3]

### Publications:

* From SQL Injection to MIPS Overflows: Rooting SOHO Routers [4]
* Introduction to Bowcaster [5],[6]
* BT HomeHub 3.0b Vulnerability Report [7],[8]

### 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

* + Vulnerability research and exploit development against embedded systems.
  + Co-instructed Introduction to Embedded Device Exploitation course.[9]
  + Helped develop Advanced Embedded Device Exploitation course.[9]
  + Developed surreptitious capability enabling connection to a target behind a well-defended boundary.  
    Encrypted, remotely triggered.
  + Developed a novel exploitation technique combining low-value, high-exposure vulnerabilities with high-value, low exposure vulnerabilities.
  + 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
  + Developed custom extensions for 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
  + Developed and maintained multipurpose C library, ensuring compatibility across multiple Windows and Unix OSes
* **Tresys Technology, LLC**

Senior Software Engineer, March 2007 - November 2009

* + Led development Java Message Service (JMS) guarding appliance
  + Achieved extremely high-performance JMS filter, developing in pure C on Linux
  + Developed automated build system producing bootable installation images from project source code
  + Led vulnerability assessment of distributed intrusion detection system, uncovering multiple vulnerabilities through software reverse engineering and architecture review
  + Developed SELinux Mandatory Access Control Policy for Red Hat Enterprise Linux based guarding solutions
  + Led development of an extensible filtering framework enabling the use of custom and off-the-shelf filter mechanisms
  + Numerous customer-facing roles including requirements analysis, system design, and on-site support
* **National Security Agency/USAF**

Operating System Vulnerability Analyst, May 2004 - June 2006

* + Developed method to fuzz executable file loaders in operating system kernels
  + Developed Linux & Unix security configuration guidance for DoD classified and unclassified Systems
  + Researched operating systems technology to identify vulnerabilities and corresponding mitigation strategies
  + Analyzed operating system source code to understand and validate implementation of security mechanisms

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

* + Led government and contractor team responsible for National Security Agency’s (NSA) Secret and Below Interoperability (SABI) network operations, and Information Assurance (IA)
* **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://github.com/zcutlip/bowcaster

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

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

[4] http://tinyurl.com/agjr6bm (media.blackhat.com)

[5] http://shadow-file.blogspot.com/2013/03/crossbow.html

[6] http://shadow-file.blogspot.com/2013/03/buffer-overflows-with-crossbow-part–1.html

[7] http://lists.grok.org.uk/pipermail/full-disclosure/2013-January/089348.html

[8] https://vimeo.com/52954499

[9] http://tacnetsol.com/training