

# Dionysus Blazakis

dion@semantiscopes.com

240-997-2591

- EDUCATION      ♦ **University of Maryland**, College Park, MD  
B.S. in Computer Science, Fall 1999 - Spring 2003
- INTERESTS      embedded security, operating systems, compilers, languages, vulnerability discovery,  
binary auditing
- PUBLICATIONS      *Interpreter Exploitation*  
D. Blazakis. 2010 USENIX Workshop on Offensive Technology (WOOT). Wash-  
ington DC, August 2010.  
*ATEMU: A Fine-grained Sensor Network Simulator.*  
J. Polley, D. Blazakis, J. McGee, D. Rusk, M. Karir, & J. S. Baras. Proceedings of  
the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc  
Communications and Networks (SECON). Santa Clara, CA, October 2004.
- PRESENTATIONS      *The Apple Sandbox.*  
Blackhat DC 2011.  
Crystal City, VA, January 2011.  
*Interpreter Exploitation.*  
Blackhat DC 2010.  
Crystal City, VA, February 2010.
- WORK  
EXPERIENCE      ♦ **Security Analyst**, Summer 2010 - Present  
Independent Security Evaluators, Inc.  
Baltimore, MD  
  
Working in a small team of 2 to 3 analysts, I evaluated the effectiveness of Digital Rights Management (DRM) systems for consumer devices such as cell phones, ebook readers, and childrens media devices. Often without source, I used static and dynamic reverse engineering techniques to understand protections, determine weaknesses, and create tools to perform attacks leveraging these weaknesses. In addition to client work, I was encouraged to spend time researching OS X and iOS system security and presented a part of that research. While DRM audits were a majority of our work, I also spent time doing source code audits for C, C++, C#, and Python applications. Additionally, I've spend some time doing software development for both clients and internal projects. Finally, at ISE, I wrote tools to discover vulnerabilities in both desktop and embedded devices. I was also part of the team that won the iPhone category of the 2011 PWN2OWN contest at the CanSecWest security conference.
- ♦ **Firmware Engineer**, Summer 2007 - Summer 2010  
EmbedICs LLC  
Columbia, MD  
  
At EmbedICs, I was tasked with evaluating the hardware memory protection features of a small microcontroller and summarizing best practices to mitigate possible attacks. Early at EmbedICs, I prototyped a multi-node simulator for networked embedded processors to support conformance testing and development. I also designed and implemented the firmware support for a proof-of-concept secure USB

Mass Storage device utilizing custom hardware crypto engines and a high speed USB controller. I also led the development of an in-field diagnostic device performing a man-in-the-middle attack to capture the smart card ISO-7816 communications.

- ◇ **Software**, Fall 2006 - Summer 2007  
Hillcrest Labs, Inc.  
Rockville, MD

The implementation and testing of a caching system for heterogeneous resources designed for an embedded target was one of my last tasks at Hillcrest Labs. The most interesting task I was given involved the reverse engineering a 2D graphics engine to reduce end-to-end latency. Coming from these results, I developed a kernel module to interface with a proprietary input device and graphics hardware.

- ◇ **Lab Manager**, Winter 2004 - Fall 2006,  
**Research Assistant**, Summer 2002 - Fall 2006,  
Hybrid Network Lab, Institute for Systems Research  
University of Maryland, College Park

While a lab manager, I participated in many levels of the research projects. I primarily developed network security techniques for networks of all scale (sensor nets to global routing). I audited a kernel implementation of MAODV, an adhoc multicast routing protocol, for memory misuse and other bugs. Driven by this experience, I developed a split kernel/userspace implementation of MAODV on top of an existing AODV implementation. I started and lead the development of ATEMU, a Mica2 sensor node emulator, and Xatdb, a gdb work-alike for multiple simultaneous sensor node simulators. Moving towards large scale networking, I developed a database for fast retrieval of internet wide routing information.

SOFTWARE

- ◇ **sbd**is, 2010  
A tool for decompiling XNU Sandbox profiles (along with a set of other scripts)
- ◇ **Voidness**, 2009  
A execution tracer for Windows using the Intel Pin DBI framework
- ◇ **DynaTrex**, 2009  
A dynamic binary instrumentation system for Windows XP
- ◇ **BGP-Inspect**, 2005-2006  
A custom database emphasizing speed and size for storage of internet wide routing information
- ◇ **ATEMU**, 2004  
A simulation and debugging suite for the Berkeley/Xbow Mica2 motes including simulations of the AVR ATmega microcontroller and the ChipCon CC1000 RF Transmitter/Receiver
- ◇ **MAODV-UMD**, 2003 - 2004  
A mostly user-space implementation of the Multicast Ad hoc On-demand Distance Vector (MAODV) routing protocol for Linux 2.4.
- ◇ **DionysOS**, 2002  
A toy OS written in IA32 assembly

SKILLS (IN ORDER OF EXPERTISE)

C, Python, C++, assembly (IA-32, x64, ARM, 6502, AVR, MIPS, 8051), gdb, OllyDbg, IDA (+ SDK), Haskell, WinDbg, C#, L<sup>A</sup>T<sub>E</sub>X

REFERENCES

Available upon request.