

Dionysus Blazakis

dion@semanticscope.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 development

PUBLICATIONS

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.

BGP-Inspect: Extracting Information from Raw BGP Data.

D. Blazakis, M. Karir, & J. S. Baras. Proceedings of the IEEE/IFIP Network Operations & Management Symposium (NOMS). Vancouver, Canada, April 2006.

Analyzing BGP ASPATH Behavior in the Internet.

D. Blazakis, M. Karir, & J. S. Baras. Proceedings of the 9th IEEE Global Internet Symposium (GIS). Barcelona, Spain, April 2006.

PRESENTATIONS

The BGP-Inspect Project.

The 35th North American Network Operators Group (NANOG-35).
Los Angeles, CA, October 2005.

WORK

EXPERIENCE

- ◇ **Firmware Engineer**, Summer 2007 - Present
EmbedICs LLC
Columbia, MD

My most recent task was the analysis of the memory protection features of a small microprocessor. I also summarized the best practices to mitigate any possible attacks. Early at EmbedICs, I prototyped a multi-node simulator for networked embedded processors to support conformance testing and development. Before the acquisition, I designed and implemented the firmware 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 a device performing a man-in-the-middle attack (on a key pairing algorithm) to capture the smart card ISO-7816 communications. This device supported the diagnosis of malfunctioning field units.

- ◇ **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

- ◇ **BaSO4**, 2009
A dynamic data-flow analysis framework for exploit development
- ◇ **Voidness**, 2009
A execution tracer for Windows using the Intel Pin DBI framework
- ◇ **DynaTrex**, 2009
A dynamic binary instrumentation system for Windows XP
- ◇ **DragonFlyBSD**, 2008
I contributed a few small bug fixes for DragonFlyBSD.
- ◇ **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 nodes 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, AVR, MIPS, 8051), OllyDbg, IDA (+ SDK), Haskell, C#, L^AT_EX

REFERENCES

Available upon request.