

JON OBERHEIDE

441 S 1st St, Apt 210
Ann Arbor, MI 48103

Cell: 248.760.3311
Email: jon@oberheide.org

EDUCATION

August 2006 - Present

University of Michigan Graduate School
Doctor of Philosophy (Ph.D.) - Computer Science / Software Systems

August 2006 - December 2008

University of Michigan Graduate School
Master of Science (M.S.) - Computer Science / Software Systems

August 2002 - May 2006

University of Michigan Undergraduate
Bachelor of Science (B.S.) - Computer Science / Mathematics

WORK EXPERIENCE

November 2009 - Present

Scio Security, Inc - Ann Arbor, MI
Co-Founder / CTO

January 2007 - Present

University of Michigan - Ann Arbor, MI
Security Researcher / PhD Candidate

September 2006 - January 2007

Arbor Networks, Inc - Ann Arbor, MI
Arbor Security & Engineering Response Team (ASERT)

- worked with ASERT to develop and deploy Arbor's Active Threat Level Assessment System (ATLAS), a distributed sensor network used to investigate emerging internet-scale threats
- assisted in the creation of Active Threat Feed (ATF) policies

May 2006 - September 2006

Arbor Networks, Inc - Ann Arbor, MI
Threat Management System (TMS) Group

- developed deep packet inspection signatures for the identification of numerous layer-7 protocols in PeakFlow TMS
- extensive security analysis and dissection of VoIP protocols such as SIP and H.323

May 2005 - May 2006

Merit Network, Inc - Ann Arbor, MI
Networking Research & Development

- efficient extraction of anomalous events from large BGP routing datasets (BGP-Inspect)
- real-time 3D visualization of network traffic and internet routing topology (Flamingo/VAST)
- published and presented research at conferences such as NANOG, NOMS, VizSec, etc

August 2004 - May 2005

Housing Information Technology Office - Ann Arbor, MI
IT Projects Office, University of Michigan

- developed a variety of web and system applications for the housing department
- audited code for security vulnerabilities including information disclosure, SQL injection, XSS attacks, and other unauthorized access

August 2000 - August 2004

FocalHost.com LLC - Troy, MI
Co-Founder

- ISP specializing in secure web services and database programming
- provided reliable and affordable web hosting to over 75 clients on *nix servers
- developed fully automated, in-house hosting management software

PAPERS / PRESENTATIONS

- **When Mobile is Harder Than Fixed: Demystifying Security Challenges in Mobile Environments**, Jon Oberheide and Farnam Jahanian, HotMobile '10, Annapolis MD, February 2010
- **Vulnerability Classes in the Linux Kernel**, Jon Oberheide, CERT Vulnerability Discovery Workshop, Arlington VA, February 2010
- **Internet Observatory Report**, Craig Labovitz, Danny McPherson, Scott Iekel-Johnson, Jon Oberheide, Farnam Jahanian, and Manish Karir, NANOG 47, Dearborn MI, October 2009
- **The More Things Change, the More They Stay the Same: Security Risk in Emerging Technologies**, Jon Oberheide, Intel Security Conference, Hillsboro, OR, September 2009
- **PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion**, Jon Oberheide, Michael Bailey, and Farnam Jahanian, WOOT '09, Montreal Canada, August 2009
- **Remote Fingerprinting and Exploitation of Mail Server Antivirus Engines**, Jon Oberheide and Farnam Jahanian, University of Michigan Technical Report CSE-TR-552-09, Ann Arbor MI, June 2009
- **If It Ain't Broke, Don't Fix It: Challenges and New Directions for Inferring the Impact of Software Patches**, Jon Oberheide, Evan Cooke, and Farnam Jahanian, HotOS XII, Monte Verita Switzerland, May 2009
- **A Look at a Modern Mobile Security Model: Google's Android Platform**, Jon Oberheide, CanSecWest 2009, Vancouver Canada, March 2009
- **Remote Security Services: Moving Security into the Network Cloud**, Jon Oberheide, IQPC Remote Services Implementation, San Francisco CA, February 2009
- **Virtualization Security Summit**, Jon Oberheide, Steve Orrin, Dino Dai Zovi, Dennis Moreau, and Hezi Moore, CSI Annual 2008, National Harbor MD, November 2008
- **CloudAV: N-Version Antivirus in the Network Cloud**, Jon Oberheide, Evan Cooke, and Farnam Jahanian, USENIX Security Symposium, San Jose CA, July 2008
- **Unraveling the VirtSec Debacle: Black Eyes and Emerging Opportunities**, Jon Oberheide, Lockdown 2008, Madison WI, July 2008
- **Understanding Malware Behavior for Network Security**, Jon Oberheide, IDGA Cyber Security for National Defense, Arlington VA, June 2008
- **Virtualized In-Cloud Security Services for Mobile Devices**, Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and Farnam Jahanian, MobiVirt '08, Breckenridge CO, June 2008
- **CloudAV: Malware Analysis in the Network Cloud**, Jon Oberheide, Merit Member Conference, Ann Arbor MI, June 2008
- **Exploiting Live Virtual Machine Migration**, Jon Oberheide, Evan Cooke, and Farnam Jahanian, Black Hat DC Briefings, Washington DC, February 2008
- **Automated Classification and Analysis of Internet Malware**, Michael Bailey, Jon Oberheide, Jon Andersen, Z. Morley Mao, Farnam Jahanian, and Jose Nazario, RAID '07, Australia, September 2007
- **Rethinking Antivirus: Executable Analysis in the Network Cloud**, Jon Oberheide, Evan Cooke, and Farnam Jahanian, HotSec '07, Boston, August 2007
- **Characterizing Dark DNS Behavior**, Jon Oberheide, Manish Karir, and Z. Morley Mao, DIMVA '07, Lucerne, Switzerland, July 2007

- **VAST: Visualizing Autonomous System Topology**, Jon Oberheide, Manish Karir, and Dionysus Blazakis, VizSEC '06, Virginia, November 2006
- **Flamingo Tutorial**, Manish Karir and Jon Oberheide, Internet2 Joint Techs Workshop, Madison WI, July 2006
- **Extracting Information from Raw Network Data**, Manish Karir and Jon Oberheide, IFIP Security Workshop, June 2006
- **Flamingo: Visualizing Internet Traffic**, Jon Oberheide, Michael Goff, and Manish Karir, Proceedings of IEEE/IFIP Network Operations & Management Symposium (NOMS), April 2006
- **Flamingo Presentation**, Manish Karir and Jon Oberheide, North American Network Operators Group (NANOG 36), Dallas TX, February 2006
- **Honeyd Detection via Packet Fragmentation**, Jon Oberheide and Manish Karir, Merit Technical Report, January 2006
- **The BGP-Inspect Project**, Manish Karir, Jon Oberheide, Dionysus Blazakis, and John Baras, North American Network Operators Group (NANOG 35), Los Angeles CA, October 2005

ADDITIONAL INTERESTS

- Independent security analysis and penetration testing
- Significant contributions to numerous open source projects
- Professional Services:
 - 2010 - DSN (Publicity Chair)
 - 2009 - CCS, DSN, IEEE S&P, IEEE TDSC, NSDI, QRASA (PC), WOOT (PC), WREN
 - 2008 - CCS, DSN, LEET, NDSS, RAID, SIGCOMM CCR, WOOT
 - 2007 - DSN, INM, LADC, RAID, SRUTI, USENIX Security, WOOT