JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DECLARATION OF MATTHEW MILLER

I, Matthew Miller, declare under penalty of perjury that:

1. I am an Assistant Professor of Computer Science and Information Technology at the University of Nebraska at Kearney. A copy of my CV is attached to this declaration. Based on my prior work analyzing FBI "Network Investigative Techniques," I have been retained by Mr. Michaud's defense team to speak to the importance of analyzing **all** source code used by the FBI in the deployment of a NIT.

2. As explained in the declaration of Vlad Tsyrklevich that has been previously presented to the Court, an NIT has four major components. Each of these components must be reviewed and verified by the defense for three basic reasons. First, to ensure that the evidence collected by the NIT is valid and accurate. Second, to ensure that the FBI's use of its NIT did not exceed what was authorized in the NIT search warrant, which is an emerging and serious problem with different types of sophisticated search and seizure technology now used by law enforcement agencies. Third, to develop potential defenses at trial based on the NIT having compromised the security settings on Mr. Michaud's computer and rendering it vulnerable to a host of viruses and

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

remote attacks that would explain to a jury why a defendant's data storage devices may contain child pornography that he or she did not intentionally download.

3. As the Court is aware, under normal circumstances the FBI would be able to target a specific user on the Internet by using their Internet Protocol (IP) address. This address identifies a user and is allocated to an Internet Service Provider (ISP). The ISP can identify each of their users and then the FBI can investigate that single user. When users use Tor, they are "anonymized" such that the FBI cannot readily identify them by their IP address because that IP address is not transmitted or shared in any retrievable way. The FBI must use an "exploit" in the software that the user is running on his or her computer to seize the IP address and other identifying information from that target computer directly. An exploit is a piece of software that takes advantage of a flaw in a computer system. Among other components, the FBI has not produced the exploit that was used in this case.

4. A computer system that has been exploited has been fundamentally altered in some way. This alteration may cause the computer to crash, lose or alter data, not respond to normal input or it may alter **any of the settings on that system.**[1] Depending on the exploit, it can affect the security posture of the computer going forward.[2]

5. Once a computer system's security has been compromised, the computer and any devices that have been connected to it (such as thumb drives, discs or other data storage devices) are also deemed to have been compromised and vulnerable to attack. As a result, the distinction the government has been trying to draw in various

---

[1] C. Smith, Dangerous Windows 10 flaw lets hackers secretly run any app on your PC, http://bgr.com/2016/04/25/windows-10-applocker-security-issue/, 2016.

[2] D. Goodin, New exploit leaves most Macs vulnerable to permanent backdooring, http://arstechnica.com/security/2015/06/new-remote-exploit-leaves-most-macs-vulnerable-to-permanent-backdooring/, 2015.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

pleadings that I have reviewed between Mr. Michaud's hard drive and other data storage devices is largely artificial, and it does not accurately reflect the realities of how devices interact or how malware and exploits can affect those devices.

6. For example, if the security firewall on a computer is disabled by an NIT or other malware, the firewall cannot prevent unauthorized access to the computer by third party attackers and remote computers. Remote attacks on computers are commonplace, with the attackers often automating the process of locating vulnerable computers and targeting them for viruses, remote transmission or storage of illicit materials, and similar misuse. These types of remote computer attacks are so pervasive that it is one of the main reasons that so much time, money and effort is expended by individuals and organizations (including the federal courts) to protect their computers and computer networks from malware.

7. Without knowing what exploit was used by the FBI in this case, we cannot determine whether the files that the government says were located on various storage devices were put on those devices by Mr. Michaud. This would include both the files on a hard drive and any files on removable devices that were connected to the hard drive at any time during or after the FBI's NIT attack on Mr. Michaud's computer. Removable media are basically extensions of the computer hard drive that can be detached. Malware has been known to infect removable media[3] (like thumb drives or data transferred to a cell phone) and this trend will only continue to escalate into the future.

8. I have had first hand experience dealing with the complex evidentiary issues that arise when the FBI uses an NIT. I was called upon to analyze a NIT used by the FBI in the Kirk Cottom case that was litigated in federal court in the District of

[3] F. Y. Rashid, CryptoLocker Morphs to Spread Over USB Drives, http://securitywatch.pcmag.com/malware/319400-cryptolocker-morphs-to-spread-over-usb-drives, 2014.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Nebraska in 2013 and 2014 (Case Number CR13-108). Mr. Cottom was a defendant in the predecessor to "Operation Pacifier" known as "Operation Torpedo."

9. Mr. Cottom's defense counsel asked to view the source code that the FBI had used to create the unique identifiers, encrypt identifiers, the NIT and the data logging code. The Government agreed to share **all** of the source code, except for specific code which the FBI reported to the court that it had lost. The binary code for the NIT was provided to our team along with the servers that supplied the NIT. The Government also provided us with access to **all** of the parts system that was used to deanonymize the users of the Tor network. Each time the defense team requested more source code, log files or server code, the Government did not dispute our need to analyze the data and provided us with access to the requested digital resources.

10. Having all the source code was key to ensuring (among other things also outlined in Mr. Tsyrklevitch's declaration) that the generation of the unique identifiers used for evidentiary data was correct. With the cooperation of the Government during discovery in the Cottom case, we were also able to verify that the NIT only sent back the data that was legally authorized by the search warrant issued in that case, something that remains unknown in Mr. Michaud's case and cannot be resolved by reference to the "data stream" or other fragments of discovery that the FBI is now offering to share.

11. We were further able to examine in the Cottom case how information was collected by both the NIT server and by the "deanonymizing" server. Perhaps most critically for the defense, we were able to determine what the FBI had or had not done to the security settings on Mr. Cottom's computer and whether a third party attack was an issue in the case. In my opinion, the FBI's unwillingness to produce the same type of NIT discovery in Mr. Michaud's case is inconsistent with the government's recognition in the Cottom case that all of the discovery that has already been ordered by this Court is relevant and indeed necessary for Mr. Michaud to prepare his defense.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

DONE this 9th day of May, 2016.

Matthew Miller

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Dr. Matthew James Miller

University of Nebraska at Kearney
Department of Computer Science and Information Systems
Otto Olsen, Room 116E
Kearney, NE USA 68845
Telephone: 308-865-8824

Cell Phone: (785) 410-3526
Email: millermj@unk.edu

Education

Ph.D. Computer Science, Kansas State University, 2012.

M.S. Computer Science, Kansas State University, 2007.

B.S. Computer Science, University of Nebraska at Kearney, 2003.

Employment

Assistant Professor: University Nebraska at Kearney **2015–Present**

- Courses taught
  - Introduction to programming CSIT-130
  - Computer Organization CSIT-301
  - Operating Systems CSIT-401
  - Software Engineering CSIT-404
  - Computer Security CSIT-458
  - Reverse Engineering CSIT-499
- Student projects
  - Developing a secure medical application for viewing Continuity of Care Documents

Consultant: Milhous Ink, LLC. Independant Contractor **2014–Present**

- Reverse Engineering a flash based Network Investigation Technique (NIT) developed by the FBI for de-anonymizing TOR end nodes Case Number 8:13-cr-00108-JFB-TDT Doc # 227-1 https://s3.amazonaws.com/s3.documentcloud.org/documents/2124281/fbi-tor-busting-227-1.pdf

Training/Certificates:

- Red Team Hunting DakotaCon 2016
- Advanced Penetration Testing DakotaCon 2015
- Advanced Reverse Engineering Black Hat Las Vegas 2014
- Malware Analysis DakotaCon 2014

Assistant Professor: Dakota State University **2012–2015**

- Courses taught with Online sections
  - Introduction to programming I CSC-150
  - Introduction to programming II CSC-250
  - Object Oriented Design CSC-260
  - Assembly CSC-314

- Reverse Engineering CSC-444
- Operating Systems CSC-456
- Android Development CSC-492
- Algorithm Analysis CSC-705
- Advanced Reverse Engineering for Ph.D. students CSC-844

◦ Service at Dakota State University
- Served as the Vice-president of General Faculty
- Helped develop the Applied Computer Science masters program
- Created a local programming contest
- Increased attendance of our ACM programming contest from 3 teams to 7 teams
- Taught at a 2 Coed Cybersecurity camp for high school students
- Taught at a 1 Girls Cybersecurity camp for high school students
- Worked on the Red-Team at the North Central CCDC Competition

◦ Student Research Projects at Dakota State University
- Created parallel password cracking software; abstract accepted at NCUR
- Developed a method of detecting and mitigating ROP attacks in software
- Developed Android applications for members of the community

◦ Advising 50+ students per semester about Computer Science and Cybersecurity

Programmer: The Onyx Collection **2007–2013**

◦ Created an online ordering system that handles $1+ million in sales per month

◦ Developed software to manage electronic order forms, electronic catalogs, product entry and product assembly

◦ Created an open source library for java to database interaction

NSF GK-12 Fellow: Kanas State University **2010–2012**

◦ Developed lessons for high school students that integrate sensory technology into the classroom
- Sensors included Wiimotes, Android phones, Lego MindStorms, Lego NXT, Wii Balance board, GPS Devices, Kinect and Cameras

◦ Taught lessons for Physical Education and Enhanced Learning Education

◦ Participated in outreach for other areas of Kansas (Dodge City, Wamego, Rock Creek)

Writer: The Master Teacher **2010–2012**

◦ Developed and wrote lesson plans for educators that explains classroom technology integration
- Topics included programming using OpenGL, Wiimotes in weightlifting, photography and Android application development

ESSI outreach program speaker: Kanas State University **2008–2012**

◦ Introduced middle school students to robotics and the use of computer science in society

EXCITE outreach program: Kansas State University **2005–2012**

◦ Developed curriculum for introducing female high school students to programming and robotics

- Coordinated, managed and taught the program to the high school students

Research Assistant: Kansas State University **2006–2008**

- Researched porting of shell scripts for SANDIA Turbo SIP from Linux to Windows
- Developed a distributed software system for the estimation of impact of irrigation on the Great Plains Aquifer in western Kansas
- Researched and developed an installer for porting the SANDIA Turbo SIP from Linux to OS X Leopard
- Developed a system for model checking the GMoDS goal model

Teaching Assistant: Kansas State University **2004–2006, 2008-2010**

- Developed curriculum and taught computer science class for non-programmers (CIS 111)
- Taught the lab portion for the Introduction to Computer Science class (CIS 200)
- Acted as a Teaching Assistant for the Computers and Society (ethics) class (CIS 415)
- Acted as a Teaching Assistant for the Concurrent Programming class (CIS 625)

Teacher for the Research Experience for Teachers (RET): Kansas State University **2004–2005**

- Taught curriculum to high school teachers that involved both hardware and software

Adjunct Instructor: University of Nebraska at Kearney **Fall 2003**

- Taught 1 section of CS-130

Course development at Dakota State University

- I redeveloped the assembly language class (CSC-314) to use an open source assemble that can be used for free on a linux server. The course was developed to lead directly into the reverse engineering course.
- I developed the reverse engineering course (CSC-444). This course is designed to meet the rigorous standards provided by the NSA. This course is key to the Center of Excellence designation that has been awarded to DSU.
- I developed the graduate reverse engineering course (CSC-844). This course is designed as the foundation for the PHD in Cybersecurity.

Works in Progress

Shadow Return a ROP Mitigation tool.

Analysis of FBI Network Investigative Tools

Publications

Tom Bulatewicz, Daniel Andresen, Stephen Welcha, Wei Jina, Sanjoy Dasb, and Matthew Miller. A software system for scalable parameter estimation on clusters. In *Proceedings of the 8th LCI International Conference on High-Performance Clustered Computing*, 2007.

Tom Bulatewicz, W Jin, S Staggenborg, S Lauwo, M Miller, S Das, D Andresen, J Peterson, David R Steward, and SM Welch. Calibration of a crop model to irrigated water use using a genetic algorithm. *Hydrology and Earth System Sciences*, 13(8):1467–1483, 2009.

Scott A DeLoach and Matthew Miller. A goal model for adaptive complex systems. *International Journal of Computational Intelligence: Theory and Practice*, 5(2):83–92, 2010.