# Tavish Vaidya

Georgetown University
Department of Computer Science
St. Mary's Hall,326A
3700 Reservoir Road, NW
Washington, DC 20057

Email: tavish@cs.georgetown.edu
Homepage: http://tvaidya.net

## Education

Ph.D. Student in Computer Science — Sept 2013 - Current
*Georgetown University, Washington D.C.*

M.S. in Computer Science — Sept 2013 - May 2015
*Georgetown University, Washington D.C.* GPA : 3.969

B. Tech. in Computer Science and Engineering — Aug 2008 – May 2012
*National Institute of Technology (NIT) Hamirpur, India* GPA : 8.54/10

## Experience

Graduate Research Assistant — Sept 2013 - Current
*Georgetown University, Washington DC*

Research focusing on network security and emerging security and privacy issues with voice as an input to smart devices.

Software Engineering Intern — June 2016 - August 2016
*Amazon, Seattle, WA*

Member of OpsTech Security team, independently developed an internal security tool for protecting mission-critical infrastructure.

Research Engineer — August 2012 - July 2013
*Centre for Development of Telematics, New Delhi*

Worked in Next Generation Networks Team, contributed to development of network stack and firewall framework for Multi-Core Terabit router.

Research Intern — May 2011 - Dec. 2011
*Indian Institute of Technology Bombay, Mumbai*

Developed "CUDA Based Out-of-Core Generic Matrix Multiplication algorithm" in C++, CUDA.
Worked on Large Scale Point-Based GPU Rendering Algorithms.

Web Developer, Student Team Leader — Feb. 2010 - March 2011
*National Institute of Technology Hamirpur, India & Laurea University of Applied Sciences, Finland*

Lead the Indian team of developers in contributing to "Massidea.org", a virtual collaborative model based on open innovation online community.

Software Developer — January 2010 - March 2011
*National Institute of Technology Hamipur, India*

Contributed to the development of "Brihaspati", a web-based virtual classroom and learning management system.
Server side development of official website for *NIMBUS*, annual technical festival of NIT Hamirpur.

## Peer-Reviewed Publications

*(**First co-authors, *Authors listed alphabetically, student authors first)*

1. Henri Maxime Demoulin**, Tavish Vaidya**, Isaac Pedisich, Nik Sultana, Yuankai Zhang, Ang Chen, Andreas Haeberlen, Boon Thau Loo, Linh Thi Xuan Phan, Micah Sherr, Clay Shields and Wenchao Zhou *A Demonstration of the DeDoS Platform for Defusing Asymmetric DDoS Attacks in Data Centers.* In Proceedings of SIGCOMM Posters and Demos '17, August 2017.

2. Tavish Vaidya, Eric Burger, Micah Sherr and Clay Shields. *Where art thou, Eve? Experiences Laying Traps for Internet Eavesdroppers.* In USENIX Workshop on Cyber Security Experimentation and Test (CSET), August 2017.
3. Ang Chen*, Akshay Sriraman, Tavish Vaidya, Yuankai Zhang, Andreas Haeberlen, Boon Thau Loo, Linh Thi Xuan Phan, Micah Sherr, Clay Shields and Wenchao Zhou. *Dispersing Asymmetric DDoS Attacks with SplitStack.* In ACM Workshop on Hot Topics in Networks (HotNets), November 2016.
4. Nicholas Carlini*, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner and Wenchao Zhou. *Hidden Voice Commands.* In USENIX Security Symposium (USENIX), August 2016.
5. Tavish Vaidya, Yuankai Zhang, Micah Sherr and Clay Shields. *Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition.* In USENIX Workshop on Offensive Technologies (WOOT), August 2015.
6. Tavish Vaidya, Eric Burger, Micah Sherr and Clay Shields. *Studying the Pervasiveness of Internet Interception with Honey{POP,SMTP,Telnet} (Poster).* In USENIX Security Symposium (USENIX), August 2015.
7. Lisa Singh, Hui Yang, Micah Sherr, Yifang Wei, Andrew Hian-Cheong, Kevin Tian, Janet Zhu, Sicong Zhang, Tavish Vaidya and Elchin Asgarli. *Helping Users Understand Their Web Footprints (Poster).* In International World Wide Web Conference (WWW), May 2015.
8. Tavish Vaidya and Micah Sherr. *Mind your $(R, \Phi)$s: Location-Based Privacy Controls for Consumer Drones.* In International Workshop on Security Protocols, March 2015.
9. Rhushabh Goradia, Tavish Vaidya, Linga Venkatesh, and Sharat Chandran. *CUDA Based Out-of-Core Generic Matrix Multiplication (Poster).* In HiPC Workshop on Hybrid Multi-core Computing, December 2011.

## Technical Reports

1. Tavish Vaidya. *2001-2013: Survey and Analysis of Major Cyberattacks.* arXiv:1507.06673v2 preprint, July 2015.
2. Tavish Vaidya. *How Private is your Privacy? Threats and Countermeasures for Protecting Digital Privacy.* December 2014.

## Talks

1. *Hidden Voice Commands.* IT-DEFENSE 2017, Berlin, February 2017 (Invited Talk).
2. *Hidden Voice Commands.* GeekPwn 2016, Palo Alto, October 2016 (Invited Talk).
3. *Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition.* USENIX Workshop on Offensive Technologies (WOOT), Washington DC, August 2015.
4. *Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition.* DC-Area Anonymity, Privacy, and Security Seminar (DCAPS), Georgetown University, Washington DC, November 2015.
5. *Mind your $(R, \Phi)$s: Location-Based Privacy Controls for Consumer Drones.* International Workshop on Security Protocols, University of Cambridge, UK, March 2015.

## Awards

1. Winner, ACM Student Research Competition at SIGCOMM 2017; awarded for *A Demonstration of the DeDoS Platform for Defusing Asymmetric DDoS Attacks in Data Centers.*, August 2017.
2. Best Paper Award, NYU Cyber Security Awareness Week Applied Research Competition; awarded for *Hidden Voice Commands* (appeared in USENIX Security 2016), November 2016.
3. 2nd Place, DHS Security Quiz, NYU Cyber Security Awareness Week, November 2016.
4. Winner, Deloitte Foundation Cyber Threat Competition, November 2015.
5. Sports Authority of India Outstanding Performance Scholarship, 2002 - 2006.

## Service

**External Reviewer**

11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2014).
9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014).

**President** August 2010 - May 2012
Forum Of Computer Engineers
National Institute of Technology (NIT) Hamirpur, India.

**Web Coordinator** August 2010 - March 2011
*NIMBUS*, annual technical festival of NIT Hamirpur.

## Teaching

Teaching Assistant, *Network Security (COSC-235)* Spring 2016, Spring 2017
Teaching Assistant, *Advanced Programming (COSC-150)* Fall 2016
Teaching Assistant, *Data Communications (COSC-255)* Spring 2014

## Selected Press

*Popular Science.* Researchers Have Successfully Tricked A.I. Into Seeing The Wrong Things.

*BBC.* 'Dalek' commands can hijack smartphones.

*CNBC.* Secret commands in online videos could hack your smartphone.

*The Atlantic.* The Demon Voice That Can Control Your Smartphone.

*The Register.* Drowning Dalek commands Siri in voice-rec hack attack.

*PCWorld.* Here's how secret voice commands in YouTube videos could hijack your smartphone.

*Popular Science.* Fooling The Machine: The Byzantine Science of Deceiving Artificial Intelligence.

*MIT Technology Review.* The 20 Most Infamous Cyberattacks of the 21st Century.