

HoTSoS *Symposium and Bootcamp*

HOT TOPICS *in the* **SCIENCE OF SECURITY**

APRIL 4-5, 2017 | HANOVER, MARYLAND

http://hot-sos.com



hosted by:

UNIVERSITY OF MARYLAND | VANDERBILT UNIVERSITY

HoTSoS Symposium and Bootcamp
HOT TOPICS in the **SCIENCE OF SECURITY**
April 4-5, 2017 | Hanover, MD

http://hot-sos.com

WELCOME

Welcome to the 4th Annual Hot Topics in the Science of Security (HoTSoS) Symposium and Bootcamp! The symposium will include a mix of invited talks, tutorials, presentations of refereed papers, a panel, and a poster session.

As in past iterations, the goal of HoTSoS is to bring together researchers, practitioners, and thought leaders from government, industry, and academia, and to provide a forum for dialogue centered upon the development and advancement of scientific foundations in cybersecurity. The technical emphasis of HoTSoS is on scientific methods, data gathering and analysis, experimental approaches, mathematical models, and the interactions among those approaches to build a foundational science of security. The HoTSoS vision is one of engaging and growing a community—including researchers and skilled practitioners from diverse disciplines—that is focused around the advancement of scientific methods as applied to cybersecurity.

As in previous years, HoTSoS 2017 specifically focuses on problems related to:

- **Scalability and composability** in the construction of secure systems,
- **Policy-governed collaboration** for handling data across different domains of authority while ensuring security and privacy,
- **Security metrics** and **improved measurement tools**, to guide choice-making in security engineering and response,
- **Resilient architectures** that can deliver service despite compromised components,
- **Analysis of human behavior**, encompassing users, operators, and adversaries, to support improved cybersecurity design.

This year, HoTSoS also solicited papers focusing on the above problems and having specific applications to **privacy**, broadly construed, and **security of cyber-physical systems**.

Submissions were subject to a rigorous reviewing process, and ultimately 9 out of 17 submitted papers were accepted. The committee also decided to accept two tutorials. We thank the members of the program committee for all their work.

We would also like to thank Amy Karns for designing the logo and helping to prepare the print materials, and Dana Purcell for her onsite support at the conference. We would especially like to express our appreciation to Katie Dey for her exceptional help throughout this entire process, including handling logistics, managing the web site, and interfacing with ACM. Finally, we acknowledge the NSA for their continual support of the science of security community.

Jonathan Katz
Michel Cukier
Xenophon Koutsoukos

TABLE OF CONTENTS

Welcome 2

Table of Contents 3

General Information 4

Organization 5

Program Agenda 6

Keynote Bios 8

Poster Listing 10

SoS Outreach 12

Local Restaurants 14

Notes 15

INFORMATION

REGISTRATION:

Registration will be located in the foyer of the Chesapeake Ballroom on the 2nd level. The registration desk will be open during the following times:

6:30 p.m. to 8:30 p.m. Monday
8:00 a.m. to 5:30 p.m. Tuesday
8:00 a.m. to 3:30 p.m. Wednesday

WIRELESS INTERNET CONNECTION:

A wireless Internet connection will be available in the Chesapeake Ballroom and foyer.

Network Name: BUSINESSGROUP-1
Username: user1
Password: one+one=2

SYMPOSIUM DINNER:

The symposium banquet will be held in the Sculpture Barn of the American Visionary Art Museum (AVAM). The AVAM is America's official national museum and education center for intuitive, self-taught artistry. The museum will be open to banquet attendees for self guided tours. Shuttle buses will be available to transport guests to the museum and then back to the hotel after the dinner. Please be in the hotel lobby at 6pm to board the shuttle bus. We will return to the hotel no later than 9:30pm.

AVAM Address:
800 Key Highway
Baltimore, Maryland 21230

POSTER SESSION:

Poster sessions will be be held in the Patuxent Ballroom during the following times:

Tuesday, April 4: 10:00 a.m. to 10:30 a.m.
Tuesday, April 4: 3:30 p.m. to 4:00 p.m
Wednesday, April 5: 10:00 a.m. to 10:30 a.m.

SYMPOSIUM PRESENTATIONS:

Symposium presentations and posters will be available online at:

http://cps-vo.org/hotsos17/agenda

SURVEY:

Please take a moment to respond to our short survey at:

http://cps-vo.org/hotsos17/survey

Your valuable feedback will help us plan future events.

ORGANIZATION

PROGRAM CHAIR:

JONATHAN KATZ is a professor in the Department of Computer Science at the University of Maryland where he conducts research on cryptography, privacy, and the science of cybersecurity. In 2013 he became director of the Maryland Cybersecurity Center. Katz has received numerous awards, including an NSF CAREER award in 2005 and a Humboldt Research Award in 2015. He was a member of the DARPA Computer Science Study Group from 2009-2010, and currently serves on the steering committee for the IEEE Cybersecurity Initiative as well as on the State of Maryland Cybersecurity Council. He is a co-author of the widely used textbook "Introduction to Modern Cryptography," now in its second edition.

CO-CHAIRS:

MICHEL CUKIER is the director for the Advanced Cybersecurity Experience for Students (ACES) and the associate director for education for the Maryland Cybersecurity Center. He also an associate professor of reliability engineering with a joint appointment in the Department of Mechanical Engineering.

XENOFON KOUTSOUKOS is a Professor of Computer Science, Computer Engineering, and Electrical Engineering in the Department of Electrical Engineering and Computer Science at Vanderbilt University. He is also a Senior Research Scientist in the Institute for Software Integrated Systems (ISIS).

PROGRAM COMMITTEE:

ADAM AVIV, United States Naval Acadamy
TRAVIS BREAUX, Carnegie Mellon University
ALVARO CARDENAS, UT Dallas
WILL ENCK, North Carolina State University
CHRIS GATES, Symantec
LIMIN JIA, Carnegie Mellon University
MICHAEL MAASS, Bosch Research
SAM MALEK, George Mason University
MICHELLE MAZUREK, University of Maryland
SAYAN MITRA, University of Illinois at Urbana Champaign
CHARLES MORISSET, Newcastle University
BILL SANDERS, University of Illinois at Urbana Champaign
BILL SCHERLIS, Carnegie Mellon University
JESSICA STADDON, North Carolina State University
ADAM TAGERT, National Security Agency
EUGENE VOROBEYCHIK, Vanderbilt University
SHOUHUAI XU, UT San Antonio

LOCAL ARRANGEMENTS AND PUBLICITY CHAIR:
KATIE DEY, Vanderbilt University

NSA LIASONS:
STEPHANIE ASKINS-YANNACCI, HEATHER LUCAS, and **TIM THIMMESCH**

GRAPHIC DESIGN:
AMY KARNS, Vanderbilt University

AGENDA

Tuesday, April 4

0800 - 1730	**Registration**
0830 - 0900	**Welcome and Introduction**
0900 - 1000	**Keynote: Security of Cyber-Physical Systems: Challenges and Approaches** *Insup Lee,* UPenn
1000 - 1030	**Posters and Break**
1030 - 1200	**SESSION 2**
	Paper: Leveraging Unique CPS Properties to Design Better Privacy-Enhancing Algorithms *Jairo Giraldo, Alvaro A. Cárdenas, Murat Kantarcioglu* University of Texas at Dallas
	Paper: Characterizing Scientific Reporting in Security Literature: An Analysis of ACM CCS and IEEE S&P Papers **Morgan Burcham, *Mahran Al-Zyoud, *Jeffrey C. Carver, †Mohammed Alsaleh, **Hongying Du, †Fida Gilani, ‡Jun Jiang, **Akond Rahman; **Özgür Kafalı, †Ehab Al-Shaer, **Laurie Williams* *University of Alabama, †UNC Charlotte, **NC State University, ‡UNC Chapel Hill
	Paper: Optimal Security Investments in a Prevention and Detection Game *Carlos Barreto, Alvaro A. Cárdenas, Alain Bensoussan* University of Texas at Dallas
1200 - 1330	**Lunch *(on your own)***
1330 - 1600	**SESSION 3**
1330 - 1430	**Keynote: Navigating Privacy Issues in A Data Driven World** *Jules Polonetsky,* Future of Privacy Forum
1430 - 1530	**Panel Discussion** **PANELISTS:** **David Melski, **Charles Nelson, †Sam Septembre, ‡Yan Shoshitaishvili* GrammaTech*, USCC**, Navy†, UC Santa Barbara‡
1530 - 1600	**Posters and Break**
1600 - 1730	**SESSION 4 - Parallel Tutorial Session**
	The Bugs Framework (BF) "Hands-On" *Irena Bojanova and Paul E. Black* National Intitute of Standards and Technology
	System Monitoring for Security *Xusheng Xiao,* Case Western Reserve University
1800	**Shuttle to AVAM for Dinner** *(Hotel Lobby)*

Wednesday, April 5

0800 - 1530 **Registration**

0900 - 1200 **SESSION 5**

0900 - 1000 **Keynote: Differential Privacy and Data Analysis**

Aaron Roth, UPenn

1000 - 1030 **Posters and Break**

1030 - 1200 **Paper: Learning a Privacy Incidents Database**

**Pradeep K. Murukannaiah, †Chinmaya Dabral, †Karthik Sheshadri, †Esha Sharma, †Jessica Staddon*

*Rochester Institute of Technology, †NC State University

Paper: On the Tradeoff Between Privacy and Utility in Collaborative Intrusion Detection Systems- A Game Theoretical Approach

**Richeng Jin, †Xiaofan He, *Huaiyu Dai*

*NC State University, †Lamar University

Paper: Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experiment

**Weining Yang, *Aiping Xiong, †Jing Chen, *Robert W. Proctor, *Ninghui Li*

*Purdue University, †New Mexico State University

1200 - 1330 **Lunch *(on your own)***

1330 - 1345 **Announcement of Best HoTSoS 2017 Poster**

HoTSoS 2018

Laurie Williams, North Carolina State University

1345 - 1515 **SESSION 6**

Paper: Global Variation in Attack Encounters and Hosting

**Ghita Mezzour, †Kathleen M. Carley, †L. Richard Carley*

*International University of Rabat, †Carnegie Mellon University

Paper: An Approach to Incorporating Uncertainty in Network Security Analysis

Hoang Hai Nguyen, Kartik Palani, David M. Nicol

University of Illinois at Urbana-Champaign

Paper: Surveying Security Practice Adherence in Software Development

***Patrick Morrison, **Benjamin H. Smith, *Laurie Williams*

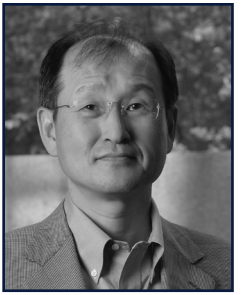
North Carolina State University*, IBM**

1515 - 1530 **Closing Remarks**

1530 **SYMPOSIUM ADJOURNED**

All sessions are in the Chesapeake Ballroom

KEYNOTE BIOS



Insup Lee is Cecilia Fitler Moore Professor of Computer and Information Science and Director of PRECISE Center, which he co-founded in 2008 at the University of Pennsylvania. His research interests include cyber-physical systems (CPS), real-time systems, embedded systems, high-confidence medical device systems, formal methods and tools, run-time verification, software certification, and trust management. The theme of his research activities has been to assure and improve the correctness, safety, and timeliness of life-critical embedded systems. His papers received the best paper awards in IEEE RTSS 2003, CEAS 2011, IEEE RTSS 2012, ACM/IEEE ICCPS 2014, and IEEE CPSNA 2016, and the best student paper award in IEEE RTAS 2012. Recently, he has been working in medical cyber-physical systems and security of cyber physical systems.

He has served on many program committees, chaired many international conferences and workshops and served on various steering and advisory committees of technical societies. He has also served on the editorial boards on the several scientific journals, including Journal of ACM, ACM Transactions on Cyber-Physical Systems, IEEE Transactions on Computers, Formal Methods in System Design, and Real-Time Systems Journal. He is Chair of ACM SIGBED (2015-2018) and was Chair of IEEE TC-RTS (2003-2004). He was a member of Technical Advisory Group (TAG) of President's Council of Advisors on Science and Technology (PCAST) Networking and Information Technology (2006-2007). He is a member of the National Research Council's committee on 21st Century Cyber-Physical Systems Education (2014-2015). He received an appreciation award from Ministry of Science, IT and Future Planning, South Korea in 2013. He is IEEE fellow and received IEEE TC-RTS Outstanding Technical Achievement and Leadership Award in 2008.



Aaron Roth is the class of 1940 Bicentennial Term Associate Professor of Computer and Information Science at the University of Pennsylvania computer science department, associated with the theory group, and the Warren Center for Network and Data Sciences. He is co-director of the program in Networked and Social Systems Engineering at the University of Pennsylvania and is also affiliated with the AMCS program (Applied Mathematics and Computational Science). He spent a year as a postdoc at Microsoft Research New England. Before that, he received his PhD from Carnegie Mellon University, where he was fortunate to have been advised by Avrim Blum. His main interests are in algorithms, and specifically in the areas of private data analysis, fairness in machine learning, game theory and mechanism design, and learning theory. Aaron is the recipient of a Presidential Early Career Award for Scientists and Engineers (PECASE), an Alfred P. Sloan Research Fellowship, an NSF CAREER award, a Google Faculty Research Award, and a Yahoo Academic Career Enhancement award.



Jules Polonetsky serves as CEO of the Future of Privacy Forum, a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the chief privacy officers of more than 110 leading companies, several foundations, as well as by an advisory board comprised of the country's leading academics and advocates. FPF's current projects focus on Big Data, Mobile, Location, Apps, the Internet of Things, Wearables, De-Identification, Connected Cars and Student Privacy.

Jules' previous roles have included serving as Chief Privacy Officer at AOL and before that at DoubleClick, as Consumer Affairs Commissioner for New York City, as an elected New York State Legislator and as a congressional staffer, and as an attorney.

Jules serves on the Advisory Board of the Center for Copyright Information. He has served on the boards of a number of privacy and consumer protection organizations including TRUSTe, the International Association of Privacy Professionals, and the Network Advertising Initiative. From 2011-2012, Jules served on the Department of Homeland Security Data Privacy and Integrity Advisory Committee.

In 2001, Crain's NY Business magazine named Jules one of the top technology leaders in New York City.

Jules is a regular speaker at privacy and technology events and has testified or presented before Congressional committees and the Federal Trade Commission.

His writing and research can be found on Google Scholar and SSRN.

POSTER LISTING

A Value Model for Implementing Cyber Metrics and Best Practices
**Natalie Scala, *Emil Manuel, *Rachel Fredman, *Jasmin Farahani and †Paul Goethals*
*Towson University, †United States Military Academy

Advanced Metrics for Risk-Based Attack Surface Approximation
Christopher Theisen and Laurie Williams
North Carolina State University

An Instruction Set Randomization Framework for Developing Secure and Resilient CPS
Brad Potteiger, Zhenkai Zhang, and Xenofon Koutsoukos
Vanderbilt University

Analysis of Two Parallel Surveys on Cybersecurity: Users & Security Administrators - Notable Similarities & Differences
**Sean Smith, *Vijay Kothari, †Jim Blythe, and ‡Ross Koppel*
*Dartmouth College, † ISI, University of Southern California, ‡ University of Pennsylvania

Convoy Leader: What Happens When They Know What They're Doing?
Carl Pearson, Allaire K. Welk, and Christopher B. Mayhorn
North Carolina State University

Cyber Knowledge is Here, but Not Evenly Distributed
Susan Campbell, Sunhee Kim, Valerie Karuzis, Scott Jackson, Meredith Hughes, and Alison Tseng
University of Maryland

Exploring Defect Categories for Infrastructure as Code
Akond Rahman and Laurie Williams
North Carolina State University

Factors for Differentiating Human from Automated Attacks
Kelly Greeling, Alex Withers, and Masooda Bashir
University of Illinois at Urbana-Champaign

FARM: a Toolkit for Finding the Appropriate Level of Realism for Modeling
Jim Blythe
ISI at University of Southern California

Flawed Mental Models Lead to Bad Cyber Security Decisions: Let's Do a Better Job
**Sean Smith, *Vijay Kothari, †Jim Blythe, and ‡Ross Koppel*
*Dartmouth College, † ISI, University of Southern California, ‡ University of Pennsylvania

Learning Factor Graphs for Preempting Multi-Stage Attacks in Cloud Infrastructure
Phuong Cao, Alexander Withers, Zbigniew Kalbarczyk, and Ravishankar Iyer
University of Illinois at Urbana Champaign

Formulating a Method for Using Search Query Trends as a Measure of Mass-User Interest
Shaown Sarker, Andrew McNamara, and Jessica Staddon
North Carolina State University

Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid
**Esther Amullen, **Hui Lin, and **Zbigniew Kalbarczyk*
Tennessee State University*, University of Illinois at Urbana-Champaign**

No (Privacy) News is Good News: An Analysis of Privacy News in the U. S. and U. K. from 2010-2016
Karthik Sheshadri, Nirav Ajmeri, and Jessica Staddon
North Carolina State University

Obsidian: A Safer Blockchain Programming Language
Michael Coblenz, Tyler Etzel, Joshua Sunshine, Jonathan Aldrich, Brad Myers, Eli Kanal, and Mark Sherman
Carnegie Mellon University

On the Disconnect between CVSS Scores and Vulnerability Bounties
Nuthan Munaiah and Andrew Meneely
Rochester Institute of Technology

Semantic Similarity in Security Regulations
Sarah Elder, Hui Guo, Munindar Singh, and Laurie Williams
North Carolina State University

Toward Effective Adoption of Security Practices
Shams Al-Amin, Nirav Ajmeri, Emily Berglund, Jon Doyle, and Munindar P. Singh
North Carolina State University

Toward Normative Threat Models to Prevent Misuse
Özgür Kafalı, Munindar P. Singh, and Laurie Williams
North Carolina State University

Towards Privacy-Preserving Mobile Apps: A Balancing Act
**Dengfeng Li, *Wing Lam, *Wei Yang, *Zhengkai Wu, †Xusheng Xiao, and *Tao Xie*
*University of Illinois at Urbana-Champaign and †Case Western Reserve University

What Makes Air Force Cyber Warfare Training Hard?
Lelyn Saner, Amber N. Bloomfield and Susan G. Campbell
University of Maryland

SOS OUTREACH

SCIENCE OF SECURITY LABLETS

The Science of Security Lablets, established in 2012, are dedicated to furthering Science of Security (SoS) goals for foundational research, enhancing the scientific rigor of cybersecurity, and growing the Science of Security community. The four lablets, Carnegie Mellon University (CMU), North Carolina State University (NCSU), University of Maryland (UMD), and University of Illinois at Urbana-Champaign (UIUC), work with a network of collaborating institutions, a total of 26 in all. The lablets meet together on a quarterly basis to present updates on current research against hard problems, exchange perspectives on progress in Science of Security, and strengthen the Science of Security community.

SCIENCE OF SECURITY AND RESILIENCE (SURE)

In 2014, the System Science of SecUrity and REsilience for cyber-physical systems (SURE) project was founded to investigate cybersecurity in the cyber-physical systems realm. SURE focuses on developing foundations and tools for designing, building, and assuring cyber-physical systems (CPS) that can maintain essential system properties in the presence of adversaries. The technology base of SURE will provide CPS designers and operators with models, methods, and tools that can be integrated with an end-to-end model-based design flow and tool chain.

BEST SCIENTIFIC PAPER COMPETITION

The Best Scientific Paper Competition, now in it's fifth year, is sponsored by the NSA Research Directorate to promote rigorous research methods by identifying and highlighting excellence. The competition is open to all authors and nominated papers are evaluated by a panel of distinguished experts in cybersecurity. Winners are invited to NSA for recognition and to present their research.

Last year, three papers were selected for recognition from the 54 nominations received. The winning paper was *Nomad: Mitigating Arbitrary Cloud Side Channels via Provider-Assisted Migration* by Soo-Jin Moon, Vyas Sekar and Michael Reiter from Carnegie Mellon University and University of North Carolina.

Two papers were recognized as honorable mentions: *Quantum-Secure Covert Communication on Bosonic Channels* by Boulat A. Bash, Andrei H. Gheorghe, Monika Patel, Jonathan L. Habif, Dennis Goeckel, Don Towsley, and Saikat Guha. *Increasing Cybersecurity Investments in Private Sector Firms* by Lawrence Gordon, Martin Loeb, William Luchshyn and Lei Zhou.

http://sos-vo.org/papercompetition

ANNUAL REPORT

The Science of Security Annual Report details the progress of the activities in the Science of Security research initiative. The most recent annual report, published in April 2017, highlights the work done in Fiscal Year 2016. For more information about the activities associated with the SoS initiative, browse through the SoS Annual Report at http://sos-vo.org/annualreport2016

THE SCIENCE OF SECURITY 5 HARD PROBLEMS

The Principal Investigators (PIs) of the Science of Security Lablets in collaboration with NSA Research, developed the 5 Hard Problems as a measure to establish the beginnings of a common language and guage progress. These 5 were selected for their level of technical challenge, their potential operational significance, and their likelihood of benefiting from emphasis on scientific research methods and improved measurement capabilities. The five are not intended to be all inclusive of everything that needs to be done in cybersecurity but rather five specific areas that need scientific progress. The five problems are: Scalability and Composability; Policy-Governed Secure Collaboration; Security Metrics Driven Evaluation, Design, Development, and Deployment; Resilient Architectures; and Understanding and Accounting for Human Behavior.



Scalability and Composability: Develop methods to enable the construction of secure systems with known security properties from components with known security properties, without a requirement to fully re-analyze the constituent components.



Policy-Governed Secure Collaboration: Develop methods to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains.



Security Metrics Driven Evaluation, Design, Development, and Deployment: Develop security metrics and models capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically), in a given context.



Resilient Architectures: Develop means to design and analyze system architectures that deliver required service in the face of compromised components.



Understanding and Accounting for Human Behavior: Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties.

INTERNATIONAL INTEL SCIENCE FAIR AWARD

The Intel International Science and Engineering Fair (ISEF) is the world's largest international pre-college science competition with approximately 1,800 high school students from more than 75 countries, regions, and territories. For the second consecutive year, the NSA Research Directorate sponsored a special award at the ISEF 2016. T he NSA Research Award at ISEF recognizes outstanding scientific accomplishment in cybersecurity.

Awards were presented to three research projects at the 2016 Intel International Science and Engineering Fair on May 12, 2016. Charles Noyes, 17, of Villa Park, California, won the special award for his project, "Efficient Blockchain-Driven Multiparty Computation Markets at Scale". Karthik Yegnesh, 16, of Eagleville, Pennsylvania and Rucha Joshi, 16, of Austin, Texas, received runner-up awards for their projects.

RESTAURANTS

George Martin's Grillfire
American Restaurant
7793 Arundel Mills Blvd A
Hanover, MD 21076
(410) 799-2883

Rangoli Restaurant
Indian Restaurant
10223 Nokesville Road
Manassas, VA 20110
(703) 957-4900

Vivo
Italian Restaurant
7793 Arundel Mills Blvd
Hanover, MD 21076
(410) 799-7440

Bagels and Grinds
Casual Cuisine
7791 Arundel Mills Blvd
Hanover, MD 21076
(410) 799-8333

Squisito Pizza and Pasta
Informal Italian Cafe
7690 Dorchester Blvd
Hanover, MD 21076
(410) 799-3325

Five Guys
Fast Food
7690 Dorchester Blvd
Hanover, MD 21076
(410) 799-3933

Maiwand Kabob
Afghani Restaurant
7698 Dorchester Blvd
Hanover, MD 21076
(443) 755-0461

Subway
Casual Cuisine
7000 Arundel Mills Cir
Hanover, MD 21076
(443) 755-9900

Red Lobster
Seafood Restaurant
7063 Arundel Mills Cir
Hanover, MD 21076
(410) 796-2390

Olive Garden
Casual Italian
7061 Arundel Mills Cir
Hanover, MD 21076
(410) 796-2750

Longhorn Steakhouse
Casual Steakhouse
7059 Arundel Mills Cir
Hanover, MD 21076
(410) 796-1427

Chick-fil-A
Fast Food
7055 Arundel Mills Cir
Hanover, MD 21076
(410) 799-2812

Chipotle Mexican Grill
Mexican Fast Food
7049 Arundel Mills Blvd
Hanover, MD 21076
(410) 796-5028

TGI Fridays
Casual Cuisine
7655 Arundel Mills Blvd
Hanover, MD 21076
(410) 379-6762

Potbelly Sandwich Shop
Retro-style Counter-serve
7049 Arundel Mills Blvd #103
Hanover, MD 21076
(410) 796-0415

Baja Fresh
Mexican Fast Food
7645 Arundel Mills Blvd #140
Hanover, MD 21076
(443) 755-0485

Flippin Pizza
New York-style Pizza
7645 Arundel Mills Blvd #100
Hanover, MD 21076
(443) 749-7919

The Greene Turtle
Casual Cuisine
7556 Teague Rd #100
Hanover, MD 21076
(410) 799-5001

NOTES

NOTES



sos-vo.org