# Sharon Goldberg

Associate Professor, Computer Science, Boston University
http://www.cs.bu.edu/~goldbe/
goldbe@cs.bu.edu

## Education

**Ph.D., Princeton University.** Department of Electrical Engineering. (2009)
Advisors: Jennifer Rexford (Computer Science), Boaz Barak (Computer Science)
Research area: Network security

**M.A., Princeton University.** Department of Electrical Engineering. (2006)
Research area: Optical communications

**B.A.Sc., University of Toronto.** Division of Engineering Science. Electrical Option. (2003)

## Employment

| | | |
|---|---|---|
| Commonwealth Crypto, Inc. | CEO/Co-Founder | (2017-Present) |
| Computer Science, Boston University. | Associate Professor. | (2015-Present) |
| Computer Science, Boston University. | Assistant Professor. | (2010-2015) |
| Microsoft Research New England. | Postdoc Researcher. | (2009-2010) |
| Princeton University. | Research Assistant | (2004-2009) |
| Cisco Systems. | Research Intern. | (Summer 2008) |
| IBM Research. Cryptography Group. | Research Intern. | (Summer 2007) |
| Hydro One Networks Inc. | Telecom Engineer. | (2003-2004) |
| Bell Canada. | Database Designer. | (Summer 2002) |
| Bell Nexxia. | Junior Internetworking Engineer. | (Summer 2001) |
| Personification Inc. | Intern. | (1999-2000) |

## Research Areas

As a network security researcher, I use tools from theory (cryptography, game-theory, algorithms) and networking (measurement, modeling, and simulation) to develop solutions that help practitioners surmount the hurdles they face when adopting new security technologies.

## Awards

N2Women: Rising Star in Networking and Communications (2017).
Hariri Faculty Fellowship, Boston University (2015-Present).
Sloan Research Fellowship (2014).
NSF CAREER Award (2014).
IETF/IRTF Applied Networking Research Prize for paper [W3] (2014).
IETF/IRTF Applied Networking Research Prize for paper [C9] (2014).
Hariri Junior Faculty Fellowship, Boston University (2013-2015).
Upton Fellowship, Princeton University (2004-2008).
Dean's Honour List, University of Toronto (1999-2003).

# Publications

## Full-length peer-reviewed conference papers.

[C1] The Unintended Consequences of Email Spam Prevention.
Sarah Scheffler, Sean Smith, Yossi Gilad, Sharon Goldberg.
Passive and Active Measurement Conference 2018 **PAM'18**, Berlin. March 2018.

[C2] The Security of NTP's Datagram Protocols.
A. Malhotra, H. Kennedy, M. Varia, J. Gardner, M. Van Gundy, S. Goldberg.
Financial Cryptography **FC'17**, Malta. April 2017.
`https://eprint.iacr.org/2016/1006.pdf`

[C3] TumbleBit: An Untrusted Tumbler for Bitcoin-Compatible Anonymous Payments
E. Heilman, F. Baldimtsi, L. Alshenibr, A. Scafuro, S. Goldberg.
**NDSS'17**, San Deigo, CA, February 2017. (15 pages.)
`http://eprint.iacr.org/2016/575.pdf`

[C4] Attacking the Network Time Protocol.
A. Malhotra, I.E. Cohen, E. Brakke, S. Goldberg.
**NDSS'16**, San Deigo, CA, February 2016. (15 pages.)
`http://eprint.iacr.org/2015/1020.pdf`

[C5] Eclipse Attacks on Bitcoin's Peer-to-Peer Network.
E. Heilman, A. Kendler, A. Zohar, S. Goldberg.
24th **USENIX Security** Symposium. Washington, DC. August 2015. (12 pages.)
`http://eprint.iacr.org/2015/263.pdf`

[C6] NSEC5: Provably Preventing DNSSEC Zone Enumeration
S. Goldberg, M. Naor, D. Papadopoulos, L. Reyzin, S. Vasant, A. Ziv.
**NDSS'15**, San Deigo, CA, February 2015. (15 pages.)
`http://eprint.iacr.org/2014/582.pdf`

[C7] From the Consent of the Routed: Improving the Transparency of the RPKI
E. Heilman, D. Cooper, L. Reyzin, S. Goldberg.
**SIGCOMM'14**. Chicago, Illinois. August 2014. (14 pages.)
`http://www.cs.bu.edu/~goldbe/papers/sigRPKI.pdf`

[C8] Calibrating Data to Sensitivity in Private Data Analysis: A Platform for Differentially-Private Analysis of Weighted Datasets.
D. Proserpio, S. Goldberg, F. McSherry.
$40^{th}$ Proceedings of the Very Large Databases Endowment (**VLDB'14**). September 2014. (12 pages.)
`http://www.vldb.org/pvldb/vol7/p637-proserpio.pdf`

[C9] Is the Juice Worth the Squeeze? BGP Security in Partial Deployment.
R. Lychev, S. Goldberg, M. Schapira.
**SIGCOMM'13**, Hong Kong, China. August 2013. (14 pages.)
**(Awarded an IETF/IRTF Applied Networking Research Prize, 2014.)**
`http://conferences.sigcomm.org/sigcomm/2013/papers/sigcomm/p171.pdf`

[C10] The Diffusion of Networking Technologies
S. Goldberg and Z. Liu.
Symposium on Discrete Algorithms (**SODA'13**). New Orleans, LA. January 2013. (18 pages.)
http://epubs.siam.org/doi/pdf/10.1137/1.9781611973105.113

[C11] Sequential Aggregate Signatures with Lazy Verification from Trapdoor Permutations
K. Brogle, S. Goldberg, L. Reyzin.
**ASIACRYPT'12**. Beijing, China. December 2012. (19 pages.)
http://link.springer.com/chapter/10.1007/978-3-642-34961-4_39

[C12] Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security.
P. Gill, M. Schapira, S. Goldberg.
**SIGCOMM'11**, Toronto, ON. August 2011. (14 pages.)
http://dl.acm.org/citation.cfm?id=2018439

[C13] Fine-Grained Latency and Loss Measurements in the Presence of Reordering.
M. Lee, S. Goldberg, R. R. Kompella, G. Varghese.
**SIGMETRICS'11**, San Jose, CA. June 2011. (12 pages.)
http://dl.acm.org/citation.cfm?id=1993778

[C14] How Secure are Secure Interdomain Routing Protocols?
S. Goldberg, M. Schapira, P. Hummon, J. Rexford.
**SIGCOMM'10**, New Delhi, India. August 2010. (14 pages.)
http://dl.acm.org/citation.cfm?id=1851195

[C15] Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP.
S. Goldberg, S. Halevi, A. Jaggard, V. Ramachandran, R. Wright.
**SIGCOMM'08**, Seattle, WA. August 2008. (14 pages.)
http://dl.acm.org/citation.cfm?id=1402989

[C16] Path-Quality Monitoring in the Presence of Adversaries
S. Goldberg, D. Xiao, E. Tromer, B. Barak, J. Rexford.
**SIGMETRICS'08**, Annapolis, MD. June 2008. (12 pages.)
http://dl.acm.org/citation.cfm?id=1375480

[C17] Protocols and Lower Bounds for Failure Localization in the Internet
B. Barak, S. Goldberg, D. Xiao.
**EUROCRYPT'08**, Istanbul, Turkey. April 2008. (20 pages.)
http://link.springer.com/chapter/10.1007/978-3-540-78967-3_20

### Policy reports.

[p1] Surveillance without Borders: The 'Traffic Shaping' Loophole And Why It Matters
S. Goldberg. Report: The Century Foundation. June, 2017. https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/

## Peer-reviewed journal articles.

[J1] Rethinking Security for Internet Routing.
R.Lychev, M. Schapira and S. Goldberg.
The Communications of the ACM (October 2016).
http://cacm.acm.org/magazines/2016/10/207763-rethinking-security-for-internet-routing/abstract

[J2] Attacking NTP's Authenticated Broadcast Mode.
A. Malhotra and S. Goldberg.
ACM SIGCOMM Computer Communication Review 47.2. April 2016. (5 pages.)
http://eprint.iacr.org/2016/055.pdf

[J3] Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad.
A. Arnbak, S. Goldberg. Michigan Telecommunications and Technology Law Review (MTTLR). Vol 21(2), May 2015. (46 pages.)
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2460462

[J4] Why is it Taking So Long to Secure Internet Routing?
S. Goldberg. The Communications of the ACM. (ACM Queue). October 2014 (8 pages.)
http://queue.acm.org/detail.cfm?id=2668966

[J5] Path-Quality Monitoring in the Presence of Adversaries: The Secure Sketch Protocols
S. Goldberg, D. Xiao, E. Tromer, B. Barak, J. Rexford.
IEEE/ACM Transactions on Networking. Volume:23, Issue:6. July 30, 2014. (13 pages.)
http://dx.doi.org/10.1109/TNET.2014.2339853

[J6] Sequential Aggregate Signatures with Lazy Verification from Trapdoor Permutations
K. Brogle, S. Goldberg, L. Reyzin.
Information and Computation (Elsevier). Volume 239. pp 356-376. December 2014.
http://dx.doi.org/10.1016/j.ic.2014.07.001

[J7] FineComb: Measuring Microscopic Latency and Loss in the Presence of Reordering
M. Lee, S. Goldberg, R. R. Kompella, G. Varghese.
IEEE/ACM Transactions on Networking. Volume: 22, Issue: 4. August 14, 2014. (14 pages.)
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06572888

[J8] A Survey of Interdomain Routing Policies.
P. Gill, M. Schapira, S. Goldberg.
ACM SIGCOMM Computer Communication Review 44.1. January 2013. (6 pages.)
http://dl.acm.org/citation.cfm?id=2567566

[J9] Modeling on Quicksand: Dealing with Scarcity of Ground Truth in Interdomain Routing Data.
P. Gill, M. Schapira, S. Goldberg.
ACM SIGCOMM Computer Communication Review, 42.1. pp 40-46. January 2012. (6 pages.)
http://dl.acm.org/citation.cfm?id=2096155

[J10] On the Teletraffic Capacity of Optical CDMA
S. Goldberg, P.R. Prucnal.
IEEE Transactions on Communications, 55.7. June 2007. pp 1334-1343. (10 pages.)
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4273692&tag=1

## Peer-reviewed workshop papers.

[W1] MaxLength Considered Harmful to the RPKI
Y. Gilad, O. Sagga, S. Goldberg.
**CoNEXT'17**, Seoul/Incheon, South Korea, December 2017.
https://eprint.iacr.org/2016/1015.pdf

[W2] Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Transactions
E. Heilman, F. Baldimsti, S. Goldberg.
3rd Workshop on Bitcoin and Blockchain (**BITCOIN'16**) at FC'16, Barbados, February 2016. (15 pages)
http://fc16.ifca.ai/bitcoin/papers/HBG16.pdf

[W3] On the Risk of Misbehaving RPKI Authorities.
D. Cooper, E. Heilman, K. Brogle, L. Reyzin, S. Goldberg.
Hot Topics in Networks **HotNets XII** workshop, Maryland. November 2013. (7 pages.)
**(Awarded an IETF/IRTF Applied Networking Research Prize, 2014.)**
http://dl.acm.org/citation.cfm?id=2535787

[W4] A Workflow for Differentially-Private Graph Synthesis.
D. Proserpio, S. Goldberg, F. McSherry.
SIGCOMM Workshop on Online Social Networks (**WOSN'12**). Helsinki, Finland. August 2012. (6 pages.)
http://conferences.sigcomm.org/sigcomm/2012/paper/wosn/p13.pdf

[W5] SINE: Cache-friendly Integrity for the Web.
C. Gaspard, S. Goldberg, W. Itani, E. Bertino, C. Nita-Rotaru.
5th IEEE Workshop on Secure Network Protocols (**NPSec'09**), Princeton, NJ. October 2009. pp. 7-12 (5 pages.)
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5342250

[W6] Security Vulnerabilities and Solutions for Packet Sampling.
S. Goldberg, J. Rexford.
**IEEE Sarnoff Symposium**, Princeton, NJ, May 2007. (7 pages.)
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4567339&tag=1

## Peer-reviewed posters and short papers.

[S1] RPKI vs ROVER: Comparing the Risks of BGP Security Solutions.
A. Malhotra, S. Goldberg.
Poster at **SIGCOMM'14** Chicago, IL. August 2014. (2 pages.)
http://eprint.iacr.org/2014/444.pdf

[S2] Brief announcement: Network Destabilizing Attacks
R. Lychev, S. Goldberg, M. Schapira.
**PODC'12.** Madeira, Portugal. July 2012. (2 pages; full technical report 14 pages.)
http://arxiv.org/pdf/1203.1681.pdf

[S3] Source matched spreading codes for optical CDMA
S. Goldberg, V. Baby, T. Wang, P. R. Prucnal.
IEEE Transactions on Communications 55.5. pp 850-854. May 2007. (4 pages.)
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4200945

[S4] Towards a Cryptanalysis of Spectral-Phase Encoded Optical CDMA with Phase-Scrambling.
S. Goldberg, R. Menendez, P. Prucnal
OSA Optical Fiber Communications Conference **(OFC'07)**, Anaheim, CA, March 2007. (3 pages; full technical report 19 pages.)
`http://www.opticsinfobase.org/abstract.cfm?uri=OFC-2007-OThJ7`

[S5] CMOS Limiting Optical Preamplifiers Using Dynamic Biasing for Wide Dynamic Range.
S. Goldberg, S. Lui, S. Nicolson, K. Phang.
ISCAS'04, Vancouver, BC, May 2004. (4 pages)
`http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1328979`

### Technical Reports.

[TR1] Can NSEC5 be Practical for DNSSEC Deployments?
D. Papadopoulos, D. Wessels, S. Huque, J. Vcelak, M. Naor, L. Reyzin, S. Goldberg.
ePrint (Cryptology) report 2017/099, February 2017.
`https://eprint.iacr.org/2017/099.pdf`

[TR2] An Efficient Zero-Knowledge Proof that RSA is a Permutation over $Z_N$
S. Goldberg, O. Sagga, F. Baldtimsi, L. Reyzin. September 2017.

[TR3] Passport: Enabling Accurate Country-Level Router Geolocation using Inaccurate Sources.
M.A. Rehman, S. Goldberg and D. Choffnes. September 2017.

## Security Vulnerability Disclosure

1. **CVE-2015-7704:** NTP: Denial of Service by Spoofed Kiss-o'-Death. (A. Malhotra, I. Cohen, and S. Goldberg.) `https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2015-7704`
2. **CVE-2015-7705:** NTP: Denial of Service by Priming the Pump. (A. Malhotra, I. Cohen, and S. Goldberg.) `https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2015-7705`
3. **CVE-2015-5300:** NTP: Small-step-big-step attack. (A. Malhotra, I. Cohen, and S. Goldberg.) `https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2015-5300`
4. **CVE-2016-7431:** NTP: Regression: 010-origin: Zero Origin Timestamp Bypass. (M. Van Gundy, A. Malhotra and S. Goldberg.) `http://support.ntp.org/bin/view/Main/NtpBug3102`
5. **CVE-2016-7433:** NTP: Reboot sync calculation problem. (A. Malhotra, S. Goldberg) `http://support.ntp.org/bin/view/Main/NtpBug3067`

# Internet Standards (Internet Engineering Task Force (IETF)

## Internet drafts.

An Internet Draft is a document published by the Internet Engineering Task Force (IETF) containing preliminary technical specifications.

[ID1] Verifiable Random Functions (VRFs)
S. Goldberg, L. Reyzin, D. Papadopoulos, J. Vcelak.
First posted as draft-goldbe-vrf in March 2017.
Adopted by the Crypto Forum Research group as draft-irtf-cfrg-vrf in August 2017.
`https://datatracker.ietf.org/doc/draft-irft-cfrg-vrf/`

[ID2] The Use of Maxlength in the RPKI.
Y. Gilad, S. Goldberg, K. Sriram.
First posted in March 2017.
`https://datatracker.ietf.org/doc/draft-yossigi-rpkimaxlen/`

[ID3] Message Authentication Codes for the Network Time Protocol.
A. Malhotra and S. Goldberg.
First posted as draft-aanchal4-ntp-mac in July 2016.
Adopted by the Network Time working group as draft-ietf-ntp-mac in January 2017.
`https://datatracker.ietf.org/doc/draft-ietf-ntp-mac/`

[ID4] Network Time Protocol REFID Updates.
H. Stenn and S. Goldberg.
First posted as draft-stenn-ntp-not-you-refid in July 2016.
Adopted by the Network Time working as draft-ietf-ntp-refid-updates in November 2016.
`https://datatracker.ietf.org/doc/draft-ietf-ntp-refid-updates/`

[ID5] NSEC5, DNSSEC Authenticated Denial of Existence.
J. Vcelak, S. Goldberg, D. Papadopoulos, S. Huque, D. Lawrence
First posted March 2015. Currently in -06 revision.
`https://datatracker.ietf.org/doc/draft-vcelak-nsec5/`

## Contributions.

I have contributed to the following IETF standards & drafts:

[IETF1] M. Lepinski. BGPSEC Protocol Specification.
`https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-protocol/`

[IETF2] D. Reilly, Ed., H. Stenn, D. Sibold. Network Time Protocol Best Current Practices.
`https://datatracker.ietf.org/doc/draft-ietf-ntp-bcp/`

[IETF3] N. Duffield, D. Chiou, B. Claise, A. Greenberg, M. Grossglauser, J. Rexford.
RFC 5474: A Framework for Packet Selection and Reporting. March 2009.
`http://tools.ietf.org/html/rfc5474`

### Participation in IETF working groups.

IETF Working Groups (WGs) are the primary mechanism for development of IETF specifications and guidelines. I am actively involved with the following working groups:

**IRTF CFRG (Crypto Forum Research Group).** (2017-Present)
Standardization of verifiable random functions (VRFs), a cryptographic primitive that the public-key version of a keyed cryptographic hash.

**IETF DNS Operations Working Group.** (2016-Present)
Standardization of innovations to the domain name system (DNS). My contributions focus on network security and the DNSSEC protocol.

**IETF Network Time Working Group.** (2016-Present)
Standardization of the network time protocol (NTP). My contributions focus mainly on network security.

**NTS IETF design team** (2016-Present)
I am part of a formal design team that is reviewing the design of the Network Time Security (NTS) protocol.

**IETF SIDR (Secure Interdomain Routing) Working Group.** (2012-Present)
Developing a standard for secure interdomain routing protocols.

**Member, BGPsec informal design team** (2009-11)
Part of a design team that developed a standard for a new secure interdomain routing protocol (BGPSEC) prior to beginning formal proceedings within the IETF.

## Policy working groups

### Cybersecurity Ideas Lab.

Worked with academics, industry, and U.S. government representatives to develop cybersecurity recommendations for the White House. (February 2014)

[A1] Cybersecurity Ideas Lab Report: Interdisciplinary Pathways towards a More Secure Internet. February 2014. `http://www.nsf.gov/cise/oad/cybersecurity_ideas_report.jsp`

### Federal Communications Commission (FCC).

**Member, FCC Communications Security, Reliability and Interoperability Council's (CSRIC) Working Group 6: Secure BGP Deployment.** Recommending the framework for industry regarding incremental adoption of secure routing protocols. (2012-Present)
I have coauthored the following reports:

[FCC1] FCC CSRIC III WORKING GROUP 6, Secure BGP Deployment, Final Report. March 2013. (33 pages.) `http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf`

[FCC2] FCC CSRIC III WORKING GROUP 6, Secure BGP Deployment, Interim Report. September 2012. (19 pages.) `http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG6-Final-Report.pdf`

[FCC3] FCC CSRIC III WORKING GROUP 6, Secure BGP Deployment, Interim Report. March 2012. (15 pages.) http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Fina pdf

# Presentations

### Congressional Briefing.

**Panelist.** Congressional Cybersecurity Caucus & Boston University
Congressional Briefing: The Other 95%: The Unsecure Internet You Dont Know About
With panelists J. Calendrino and J. Hall and moderator Provost J. Morrison.
Capitol Hill, DC, 06/2016.
http://www.bu.edu/today/2016/congressional-cybersecurity-caucus-briefing/

### Tutorials.

[T1] Tutorial: Why is it Taking so Long to Secure BGP?
TCE Summer School on Computer Security (Technion, Haifa, Israel. 09/2016. 3 hours.)
https://youtu.be/bjwbhmXTJKw?list=PLRC9d9zVR4XSTUhqv1zb-xnzXRznxBBhG

[T2] Tutorial: Securing the Domain Name System (DNS): Challenges and Pitfalls
TCE Summer School on Computer Security (Technion, Haifa, Israel. 09/2016. 1.5 hours.)

[T3] Tutorial: On the Security of the Network Time Protocol (NTP)
TCE Summer School on Computer Security (Technion, Haifa, Israel. 09/2016. 1.5 hours.)

[T4] Tutorial: The Diffusion of Networking Technologies
The 13th Conference on Electronic Commerce, EC'12 (Valencia, Spain. 06/2012. 3 hours.)

### Presentations to policy and standardization working groups.

[P1] Verifiable Random Functions (VRFs)
IETF'99, Crypto Forum Research Group (cfrg) Working Group meeting (Prague, CZ, 07/2017);
IETF'98, Security Area Advisory Group (saag) Working Group meeting (Chicago, IL, 03/2017);

[P2] NSEC5, DNSSEC Authenticated Denial of Existence
IETF'98, DNS Operations (dnsop) Working Group meeting (Chicago, IL, 03/2017).

[P3] Can NSEC5 be practical for DNSSEC deployments?
IETF Boston Hub (Cambridge, MA, 02/2017).

[P4] A Proposal for signaling consent from whacked RPKI objects.
IETF'91, Secure Interdomain Routing (sidr) Working Group meeting. (Honolulu, HI, 11/2014)

[P5] On the Risk of Misbehaving RPKI Authorities
Internet Engineering Task Force (IRTF) (Applied Networking Research Prize Talk) (Honolulu, HI 11/2014).

[P6] The Transition to BGP Security: Is the Juice Worth the Squeeze?
Internet Architecture Board (IAB) TechTalk (Conference call, 1/2014)
Department of Homeland Security (DHS) (12/2014).

[P7] Surgical Manipulations of the RPKI
Federal Communications Commission CSRIC Working group 6 - Secure BGP Deployment. (Conference call, 06/2012).

[P8] A Strategy for Transitioning to BGP Security
Department of Homeland Security BGPSec design team (Arlington, VA, 02/2011).

[P9] Cryptographic Signature Options for BGPsec
Department of Homeland Security BGPSec design team (Arlington, VA, 06/2010, 12/2010, 02/2011)

[P10] How Secure are Secure Routing Protocols?
Department of Homeland Security BGPSec design team (Arlington, VA 04/2010)

**Presentations at conferences and workshops.**

[L1] Surveillance without Borders: The Traffic Shaping Loophole and Why It Matters
SUMIT IT Conference, University of Michigan. (10/2017)

[L2] Can NSEC5 be Practical for DNSSEC Deployments?
DNS Privacy Workshop at NDSS'17 (San Deigo, CA, 3/2017).

[L3] NSEC5: Provably Preventing DNSSEC Zone Enumeration (Optimized & Implemented)
Real-World Cryptography Conference (New York, NY, 1/2017).

[L4] Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad
HotPETS'14, (Amsterdam, NL, 7/2014).
Telecommunications Policy Research Conference, (Washington, DC, 9/2014).
International Cybersecurity Conference, Academic Track. (Tel Aviv University, Israel, 6/2015).

[L5] NSEC5: Provably Preventing DNSSEC Zone Enumeration
Annual General Meeting of the DNS Operations, Analysis, and Research Center (DNS-OARC), (Los Angeles, CA, 10/2014).

[L6] The Transition to BGP Security: Is the Juice Worth the Squeeze?
I-CORE Day (Israeli Computer Science Day), Hebrew University (4/2014).
ICERM: Workshop on Mathematics of Data Analysis in Cybersecurity. (Providence, RI. 11/2014).
CyberSEED: Cybersecurity, Education & Diversity Week. (University of Connecticut. 11/2014).

[L7] From Internet Security to Internet Freedom: The Case of the RPKI
Citizen Lab's Connaught Summer Institute. (Toronto, ON, 7/2013).

[L8] A Workflow for Differentially-Private Graph Synthesis
DIMACS Workshop on Recent Work on Differential Privacy across Computer Science (10/2012).

[L9] The Diffusion of Networking Technologies
Bellairs workshop on algorithmic game theory. (Barbados. 04/2012).

[L10] A Strategy for Transitioning to BGP Security
Meeting of the North American Network Operators Group (NANOG'52) (Denver, CO. 06/2011)

[L11] How Secure are Secure Routing Protocols?
SIGCOMM'10 (New Delhi, India, 08/2010)
Meeting of the North American Network Operators Group (NANOG'49) (San Francisco 06/2010)
Microsoft Techfest (Redmond, 03/2010)
DIMACS Secure Routing Workshop (New Brunswick, NJ, 03/2010), ALIO-INFORMS session on "Routing and Incentives" (Buenos Aires, 06/2010)

[L12] Incentives for Honest Path Announcements in BGP
ACM SIGCOMM 2008 (Seattle, WA, 08/2008)
DIMACS Secure Routing Workshop (New Brunswick, NJ, 02/2008)

[L13] Path-Quality Monitoring in the Presence of Adversaries
ACM SIGMETRICS 2008 (Annapolis, MD, 06/2008)

[L14] Security Vulnerabilities and Solutions for Packet Sampling
IEEE Sarnoff Symposium (Princeton, NJ, 05/2007)

[L15] Towards a Cryptanalysis of Optical CDMA with Phase Scrambling
Optical Fiber Conference, OFC'07 (Anaheim, CA, 03/2007)
IPAM Securing Cyberspace Workshop on Hardware for Crypto (Los Angeles 12/2006)

[L16] Exploring the Benefits of CDMA in Optical Networks
PRISM Workshop on Optical Communications Technologies (Princeton, NJ, 02/2006)

**Research seminars in academia and industry.**

[S1] Routing through Loopholes in U.S. Surveillance Law,
Princeton University, Center for Information Technology and Policy (5/2017).

[S2] Fixing the Plumbing: Securing the Internet's Core Protocols
University of Michigan, Computer Science Seminar (1/2017),
University of Southern California, Computer Science Seminar (2/2017).
Princeton University, Computer Science Seminar (11/2017).

[S3] Attacking the Network Time Protocol
National Science Foundation, WATCH Seminar (Arlington, VA, 3/2017)
Google Networking Research Summit (Mountain View, CA, 2/2017),
Tufts, Computer Science Colloquium (Boston, MA, 3/2016),
Cisco Tech Talk (Cambridge, MA, 3/2016).

[S4] Using Traffic Shaping to Evade Oversight for Internet Surveillance
Boston University School of Law (11/2016),
UMass Amherst, CS & Policy Seminar (12/2016).

[S5] Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad
BU STEAM: Science, Technology, Engineering, Art, and Math. Undergraduate group. (Boston, MA, 05/2016).

[S6] On the Risk of Misbehaving RPKI Authorities
NYU Polytechnic University (Brooklyn, NY 3/2015),
IBM Research, Cryptography seminar (Yorktown, NY, 3/2015).
MIT Systems Security Seminar (Cambridge, MA, 5/2015).
Hebrew University Networking Seminar (Jerusalem, Israel, 6/2015).

[S7] The Transition to BGP Security: Is the Juice Worth the Squeeze?
Boston University, Hariri Institute (4/2014),
Princeton (9/2013),
Northeastern (10/2013),
UC San Deigo (10/2013),
Stanford (11/2013),
Berkeley (11/2013),
UMass Amherst (11/2013).
Cisco (San Jose, 11/2013),
Microsoft (Silicon Valley, 11/2013).

[S8] The Diffusion of Networking Technologies
Harvard Colloquium. (02/2013),
University of Toronto (08/2012),
Google Tech Talk (11/2013).

[S9] A Workflow for Differentially-Private Graph Synthesis
Microsoft Research. (Redmond, WA 07/2012).

[S10] A Strategy for Transitioning to BGP Security
MIT LIDS Seminar (11/2011),
MIT Security Seminar (02/2011),
Bar Ilan University (Tel Aviv, 05/2011),
Hebrew University of Jerusalem (05/2011),
Tel Aviv University (05/2011)
Google (Tel Aviv. 05/2011)

[S11] Cryptographic Signature Options for BGPsec
IBM Research Cryptography Seminar (Hawthorne, NY, 04/2011)

[S12] How Secure are Secure Routing Protocols?
MIT crypto seminar (03/2009),
Harvard colloquium (10/2009),
UC San Diego (02/2011),
Technion colloquium (Haifa, Israel 05/2011)
Cisco Tech Talk (San Jose 04/2010)

[S13] Securing Internet Routing
Microsoft Research (Cambridge, MA 01/2009),
MIT (02/2009),
Boston University (02/2009),
U Penn (02/2009),
Georgia Tech (03/2009)

[S14] Incentives for Honest Path Announcements in BGP
IBM Research (Hawthorne, NY, 08/2007 and 03/2008)
Cisco (San Jose, CA, 08/2008)
UC Berkeley (03/2008),
Tel Aviv University (Israel 04/2008),
Hebrew University (Jerusalem, Israel, 04/2008),
Stanford University (08/2008),
University of Toronto (08/2008),
Northwestern (2/2010)

[S15] Path-Quality Monitoring in the Presence of Adversaries
Microsoft Research (Cambridge, MA 01/2009),
Cisco (San Jose, CA, 03/2008).
Georgia Tech (02/2009),
New York University (12/2009),
Weizmann Institute (Israel, 04/2008),
Ben Gurion University (Be'er Sheva, Israel 04/2008),
University of Toronto (09/2009),
Brown University (11/2009)

[S16] A Cryptographic Study of Secure Internet Measurement
Stanford University (03/2007),
New York University (04/2007),
University of Maryland (05/2007),
Penn State (10/2007).

[S17] Towards a Cryptanalysis of Optical CDMA with Phase Scrambling
IBM Research (Hawthorne, NY, 01/2007),
Telcordia (Red Bank, NJ, 03/2007).

## Panels.

[O1] BU Tech Connect.
Panelist: Cryptocurrency panel.
With Panelists: Jamie Goldstein, Chetan Manikantan, Michael Sullivan, Jeremy Kauffman, Nathan Kaiser (Boston 2/2018).
`https://www.butechconnect.com/`

[O2] TIE StartupCon.
Panelist: Cybersecurity panel.
With panelists Deepak Taneja, Prasanna Gopalakrishnan, Ryan Rodrigue. (Boston, 10/2017).
`http://tiestartupcon.com/`

[O3] New England Security Day
Moderator: Panel on Bitcoin.
With panelists G. Andresen, I. Eyal, F. Baldimtsi. (Harvard, 05/2016).

[O4] Princeton CITP: Law and Technology Lunch Talk
Panelist: Online Privacy in Europe Versus the United States.

With panelist J. Reidenberg and moderator S. Barocas. (Princeton, 05/2016).
https://citp.princeton.edu/event/lt-onlineprivacy/

[O5] Beyond the Headlines: Cybersecurity Lessons From FBI vs. Apple
Panelist: Boston University Pardee School.
With panelist I. Arreguin-Toft and moderator J. Woodward. (Boston, 04/2016).
http://www.bu.edu/pardeeschool/2016/04/06/bth-lessons-in-cybersecurity-from-fbi-vs-apple/

[O6] 5th Annual International Cybersecurity Conference
Panelist: Privacy by Design. (Tel Aviv, Israel, 06/2015).

[O7] Boston University College of Arts and Science Teaching Workshop.
Presenter: Experiences with flipping the classroom. (Boston, 03/2015).

[O8] Comcast Cybersecurity Practitioner Symposium.
Panel moderator: Zero Trust Network Architecture, with panelists E. Amoroso, A. Boehme, C. Fulgham. (New York, 02/2015).

[O9] BU Alumni Relations: Gitner Lecture
Panel: Advancing the Human Condition.
With panelists R. Cappella, J. Harris, L. Hutyra, J. Menchik, H. Selin, V. Sapiro, A. Najam, and A. Janetos (Boston, 09/2014).

[O10] BU Alumni Relations, Breakfast Briefing:
Panel: Cybersecurity in a Post-Snowden World
With panelists Joseph Wippl and Tracey Maclin (Boston, 05/2014).

## Video

[V1] Internet Insecurity: A Primer on BGP
BU Today Video. (Boston University, 04/2015)
https://www.youtube.com/watch?v=PQoa2coBCDs

[V2] Security Weekly #445: Interview with Sharon Goldberg.
Paul Asadoorian. Security Weekly (1 hour live podcast/show.) December 17, 2015.
http://securityweekly.com/2015/12/22/security-weekly-445-interview-with-sharon-goldberg/

## National & Trade Press

The following stories covered my research paper [C3]:

[M1] "Legal loopholes could allow wider NSA surveillance, researchers say" CBS News. June 30, 2014. http://www.cbsnews.com/news/legal-loopholes-could-let-nsa-surveillance-circumvent-fo

[M2] "Scholars warn of NSA loopholes" The Boston Globe. July 10, 2014. http://www.bostonglobe.com/business/2014/07/09/scholars-warn-nsa-loopholes/Q0Gk1Jsnua25qb5DGXquRP/story.html#skip-target2

[M3] "Loopholes In U.S. Law Could Make It Easier For NSA Surveillance" Radio: WBUR 90.9 Boston (Boston's NPR radio station). July 11, 2014. http://radioboston.wbur.org/2014/07/10/nsa-loopholes

[M4] "How Traffic Shaping Can Help the NSA Evade Legal Oversight" Schneier on Security. July 1, 2014. https://www.schneier.com/blog/archives/2014/07/how_traffic_sha.html

[M5] "Loopholes for Circumventing the Constitution." Sounds of Dissent Radio Program, WZBC 90.3 Newton MA. 25-minute live interview. June 7, 2015.

[M6] "Secret loopholes drive NSA's 'unrestrained surveillance' on Americans" CNET. June 30, 2014. http://www.cnet.com/news/secret-loopholes-drive-nsas-unrestrained-surveillance-on-am

[M7] "Americans as 'vulnerable' to NSA surveillance as foreigners, despite Fourth Amendment" ZDNET. June 30, 2014. http://www.zdnet.com/americans-as-vulnerable-to-nsa-surveillance-as-f

[M8] "President Obama Needs to Cancel Executive Order 12333". Truthdig. July 23, 2014. http://www.truthdig.com/report/item/president_obama_needs_to_cancel_executive_order_12333_20140723

[M9] "Government can exploit loopholes for warrantless surveillance on Americans" Network World, Privacy and Security Blog. June 30, 2014. http://www.networkworld.com/article/2429409/microsoft-subnet/government-can-exploit-loopholes-for-warrantless-surveillance-on-america.html

[M10] "NSA Allowed to Spy On Pretty Much Anyone, Anywhere, Documents Reveal" reason.com. July 1, 2014. http://reason.com/24-7/2014/07/01/nsa-allowed-to-spy-on-pretty-much-anyone

[M11] "University Researchers Show NSA Can Legally Spy By Rerouting Internet Traffic" The College Fix. August 8, 2014. http://www.thecollegefix.com/post/18731/

The following stories covered my research paper [C3]:

[$\tau$1] Aaron van Wirdum. With TumbleBit, Bitcoin may have found it's winning answer. Bitcoin Magazine. October 25, 2016. https://bitcoinmagazine.com/articles/with-tumblebit-bitcoin-mixing Also posted on NASDAQ.com. http://www.nasdaq.com/article/with-tumblebit-bitcoin-mixing-may-

[$\tau$2] Kyle Torpey. TumbleBit Part 1: How Does This Bitcoin Privacy Proposal Compare to Monero and Zcash? Coin Journal. October 27, 2016. http://coinjournal.net/tumblebit-part-1-bitcoin-priva

[$\tau$3] Kyle Torpey. TumbleBit Part 2: How Does This Bitcoin Privacy Improvement Compare with CoinJoin and CoinShuffle? Coin Journal. November 13, 2016. http://coinjournal.net/bitcoin-privacy-improvement-compare-coinjoin-coinshuffle/

[$\tau$4] Kyle Torpey. TumbleBit Part 3: Potential Privacy Improvements for Bitcoins Lightning Network Coin Journal. November 21, 2016. http://coinjournal.net/tumblebit-part-3-potential-privacy

[$\tau$5] Elliot Maras. How TumbleBit Builds On CoinSwap To Improve Bitcoin Privacy And Fungibility. Crypto Coins News. October 30, 2016. https://www.cryptocoinsnews.com/how-tumblebit-builds-or

[$\tau$6] JP Buntix. TumbleBit Promises Guaranteed Anonymity For Bitcoin. BTC Manager. August 30, 2016. https://btcmanager.com/news/tech/tumblebit-promises-guaranteed-anonymity-for-bitco

[$\tau$7] Christopher Bergmann. TumbleBit: ein neues Protokoll zur Anonymisierung von Bitcoins. Bitcoin Blog.DE August 31, 2016. (In German). https://bitcoinblog.de/2016/08/31/tumblebit-ein-neues-protokoll-zur-anonymisierung-von-bitcoins/

[$\tau$8] Aaron van Wirdum. Better Bitcoin Privacy, Scalability: Developers Making TumbleBit a Reality February 10, 2017, 04:18:49 NASDAQ.com. http://www.nasdaq.com/article/better-bitcoin-privacy-scalability-developers-making-tumblebit-a-reality-cm746559

[$\tau$9] Olusegun Ogundeji. Bitcoin Payments, ZCash Mining in Focus of Two Latest Academic Works. Coin Telegraph. February 12, 2017. https://cointelegraph.com/news/bitcoin-payments-zcash-

[$\tau$10] Joseph Young. Why High Transaction Fees Arent a Big Issue for Bitcoin. CryptoCoins News. February 2, 2017. https://www.cryptocoinsnews.com/high-transaction-fees-arent-big-issue-bitco

The following stories covered my research paper [C4]:

[PS1] Richard Chirgwin. "Researchers Tag a New Brace of Bugs in NTP". The Register. October 28, 2016. http://www.theregister.co.uk/2016/10/28/researchers_tag_new_brace_of_bugs_in_ntp_but_theyre_fixable/

[PS2] Dan Goodin. "New attacks on Network Time Protocol can defeat HTTPS and create chaos." ars technica. October 21, 2015. http://arstechnica.com/security/2015/10/new-attacks-on-network-time-protocol-can-defeat-https-and-create-chaos/

[PS3] Joe Uchill. "Researchers warn computer clocks can be easily scrambled" Passcode, CS Monitor. October 21, 2015. http://www.csmonitor.com/World/Passcode/2015/1021/Researchers-reveal-how-attackers-could-turn-back-Internet-time
Also featured on MSN news. http://www.msn.com/en-us/news/technology/researchers-reveal-how-ar-BBmiK0k

[PS4] Jeremy Kirk. "Researchers warn computer clocks can be easily scrambled" Network World. October 21, 2015. http://www.networkworld.com/article/2996260/security/researchers-warn-comp html Also featured in PC World. http://www.pcworld.com/article/2996263/security/researchers-warn-computer-clocks-can-be-easily-scrambled.html

[PS5] Michael Mimoso. "Novel NTP Attacks Roll Back Time." Threatpost. October 22, 2015. https://threatpost.com/novel-ntp-attacks-roll-back-time/115138/

[PS6] Gil Gross. "Attacking the Network Time Protocol." Live Radio Interview. Talk 910am San Francisco. October 22, 2015.

[PS7] Jai Vijayan. "Undermining Security By Attacking Computer Clocks". Dark Reading. October 22, 2015. http://www.darkreading.com/vulnerabilities---threats/undermining-security-by-ad/d-id/1322800

The following stories covered my research paper [J4]:

[m1] Slashdot. "Why Is It Taking So Long To Secure Internet Routing?" http://tech.slashdot.org/story/14/09/17/0016241/why-is-it-taking-so-long-to-secure-internet-routing

[m2] "Sprint, Windstream traffic routing errors hijacked other ISPs". PC World. http://www.pcworld.com/article/2683052/sprint-windstream-traffic-routing-errors-hijacked-other-isps.html

[m3] "Who's Hijacking Internet Routes? Attacks Increase, But There's No Easy Fix in Sight" infoRisk Today. Mathew J. Schwartz, February 4, 2015. http://www.inforisktoday.co.uk/whos-hijacking-internet-routes-a-7874

Other press:

[ps1] "Supreme Court Rules Police Can't Search Cellphones Without a Warrant" Channel 5 News Boston, 6 O'Clock News. (Television.) June 26, 2014. http://www.wcvb.com/news/Supreme-Court-Police 26664880

[ps2] "The Long Life of a Quick Fix: Internet Protocol from 1989 Leaves Data Vulnerable to Hijackers." Craig Timberg. The Washington Post. (Print edition, page A1.) May 31, 2015. http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

[ps3] "Can an Israeli Solution Stop Network Hijacking?" Oded Yaron. Haaretz (National Newspaper of Israel). June 30, 2015. http://www.haaretz.co.il/captain/net/.premium-1.2671381

[ps4] "Problematic protocol that directs all Web traffic finally gets attention" Joe Uchill. CS Monitor (Passcode). August 8, 2015. http://www.csmonitor.com/World/Passcode/2015/0807/Problematic-protocol-that-directs-all-Web-traffic-finally-gets-attention

## Boston University Press

[BU1] Sara Rimer. "Cybersecurity Experts Go to Washington: Sharon Goldberg briefs Congressional staffers on internet insecurities" BU Today. 07.05.2016 https://www.bu.edu/today/2016/congressional-cybersecurity-caucus-briefing/

[BU2] Sara Rimer. "Will Unlocking Apples iPhone Unlock a Pandoras Box? CAS network security expert: move will weaken US cybersecurity." BU Today. 03.15.2016 http://www.bu.edu/today/2016/unlocking-terrorist-iphone-cybersecurity/

[BU3] Rich Barlow. "CAS Team Finds Flaw in Computers Timekeeping." BU Today. 10.22.2015. http://www.bu.edu/today/2015/hacking-network-time-protocol/

[BU4] Lara Ehrlich. "Internet Insecurity: CAS computer scientists are safeguarding the internet and defending civil rights." BU Today. 04.23.2015 http://www.bu.edu/today/2015/internet-insecurity/

[BU5] Amy Laskowski. "BU Duo Named 2014 Sloan Fellows: CAS early career scientists honored." BU Today. 03.24.2014. http://www.bu.edu/today/2014/bu-duo-named-2014-sloan-fellows/

# Funding

[G1] **Principal Investigator.** Cisco Research Center.
Securing the Network Time Protocol.
Awarded October, 2015. (Duration unspecified.)

[G2] **co-Principal Investigator.** Verisign Labs.
NSEC5: Provably Preventing DNSSEC Zone Enumeration. (With co-PI: L. Reyzin).
Awarded December, 2014. (Duration unspecified.)

[G3] **co-Principal Investigator.** National Science Foundation.
TWC: Collaborative: Frontier: Secure Cloud Services: A Compositional Approach.
(With co-PIs: R. Canetti, J. Appavoo, A. Bestavros, S. Goldwasser, F. Kaashoek, G. Kollios, O. Krieger, M. Van Dijk, D. Wichs, N. Zeldovich)
Awarded Fall 2014. (Duration: 2014-2019.)

[G4] **co-Principal Investigator.** Cisco Research Center.
Hardening the RPKI against Faulty or Misbehaving Authorities. (With co-PI: L. Reyzin)
Awarded April 8, 2014. (Duration unspecified.)

[G5] **Sloan Research Fellowship.** Sloan Research Foundation.
Awarded February 18, 2014. (Duration: 2014-2016.)

[G6] **Principal Investigator.** National Science Foundation.
CAREER: Centralized Authorities in Internet Security: Risk Assessment, Mitigation, and New Architectures.
Awarded February 2014. (Duration: 2014-2019.)

[G7] **co-Principal Investigator.** National Science Foundation.
EAGER: Holistic Security for Cloud Computing: Architecture for Modular System and Network Design. (With co-PIs: O. Krieger, J. Appavoo, J. Byers)
Awarded Summer 2013. (Duration: 2013-2014.)

[G8] **Principal Investigator.** National Science Foundation.
TC: SMALL: Deployment Incentives for Secure Internet Routing.
Awarded Summer 2010. (Duration: 2010-2014.)

[G9] **Co-Principal Investigator.** National Science Foundation.
TC: LARGE: Securing the Open Softphone. (With co-PIs: M. Crovella, L. Reyzin, A. Trachtenberg, S. Homer, N. Triandopoulos, D. Starobinski, M. Karpovsky, T. Zlateva)
Awarded Summer 2010. (Duration: 2010-2015.)

[G10] **Principal Investigator.** Cisco Research Center.
Partial Deployments of Secure Routing Protocols.
Awarded Summer, 2010. (Duration unspecified.)

# Teaching

| Term | Year | Course Number and Name | # Students | |
|---|---|---|---|---|
| Spring | 2017 | CS558 Network Security | 103 | Scaled course to 100 students |
| Fall | 2016 | CS237 Probability and Computing | 94 | |
| Fall | 2015 | CS558 Network Security | 50 | |
| Spring | 2015 | CS558 Network Security | 59 | |
| Fall | 2014 | CS237 Probability and Computing | 45 | Updated syllabus |
| Spring | 2014 | CS558 Network Security | 53 | Updated syllabus |
| Spring | 2013 | CS558 Network Security | 15 | Updated syllabus |
| Fall | 2012 | CS237 Probability and Computing | 63 | Revamped course |
| Spring | 2012 | CS558 Network Security | 19 | New course |
| Fall | 2011 | CS237 Probability and Computing | 46 | |
| Spring | 2011 | CS237 Probability and Computing | 61 | New course |
| Fall | 2010 | CS591 Seminar in Network Security | 15 | New Research seminar |

Organizer of BUsec weekly seminar in cryptography and security at Boston University since 2011.

**Notes on course development.**

CS558 in Fall 2015 was co-taught with Dr. Foteini Baldimtsi. No other courses were team taught.

**CS237** was offered before I arrived at BU. The first time I taught this course, in 2011, I completely revamped it, basing it on course that is offered at MIT (6.042), and adding material on randomized algorithms. In 2013, I once again revamped the course to include a significant programming and active learning component; the programming aspects of the course are constantly evolving.

**CS558** was offered before I arrived at BU. I completely revamped this course the first time I taught it in 2011. In 2011-2013, the course was taught to a small class, without no support from graders or teaching fellows; each of those years I substantially revised the course material, most of which I developed on my own, and some of which was based on courses at Stanford (CS 155) and Princeton (CS 433). In 2014, the course was scaled to 60 students, with support from a teaching fellow and a grader; in addition to once again revising the course material, we added a significant programming component, including two original assignments and three assignments developed at University of Michigan (ECE388). In 2017, the course was again scaled up to a class of 100 students with support from three teaching assistants.

Material and pedagogy from CS558 has been incorporated into courses at Stonybrook University, U Mass Amherst, George Mason University, University of Rochester, Mills College in Oakland, CA, an AP Computer Science Course at the Advanced Math and Science Academy High School in Marlborough, MA, and discussed at meetings of the CSTA of MA (the CS Teachers Association of MA, an association of local CS high school teachers).

# Students

## Post-Doctoral research advisees.

**Foteini Baldmitsi (2014-2016)**
Research on electronic cash, credentials and cryptocurrency.
Started as an assistant professor of computer science at George Mason University.

**Yossi Gilad. (2015-Present)**
Research on network protocol and cloud security.

## Doctoral research advisees.

**Phillipa Gill. (Ph.D. University of Toronto 2012)**
Thesis: "Improving Dependability for Internet-Scale Services"
Visited from University of Toronto in Fall 2010. I chaired her PhD Committee.
Started as an assistant professor of computer science at Stonybrook University.

**Robert Lychev. (Ph.D. Georgia Tech 2014)**
Visited BU August 2011-December 2013.
Research on routing security.
Awarded IETF/IRTF Applied Networking Research Prize.
Started as a researcher at MIT Lincoln Labs.

**Davide Proserpio. (Ph.D. Boston University, 2016)**
Research on data privacy and electronic commerce.
Started as an assistant professor of marketing at University of Southern California (USC).

**Ethan Heilman. (Ph.D. Candidate, BU, since 2013)**
Research on Internet freedom, RPKI abuse, bitcoin.
Awarded IETF/IRTF Applied Networking Research Prize.

**Aanchal Malhotra. (M.S., BU, 2015. Ph.D. Candidate, BU, since 2015)**
Research on the security of the Network Time Protocol (NTP).

## Masters research advisees.

**Jef Guarante. (M.S. BU 2012.)**
Thesis: "On the Computational Efficiency of Private Information Retrieval"
Co-advised with Leo Reyzin.

**Sachin Vasant. (M.S. BU 2014)**
Thesis: "Cryptographic Evaluation of Zone-Enumeration in DNSSEC"
Co-advised with Leo Reyzin.
Started as a security engineer at Cisco.

**Yun Sheng. (M.S. BU 2016.)**
Research on interdomain traffic measurement, Summer 2015.
Co-advised with David Choffnes (Northeastern).
Started as an engineer at Zoominfo.

## Undergraduate research advisees.

**Kyle Brogle. (B.A. BU 2012.)**
Research on routing security and cryptography. Co-advised with Leo Reyzin. (2010-2012.)
Honorable mention for the CRA Outstanding Undergraduate Researcher Award (2012).
Boston University Computer Science Undergraduate Research Award (2012).
IETF/IRTF Applied Networking Research Prize. (2014)
Started as a graduate student at Stanford. Now on a security team at Apple.

**Danny Cooper. (B.A. BU 2014)**
Research on RPKI abuse, Summer 2012 - Summer 2014.
Awarded IETF/IRTF Applied Networking Research Prize. (2014)
Boston University Computer Science Undergraduate Research Award (2014)
Started as a security researcher at Akamai.

**Adam Udi. (B.A./M.A. BU 2013)**
CS237 course design assistant.
Research on BGP-based censorship, Summer 2012-Summer 2013.
Started as a developer at tripadvisor.

**Anthony Faraco-Hadlock. (B.A. BU 2015)**
Research on interdomain traffic measurement, Fall 2013 - Spring 2014.
Started as intern with Microsoft's security team in Summer 2014.

**AJ Trainor. (B.A. BU expected 2016)**
Research on interdomain traffic measurement, Summer 2014.

**Alison Kendler. (B.A. BU expected 2016)**
Research on routing security and bitcoin, Summer 2014-Summer 2015.
Finalist for 2016 CRA undergraduate research award.
Started as a security researcher at MITRE.

**Isaac Cohen. (B.A. BU expected 2016)**
Research on NTP security, Summer 2015.
Honorable mention for 2016 CRA undergraduate research award.
Started as a developer at Microsoft.

**Erik Brakke. (B.A. BU expected 2016)**
Research on NTP security, Spring 2015.
Started as a developer at Carbonite.

**Monica Martin. (B.A. BU expected 2016)**
Research on routing protocol security, May 2015.
Interned at NIST (Summer 2015) to develop monitoring infrastructure for the RPKI.
Started as a developer at Wayfair.

**Ann Ming Samborski. (B.A/M.A. BU 2017)**
Research on bitcoin, Spring 2016.
Interned on a security team at Cisco (Summer 2016).
Started as a developer at Microsoft.

**Leen Alshenibr. (B.A. BU 2017)**
Research on TumbleBit, Spring-Summer 2016.
Started on a blockchain team at Akamai.

**Haydn Kennedy. (B.A. BU expected 2019)**
Research on cryptography, NTP and network measurement, Summer 2016.

**Rahul Bazaz. (B.A. BU expected 2017)**
Research on network measurement, Summer 2016.

**Omar Sagga. (B.A. BU expected 2019)**
Research on TumbleBit, cryptography, RPKI security, Summer 2016-Present.

**Daniel Gould. (B.A. BU expected 2019)**
Research on TumbleBit, Winter 2017.

**Ezequiel Gomez. (B.A. BU expected 2019)**
Research on TumbleBit, Winter 2017.

**Sean Smith. (B.A./M.A. BU 2017)**
Research on DNS security. Winter 2017.
Started as an developer at Amazon.

### High school research advisees.

**Lydia K. Goldberg.**
Intern Summer 2013 as part of MIT Research Science Institute.
Research on SSL Certificates. Semi-Finalist for Intel Science Talent Search 2014.
Started as an undergraduate at Harvard in Fall 2014.

**Hristo Stoyanov.**
Intern Summer 2014 as part of MIT Research Science Institute.
Research on RPKI robustness. Finalist in the International Science and Engineering Fair 2015.
Started as an undergraduate at Stanford in Fall 2015.

**Yuval Marcus.**
Intern Summer 2016 and Summer 2017. Research on bitcoin and ethereum.

## Doctoral Committees.

**Bhavanna Kanukurthi. (Ph.D., Boston University, 2010.)**
**Phillipa Gill. (Ph.D., University of Toronto, 2012.)**
**Benjamin Fuller. (Ph.D., Boston University, 2014.)**
**Robert Lychev. (Ph.D., Georgia Tech, 2014.)**
**Davide Proserpio. (Ph.D., Boston University, 2016.)**
**Dimitris Papadopoulos. (Ph.D., Boston University, 2016.)**
**Giovanni Comerela (Ph.D., Boston University, 2017.)**
**Cody Douchette (Ph.D. Candidate, Boston University.)**

## Service: Peer review and conference organization

**Technical Program Committee Chair:**
2018: Applied Networking Research Workshop, ANRW'18;

**Technical Program Committees:**
2018: Applied Networking Research Prize TPC, BITCOIN'18;
2017: SIGCOMM'17, HotCloud'17;
2016: IMC'16;
2015: NSDI'15, SIGCOMM'15; 2015 Workshop on Surveillance and Technology (SAT);
2014: IMC'14, SIGCOMM'14, NSDI'14, SIGCOMM'14 poster and demo session;
2013: CoNext'13, NSDI'13 poster and demo session, HotCloud'13, NPSec'13;
2012: IMC'12, HotCloud'12, SysStore'12;
2011: SIGCOMM '11, NetEcon'11, CoNEXT Student Workshop'11;
2010: HotCloud'10, NetEcon'10;
2009: NetEcon'09;

**Workshop co-Organizer & Founder:**
New England Networking and Systems Day 2016; `http://systems.cs.brown.edu/nens/2016/`
New England Networking and Systems Day 2014; `http://systems.cs.brown.edu/nens/2014/`
Boston Freedom in Online Communications Day 2013; `http://www.bu.edu/cs/bfoc/`

**Steering Committee:**
Hebrew University Networking Summer: `http://www.cs.huji.ac.il/event/networking_summer/`
New England Networking and Systems Day: `http://systems.cs.brown.edu/nens/`
New England Security Day: `http://nesd.cs.umass.edu/NESD2015.html`

**Organizing Committee:**
SIGCOMM'16 (Registration chair).
SIGCOMM'12 (Travel grants chair).

**Conference Session Chair:**
2014: PETS'14;
2012: IMC'12, EC'12, HotCloud'12;
2011: SIGCOMM'11;
2010: HotCloud'10;

**Other Conference Organization:**
SIGCOMM'14 Student Poster Competition (Judge);
ICDE'14 Doctoral Symposium (Panelist);
SIGCOMM'10 Student Poster Competition (Judge).

**External Reviewer:**
2015: HotMiddleboxes'15;
2014: HotSDN'14;
2011: INFOCOMM'11;
2010: NSDI '10, EUROCRYPT '10;
2009: NSDI '09, TCC '09, SODA '09, CNCC'09;
2008: CRYPTO'08, CCS'08, ANCS'08, MobiCom'08, CNCC'08;

2007: ANCS'07;
2006: SIGCOMM'06;

**Journal Reviewer:** Journal of Cryptology, SIGCOMM Computer Communications Review, IEEE Transactions on Internet Technology, IEEE Transactions on Networking, IEEE Transactions on Communications, Journal of Computer Networks, Transactions on Internet Technology, IEEE Transactions on Security & Privacy, ACM Transactions on Database Systems, Proceedings of the Very Large Databases Endowment, Journal of Knowledge and Information Systems, IEEE Transactions on Education.

**Proposal Reviewer:** National Science Foundation (2010, 2014, 2015). Israel Science Foundation (2016).

## Service: Internal (Boston University)

**Seminar and colloquia organization.**
2011-2017: Organizer, BUsec weekly seminar in cryptography & security;
2011-2014: Chair, Computer Science Distinguished Colloquium Series;
2010-2011: Organizer, BU Computer Science Student Seminar;
2010-2011: Chair, Computer Science Colloquium Series.

**Departmental Service.**
2014, 2015, 2017: Candidate Host, Faculty Hiring;
2013, 2014: CS Faculty Merit Committee;
2010, 2011: Graduate Admission Committee. (Reviewed $\approx$ 200 applications with a 6-person team.);
2010-Present: Undergraduate advisor;

**Curriculum development.**
2014: Introduced new course: CS591/IR500 Cyber Conflict and Internet Freedom.
2014: Member, CS Introductory Course Sequence Curriculum Committee.

**Invited/Alumni/Fundraising talks.**
10/2016; Invited by Provost Morrison and President Brown to be the faculty speaker at Boston Universitys Fall 2016 Management Conference.
10/2016; Invited by Provost Morrison and President Brown to be the faculty speaker at Boston Universitys Spring 2016 International Advisory Board (IAB) meeting, Seoul, South Korea;
04/2016; CAS Leadership Advisory Board, talk about network security and surveillance.
09/2014; Alumni Association: Panelist for Gitner Lecture: Advancing the Human Condition.
05/2014; Alumni Relations: Panelist for Cybersecurity Panel;

**University Service.**
2014-2016: Member, BU Information Security & Business Continuity Governance Committee.
2015: Member, Information Security Border Protection Project Steering Committee. (Firewall deployment project).

## Service: Women in STEM

**Faculty advisor for Codebreakers: Summer program in cybersecurity.**
Codebreakers is a new 3-week program at Boston University for young women who are currently in their freshmen or sophomore year of high school to study computer and information security. Graduate and undergraduate coordinators will teach participants how to apply basic security concepts through gaming, modeling, and simulation development. Students also learn to program in python, as well as about robotics, digital forensics, cryptography, system vulnerabilities and ethics.
`http://www.bu.edu/lernet/cyber/`

**Presenter at outreach events for female high school students:**
ProjectCSGIRLS Boston Girls in Tech Program Panel (May 2016)
The Artemis Program at Boston University (July 2011-16)
The Summer Pathways Program at Boston University (July 2014-16)
CSSParks Teen Retreat (Dec 2014)
WGBH Boston "Dot Divas" program, (2009-11),
Microsoft Digi-Girlz Days (2011)
WISE@Warren, Boston University (2011).

**Curriculum development with high school teachers:**
Speaker on cybersecurity pedagogy at the 2017 Computer Science Teachers Association (CSTA) New England Regional Conference, (10/2017).
Massachusetts Computer Science Teachers Association (CSTA) meeting, (11/2014).
Curriculum development for AP Computer Science Course at the Advanced Math and Science Academy High School in Marlborough, MA (8/2015).

**Presenter at mentorship events for female graduate and undergraduate students:**
BUWiCS (BU Undergraduate Women in Computer Science) (2013)
GWISE BU (Graduate Women in Science and Engineering) (2013)
N2 Women Lunches at the SIGCOMM conference (2009, 2012, 2013).

**Grace Hopper Celebration of Women in Computing:**
Reviewer, Technical poster session (2014,2015).

**Graduate Women in Science and Engineering, (GWISE), Princeton University**
President (2007-8)
Vice-President (2006-7)
Secretary (2005-6)

**Co-organizer, Princeton/NYU High School Girls Engineering Colloquium** (May 2008)
Day-long colloquium on engineering for 120 girls from nine New York City high schools.
Oversaw program of over 20 speakers and demonstrations by graduate students and faculty.
Oversaw budget and secured funding from Google.
`http://www.princeton.edu/engineering/news/publications/equad-news/s08/articles/grad.xml?id=662`