Michael A. Specter

(412) 535 1510
specter@mit.edu
www.mit.edu/~specter/

Research Interests

I am primarily interested in **systems security, applied cryptography**, and **vulnerability discovery**, with emphasis on work that can have a positive impact on society.

Education

2017–2021 **PhD, Computer Science**, *Massachusetts Institute of Technology*.
Advisors: Gerald Jay Sussman, Daniel J. Weitzner
Thesis Committee: Ron Rivest, Matthew D. Green, Joan Feigenbaum

2013–2015 **MS, Computer Science**, *Massachusetts Institute of Technology*.

MS, Technology & Public Policy, *Massachusetts Institute of Technology*.
Advisors: David D. Clark, Daniel J. Weitzner

2006–2010 **BA, Computer Science**, *The George Washington University*.

BA, International Affairs, *The George Washington University*.

Experience

2023–Present **Georgia Tech**, *Assistant Professor*, Computer Science.
Assistant professor, joint appointment between the School of Computer Science and School of Cybersecurity and Privacy

2021–Present **Google**, *Senior Research Scientist*, Android Security & Privacy.
Research in cryptography, systems security, and applied cryptography for the world's most used OS.

2018–2021 **Google**, *Research Affiliate*, Android Security & Privacy.
Led a research team developing novel static analysis tools to improve Syzkaller, Google's Linux kernel fuzzer.

Summer 2018 **Google**, *Research Intern*, Android Security & Privacy.

Summer 2017 **Apple**, *Security & Privacy Research Intern*, Privacy Team.
Novel research into web tracking. Improvements have been deployed in Safari.

2010 – 2016 **MIT Lincoln Laboratory**, *Research Scientist*, Offensive Security Group.
Research in vulnerability discovery, static analysis, and malware analysis. Tech Lead and research lead for multiple large DARPA-funded projects.

Honors & Awards

Awards

2023 Election Verification Network – **Research Award** [link]

2016 Electronic Frontier Foundation – **EFF Pioneer Award** [link]

2015 Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) – **JD Falk Award** [link]

Grants & Fellowships

2019–2020 Google Android Security and Privacy (ASPRIE) Fellowship

2013–2015 MIT Lincoln Scholars Fellowship

2008–2010 NSF Scholarship for Service – Full Scholarship & Stipend

Selected Publications

Refereed Publications

[1] J. Cable, A. Fábrega, S. Park, and M. A. Specter, "A systematization of voter registration security," *Journal of Cybersecurity*, vol. 9, no. 1, tyad008, Jun. 2023, ISSN: 2057-2085. DOI: 10.1093/cybsec/tyad008. eprint: https://academic.oup.com/cybersecurity/article-pdf/9/1/tyad008/50540756/tyad008.pdf. [Online]. Available: https://doi.org/10.1093/cybsec/tyad008.

[2] S. Park, **M. Specter**, N. Narula, and R. L. Rivest, "Going from bad to worse: from Internet voting to blockchain voting," *Journal of Cybersecurity*, vol. 7, no. 1, Feb. 2021, tyaa025, ISSN: 2057-2085. DOI: 10.1093/cybsec/tyaa025.

[3] **M. A. Specter** and J. A. Halderman, "Security Analysis of the Democracy Live Online Voting System," in *30th USENIX Security Symposium (**USENIX Security 21**)*, 2021.

[4] **M. A. Specter**, S. Park, and M. Green, "KeyForge: Mitigating Email Breaches with Forward-Forgeable Signatures," in *30th USENIX Security Symposium (**USENIX Security 21**)*, 2021.

[5] **M. A. Specter**, J. Koppel, and D. Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections," in *29th USENIX Security Symposium (**USENIX Security 20**)*, 2020,
Acceptance Rate: 16.1%.

[6] L. H. Gilpin, D. Bau, B. Z. Yuan, A. Bajwa, **M. A. Specter**, and L. Kagal, "Explaining Explanations: An Overview of Interpretability of Machine Learning," in *2018 IEEE 5th International Conference on data science and advanced analytics (DSAA)*, IEEE, 2018, pp. 80–89,
Acceptance Rate: 20%.

[7] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, **M. A. Specter**, and D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Oxford Journal of Cybersecurity*, vol. 1, no. 1, pp. 69–79, 2015,
Names alphabetical. Also seen in the **Communications of the ACM** and **Usenix Enigma**.

Tech Reports

[1] K. Thomas, S. Meiklejohn, M. A. Specter, X. Wang, X. Llorà, S. Somogyi, and D. Kleidermacher, *Robust, privacy-preserving, transparent, and auditable on-device blocklisting*, 2023. arXiv: 2304.02810 [cs.CR].

[2] J. Blessing, M. A. Specter, and D. J. Weitzner, *You really shouldn't roll your own crypto: An empirical study of vulnerabilities in cryptographic libraries*, 2021. arXiv: 2107.04940 [cs.CR].

[3] J. Meklenburg, **M. Specter**, M. Wentz, H. Balakrishnan, A. Chandrakasan, J. Cohn, G. Hatke, L. Ivers, R. L. Rivest, G. J. Sussman, and D. Weitzner, *SonicPACT: An Ultrasonic Ranging Method for the Private Automated Contact Tracing (PACT) Protocol*. 2020,
Co-First Author with Wentz & Meklenburg.

[4] R. L. Rivest, J. Callas, R. Canetti, K. Esvelt, D. K. Gillmor, Y. T. Kalai, A. Lysyanskaya, A. Norige, R. Raskar, A. Shamir, I. Shen Emily Soibelman, **M. A. Specter**, V. Teague, A. Trachtenberg, M. Varia, M. Viera, D. Weitzner, J. Wilkinson, and M. Zissman, *The PACT Protocol Specification*. 2020,
Names alphabetical. Specification for MIT's proposed cryptographic privacy-preserving contact tracing protocol.

[5] B. Cyr, W. Horn, D. Miao, and **M. A. Specter**, "Security Analysis of Wearable Fitness Devices (Fitbit)," *Massachusetts Institute of Technology Tech Report*, 2014.

Thesis

[1] **M. A. Specter**, "The Economics of Cryptographic Trust: Understanding Certificate Authorities," Master's thesis, Massachusetts Institute of Technology, 2016.

Policy and Op Eds

[1] J. Cable, S. Frankenberg, P. Lowary, C. Small, **M. A. Specter**, A. Stephan, and A. Zaheer, *Online Voting Wasn't Ready for 2020. Don't Count on It Anytime Soon.* en, Sep. 2020. [Online]. Available: https://lawfareblog.com/online-voting-wasnt-ready-2020-dont-count-it-anytime-soon.

[2] **Michael A. Specter**, *Apple's Cloud Key Vault, Exceptional Access, and False Equivalences*, en, Sep. 2016. [Online]. Available: https://lawfareblog.com/apples-cloud-key-vault-exceptional-access-and-false-equivalences.

[3] Contributor and Amicus to the EFF-led Amicus Brief to the U.S. Supreme Court on the need to reform the Computer Fraud and Abuse Act (CFAA)

Media & Policy Recognition

Elections Security

Jun 10, 2020 Senator Ron Wyden's keynote at DEFCON: *"Earlier this year a team from MIT conducted a thorough audit of Voatz's product and found it riddled with basic flaws...I commend the team from MIT for showing yet again, that internet voting is dangerous"*

Jun 10, 2020 ArsTechnica: *Researchers say online voting tech used in 5 states is fatally flawed*

Jun 7, 2020 The New York Times: *Amid Pandemic and Upheaval, New Cyberthreats to the Presidential Election*

Apr 28, 2020 The Economist: *Why voting online is not the way to hold an election in a pandemic*

Mar 31, 2020 Fortune: *'Security Botox' or 'amazingly successful'? Inside the battle to patch bug bounties' biggest vulnerability*

Mar 13, 2020 Vice: *A Mobile Voting App That's Already in Use Is Filled With Critical Flaws*

Feb 14, 2020 CNN: *Security experts raise concerns about voting app used by military voters*

Vice: *Sloppy Mobile Voting App Used in Four States Has Elementary Security Flaws*

The Verge: *Blockchain voting app is dangerously vulnerable, researchers say*

Feb 13, 2020 The New York Times: *Voting on Your Phone: New Elections App Ignites Security Debate*

May 13, 2020 FiveThirtyEight: *Why A Voting App Won't Solve Our Problems This November*

Encryption & Surveillance

Oct 31, 2019 Congresswoman Anna Eshoo & Senator Ron Wyden: Cited in a letter to U.S. Attorney General Barr

Feb 6, 2017 MIT Technology Review: *The Next Big Encryption Fight*

Dec 14, 2015 Ars Technica: *What the government should've learned about backdoors from the Clipper Chip*

MIT News: *CSAIL report: Giving government special access to data poses major security risks*

TechCrunch: *Top Security Experts Say Government Limits On Encryption Present Risks*

Jul 7, 2015 The New York Times: *Security Experts Oppose Government Access to Encrypted Communication*

Email Deniability

Nov 19, 2020 The Register: *Compsci guru wants 'right to be forgotten' for old email, urges Google and friends to expire, reveal crypto-keys*

Invited Talks

Election Security

Feb 19, 2021 **Georgia Tech, Cybersecurity Lecture Series**.

Oct 12, 2020 **Carnegie Mellon University, Cylab**, *Security and Privacy of U.S. Deployed Internet Voting Systems.*

Sep 18, 2020 **University of Connecticut**, *Why Election Security is Hard.*

Aug 26, 2020 **MIT's Decentralized Currency Initiative**, *Why Election Security is Hard.*

Aug 12, 2020 **USENIX Security 2020**, *The Ballot is Busted Before the Blockchain.*

Aug 8, 2020 **DEFCON 2020**, *The Ballot is Busted Before the Blockchain [video link].*

Jul 23, 2020 **White House Office of Science and Technology Policy, Networking and Information Technology Research and Development Program**, *Open Problems in Elections Security.*

Mar 12, 2020 **U.S. Senate Staff, Homeland Security & Governmental Affairs**, *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz.*

Email Deniability

Apr 16, 2019 **World Wide Web Consortium (W3C)**, *KeyForge: Regaining Cryptographic Deniability for Email.*

Jun 18, 2019 **George Washington University**, *KeyForge: Regaining Cryptographic Deniability for Email.*

Encryption & Surveillance

Jul 20, 2016 **Stanford University's Hoover Institution**, *Panelist for "Encryption Policy: The International Dimension".*

May 17, 2016 **The George Washington University**, *NSF Scholarship for Service Alumni Keynote.*

Jan 20, 2016 **Center for Strategic & International Studies (CSIS)**, *CSIS Encryption Roundtable.*

Mar 30, 2016 **Rightscon**, *Encryption & Lawful Hacking, a Middle Ground?.*

Jun 23, 2015 **Carnegie Mellon University, Technology Management & Policy Conference**, *Understanding the Economics of Web Cryptography [link] .*

Teaching and Mentorship

Fall 2023 **GATECH 8803: Security & Privacy for Democracy**.
A survey course on topics involving security and privacy challenges for democratic institutions, [Syllabus link].

Spring 2021 **MIT 6.885: Critical Perspectives on Security and Privacy Architectures**.
Instructors: Michael A. Specter, Gerry Sussman, Daniel J. Weitzner
Co-created a security and privacy course based on my dissertation, an introduction to security and privacy [Syllabus link]

Fall 2021 **Lab Assistant, MIT 6.857: Computer and Network Security**.
Instructors: Ron Rivest & Yael Kalai

Fall 2017 & 2018 **Teaching Assistant, MIT 6.943: How to Make Almost Anything**.
Responsible for independently teaching and mentoring a recitation section. Focus on introductory embedded systems concepts and programming, and building, well, almost anything.

2018 & 2019 **Instructor, MIT: Introduction to Reverse Engineering** .
Created a two week short course on introductory reverse engineering. Topics include material on decompilers ida pro & Ghidra, x86_64 assembly, basic memory management, and basic vulnerability discovery.

Invited Lectures

March 24, 2021 **MIT EECS 6.808: Mobile and Sensor Computing**.
SonicPACT: Device-to-Device Acoustic Sensing
Instructor: Fadel Abib

Nov 19, 2020 **University of Michigan: EECS 498.5, Election Cybersecurity**.
An introduction to cryptography & election security
Instructor: J. Alex Halderman

Oct 29, 2020 **Stanford INTLPOL 268: Hack Lab**.
An introduction to cryptography & election security
Instructors: Alex Stamos & Riana Pfefferkorn

Apr 26, 2020 **MIT 6.857: Computer and Network Security**.
An introduction to cryptography & election security
Instructors: Ron Rivest & Yael Kalai

Jan, 2012 **Harvard Law School: International Cybersecurity: Public and Private Sector Challenges**.
Introduction to Computer Security
Instructor: Jack Goldsmith

Mentor & Advising

Fall 2018 & 2019 **Staff Mentor, 6.805: Foundations of Internet Policy**.
Worked with project groups studying law and technology issues, lectured, and helped guide student final projects.

2018-2020 **Mentor: Jenny Blessing, Masters Candidate in EECS & Technology Policy MIT**, *Towards Empirical Evaluation of Software Security Risk*, 2020.

2020 **Mentor: Nakul Bajaj, University of Michigan**, *The Security and Privacy of Remote Accessible Vote by Mail Systems*.

Service

Committees

2023 **Usenix Security**, *PC Member*.

2022 **Usenix Security**, *PC Member*.

2022 **IEEE S&P**, *PC Member*.

2021 **IEEE Euro S&P**, *Program Committee member*.

2021 **Usenix Security**, *Artifact Evaluation Committee*.

Member

2019-Present Caltech/MIT Voting Technology Project

2019-Present Election Verification Network (EVN)

Conferences

2019 **Organizer, Invite-only Encryption & Surveillance workshop, co-located with CRYPTO 2019**.

2019 **Organizer, Invite-only Encryption & Surveillance workshop, co-located with Usenix Security 2019**.

Other

2017-2018 **MIT EECS Faculty Hiring Student Reviewer**.
Interviewed and attended faculty candidate talks, provided feedback to the department