COMS E6184 — Anonymity and Privacy (Spring '17)

[redacted]
IA: Daniel Schwartz

"Anonymity and Privacy" will be taught as a seminar class. Students will be expected to read and present a wide variety of papers; these will include technical papers, statutes, court opinions, and the like. Prerequisites include reasonable familiarity with networking and cryptography. Grading will be based on class presentations of these papers — the exact number will depend on the total enrollment — class discussion, and on two papers, one in lieu of the midterm and one in lieu of the final. There will be no exams.

Topics will include:

- Legal framework (US and European)
- Data mining and databases
- Anonymous commerce (digital cash)
- Anonymous use of the Internet (onion routing, anonymous browsing, P3P)
- Traffic analysis
- Biometrics and authentication
- Policy and national security considerations

The reading list is subject to change in response to current events.

Background Reading on Cryptographic Protocols

Those who have no background in cryptographic protocols should read

- Chapters 2-4 of *Applied Cryptography*, Bruce Schneier, Wiley 1996, available in the SEAS library.
- "Using encryption for authentication in large networks of computers", R. Needham and M. Schroeder, *Communications of the ACM* 21:12 (Dec 1978). This is the first cryptographic protocol published in the open literature (available via the CU library network).
- "Timestamps in key distribution protocols", D. Denning and G. Sacco, *Communications of the ACM* 24:8 (Aug 1981). A bug and a fix in the Needham-Schroeder protocol. Note: the fix is buggy, too; see if you can find the problem. There's also *another* bug in Needham-Schroeder that wasn't found until 1995. (available via the CU library network).

Courseworks

Unless there is significant sentiment to the contrary, I will not use Courseworks except for the gradebook and the discussion list. All readings will be posted on this sight.

IA

Daniel Schwartz
Office hours: [redacted]

COMS E6184 — Lectures (Spring '17)

The topics and readings listed here are subject to change, including in response to current events

Tuesday, January 17: Introduction

- Samuel D. Warren and Louis D. Brandeis. The right to privacy. *Harvard Law Review*, 4(5), December 1890. [http]
- David Brin. The transparent society. *Wired*, 4(12), December 1996. [.html]
- Jerry Kang. Cyberspace privacy: A primer and proposal. *Human Rights Magazine*, 26(1), Winter 1999. [http]
- Stephen T. Kent and Lynette I. Millett, editors. *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, 2003. (Chapter 3). [.html]
- Dr. Fun

Tuesday, January 24: Legal Foundations of Privacy

- Whitfield Diffie and Susan Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption*. MIT Press, Cambridge, MA, second edition, 2007. Chapter 7. [http]
- Stefan Kulk and Frederik Zuiderveen Borgesius. Freedom of expression and `right to be forgotten' cases in the Netherlands after Google Spain. *European Data Protection Law Review (EDPL)*, 1(2):113--124, 2015. [http]
- Katz v U.S. 389 US 347 (1967)
  Smith v Maryland 442 US 735 (1979)
  18 USC 2510-2522, 2701-2712: wiretap law; Stored Communications Act (recommended)
  18 USC 3121-3127: pen registers and trap-and-trace devices (recommended)
  50 USC 1801-1811: Foreign Intelligence Surveillance Act (recommended)
- Chapter II of the EU Privacy Directive (*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*) (You may find this page helpful, but it's not required reading.)

Tuesday, January 31: Wiretapping

- Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze. Signaling vulnerabilities in wiretapping systems. *IEEE Security and Privacy*, November/December 2005. [.pdf]
- Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vint Cerf, Whitfield Diffie, Susan Landau, Jon Peterson, and John Treichler. Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP, 2006. [.pdf]
- Vassilis Prevelakis and Diomidis Spinellis. The Athens affair. *IEEE Spectrum*, 44(7):26--33, July 2007. [http]

- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Going bright: Wiretapping without weakening communications infrastructure. *IEEE Security & Privacy*, 11(1):62--72, January--February 2013. [DOI | .pdf]
- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Northwestern Journal of Technology & Intellectual Property*, 12(1), 2014. (Optional--and long--follow-on to "Going Bright"). [http]

Tuesday, February 07: Crime and National Security

- Privacy and Civil Liberties Oversight Board. Report on the telephone records program conducted under Section 215 of the USA PATRIOT Act and on the operations of the Foreign Intelligence Surveillance Court, January 23, 2014. Parts 1-3 only. [.pdf]
- Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, Matthew Green, Peter G. Neumann, Susan Landau, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 2015. [http]
- Report of the Manhattan District Attorney's Office on smartphone encryption and public safety, November 2015. [.pdf]
- Joanna Dawson. Investigatory powers bill. Briefing paper, March 11, 2016. Sections 1-5, but ignore the "pre-legislative scrutiny portions". [http]

Tuesday, February 14: Web Privacy

- Joseph Reagle and Lorrie Faith Cranor. The platform for privacy preferences. *Commun. ACM*, 42(2):48--55, February 1999. [DOI | http]
- D. Kristol and L. Montulli. HTTP State Management Mechanism. RFC 2965, October 2000. [.txt]
- Simon Byers, Lorrie Faith Cranor, Dave Kormann, and Patrick McDaniel. Searching for privacy: Design and implementation of a P3P-enabled search engine. In *International Workshop on Privacy Enhancing Technologies*, pages 314--328. Springer, 2004. [.pdf]
- Peter Eckersley. How unique is your web browser? In *International Symposium on Privacy Enhancing Technologies Symposium (PETS)*, pages 1--18. Springer, 2010. [.pdf]

Midterm paper topic approval deadline

Tuesday, February 21: Social Networks

- Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 71--80, New York, NY, USA, 2005. ACM. [DOI | http]
- Balachander Krishnamurthy and Craig E Wills. Privacy leakage in mobile online social networks. In *Proceedings of the 3rd Conference on Online Social Networks*, pages 4--4. USENIX Association, 2010. [.pdf]
- Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. A study of privacy setting errors in an online social network. In *Proceedings of SESOC 2012*, 2012. [.pdf]
- Guanxiong Huang and Kang Li. The effect of anonymity on conformity to group norms in online contexts: A meta-analysis. *International Journal of Communication*, 10(0), 2016. [http]

Tuesday, February 28: Database Nation; Link Analysis

- Simson Garfinkel. *Database Nation*. O'Reilly and Associates, 2000. Read Chapter 4. The link to the book is via the Columbia library network; full text is available. However... they seem to limit the number of simultanous readers; do not wait until the night before. (In fact, you may wish to read more; it's a fast read. Chapter 9 is prescient and scary --- and it was written before the terrorist attacks of 9/11.). [http]
- C. Cortes, D. Pregibon, and C. Volinsky. Communities of interest. In *Proceedings of IDA 2001---Intelligent Data Analysis*, 2001. [http]
- Hady Wirawan Lauw, Ee Peng Lim, Tek Tim Tan, and Hwee Hwa Pang. Mining social network from spatio-temporal events. In *Workshop on Link Analysis, Counterterrorism and Security*, pages 82--93, April 2005. [http]
- Kathleen Benitez and Bradley Malin. Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association*, 17(2):169--177, 2010. [http]

Tuesday, March 07: Privacy and Data Mining

- Rakesh Agrawal and Ramakrishnan Srikant. Privacy-preserving data mining. *SIGMOD Rec.*, 29(2):439--450, May 2000. [DOI | http]
- Latanya Sweeney. *k*-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557--570, October 2002. [.pdf]
- Cynthia Dwork. Differential privacy. *ICALP 2006*, 4052:1--12, 2006. [DOI | http]

Tuesday, March 21: Anonymous Connectivity

- David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84--90, 1981. [DOI]

- G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: design of a type III anonymous remailer protocol. In *2003 Symposium on Security and Privacy, 2003.*, pages 2--15, May 2003. [DOI]
- Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004. [http]

Midterm papers due

Tuesday, March 28: Traffic Analysis

- Nick Mathewson and Roger Dingledine. Practical traffic analysis: Extending and resisting statistical disclosure. In *International Workshop on Privacy Enhancing Technologies*, pages 17--34. Springer, 2004. [.pdf]
- S. J. Murdoch and G. Danezis. Low-cost traffic analysis of Tor. In *2005 IEEE Symposium on Security and Privacy (S P'05)*, pages 183--195, May 2005. [DOI]
- Charles V Wright, Lucas Ballard, Fabian Monrose, and Gerald M Masson. Language identification of encrypted VoIP traffic: Alejandra y Roberto or Alice and Bob? In *USENIX Security*, volume 3, page 3, 2007. [http]

Final paper topic approval deadline

Tuesday, April 04: Side Channels

- Dawn Xiaodong Song, David Wagner, and Xuqing Tian. Timing analysis of keystrokes and timing attacks on ssh. In *USENIX Security Symposium*, volume 2001, 2001. [.pdf]
- Steven M. Bellovin. A technique for counting NATted hosts. In *Proc. Second Internet Measurement Workshop*, pages 267--272, Marseille, 2002. [.pdf]
- T. Kohno, A. Broido, and K. C. Claffy. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 2(2):93--108, April 2005. [DOI]
- D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. *IEEE Security & Privacy*, 8(6):40--47, Nov 2010. [DOI]

Tuesday, April 11: Digital Cash

- D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Proceedings on Advances in Cryptology*, CRYPTO '88, pages 319--327, New York, NY, USA, 1990. Springer-Verlag New York, Inc. [http]

- Markus Jakobsson and Moti Yung. Revokable and versatile electronic money (extended abstract). In *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, CCS '96, pages 76--87, New York, NY, USA, 1996. ACM. [DOI | http]
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. Note: this class is about privacy and anonymity, not economics; the economic arguments for or against the suitability of Bitcoin as a currency aren't particularly relevant. [.pdf]
- Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459--474. IEEE, 2014. [http]

Tuesday, April 18: Internet of Things

- Jan Henrik Ziegeldorf, Oscar García Morchon, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12):2728--2742, 2014. [http]
- Scott R Peppet. Regulating the Internet of Things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93, 2014. Pages 118-132. [.pdf]
- Xavier Caron, Rachelle Bosua, Sean B Maynard, and Atif Ahmad. The internet of things (iot) and its impact on individual privacy: An australian perspective. *Computer Law & Security Review*, 32(1):4--15, 2016. [http]
- Martin Henze, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, Bernhard Rumpe, and Klaus Wehrle. A comprehensive approach to privacy in the cloud-based internet of things. *Future Generation Computer Systems*, 56:701--718, 2016. [http]

Tuesday, April 25: Location Privacy

- Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, MobiSys '03, pages 31--42, New York, NY, USA, 2003. ACM. [DOI | http]
- Gerald Friedland and Robin Sommer. Cybercasing the joint: On the privacy implications of geo-tagging. In *HotSec*, 2010. [.pdf]
- Julien Freudiger, Raoul Neu, and Jean-Pierre Hubaux. Private sharing of user location over online social networks. In *HotPETs*, number EPFL-CONF-152141, 2010. [http]
- Yong Wang, Daniel Burgener, Marcel Flores, Aleksandar Kuzmanovic, and Cheng Huang. Towards street-level client-independent IP geolocation. In *NSDI*, volume 11, 2011. [.pdf]

Tuesday, May 09: Final Presentations: 6:00-10:00, in the CS Conference Room

COMS E6184 — Papers (Spring '17)

Anonymity and Privacy — Papers

The midterm papers should be 5-10 pages; the final paper should be 10-15. Papers are expected to conform to the usual academic standards. Apart from the obvious — no cheating; your work should be entirely your own — I expect a proper bibliography. Make sure you indicate, via proper appropriate bibliographic pointers, what material you've taken from other works.

The midterm paper is due by the start of class on Tuesday, March 21. The final paper is due by 7:00 pm, on the day of the final exam schedule posted by the registrar. NO EXCEPTIONS.

On the day scheduled for the final, there will be in-class presentations of the final paper. Each student will have about 10 minutes. There will likely be an alternate presentation day for those interested in attending.

To avoid the hassle of switching laptops, please make sure your presentation is accessible from Internet. For this presentation, you probably do want to have slides.

Updated Tuesday, 17-Jan-2017 17:11:14 EST