Course Schedule

Spring 2018

This schedule is subject to change. Please check back frequently.

Week	Date	Topic	Readings
Week 1	Mar 27	**Intro; Security & Crypto Crash Course I**	
	Mar 29	**Accountability & Transparency I**	Assigned: CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds. Nikitin, Kokoris-Kogias, Jovanovic, Gasser, Gailly, Khoffi, Cappos, Ford. USENIX Security. 2017.
Week 2	Apr 3	**Accountability & Transparency II; Security & Crypto Crash Course II**	Assigned: Accountable Virtual Machines. Haeberlen, Aditya, Rodrigues, Druschel. OSDI. 2010. Recommended: • PeerReview: Practical Accountability for Distributed Systems. Haeberlen, Kouznetsov, Druschel. SOSP. 2007. • Efficient Data Structures for Tamper-Evident Logging. Crosby, Wallach. Usenix Security. 2009. • Verena: End-to-End Integrity Protection for Web Applications. Karapanos, Filios, Popa, Capkun, Berkeley. Oakland. 2016.
	Apr 5	**Accountability & Transparency III**	Assigned: The Efficient Server Audit Problem, Deduplicated Re-execution, and the Web. Tan, Yu, Leners, Walfish. SOSP. 2017.
Week 3	Apr 10	**Certificates & Keys**	Assigned: • **[Present]** CONIKS: Bringing Key Transparency to End Users. Melara, Blankstein, Bonneau, Felten, Freedman. Usenix Security. 2015. • Certificate Transparency with Privacy. Eskandarian, Messeri, Bonneau, Boneh. PETS. 2017. Recommended: • SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. Clark, Van Oorschot. Oakland. 2013. • Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning. Syta, Tamas, Visher, Wolinsky, Gasser, Gailly, Ford. Oakland. 2016. • Tracking Certificate Misissuance in the Wild. Kumar, Wang, Hyder, Dickinson, Beck, Adrian, Mason, Durumeric, Halderman, Bailey. Oakland. 2018.
	Apr 12	**TLS and HTTPS**	Assigned: TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation. Ritzdorf, Wüst, Gervais, Felley, Čapkun. NDSS. 2018.
Week 4	Apr 17	**Anonymity I**	Assigned: • **[Present]** Atom: Horizontally Scaling Strong Anonymity. Kwon, Corrigan-Gibbs, Devadas, Ford. SOSP. 2017. • Tor: The second-generation onion router. Dingledine, Mathewson, Syverson. Usenix Security. 2004.
	Apr 19	**Anonymity II**	Assigned: Stadium: A Distributed Metadata-Private Messaging System. Tyagi, Gilad, Zaharia, Zeldovich. SOSP. 2017.
Week 5	Apr 24	No class.	
	Apr 26	**Oblivious Storage**	Assigned: ObliviSync: Practical Oblivious File Backup and Synchronization. Aviv, Choi, Mayberry, Roche. NDSS. 2017.
Week 6	May 1	**Trusted Execution Environments**	Assigned: • Shielding applications from an untrusted cloud with haven. Baumann, Peinado, Hunt. SOSP. 2014. • **[Present]** Opaque: An Oblivious and Encrypted Distributed Analytics Platform. Zheng, Dave, Beekman, Popa, Gonzalez, Stoica. NSDI. 2017. Recommended: • Intel SGX Explained. Costan, Devadas. 2015. • OpenSGX: An Open Platform for SGX Research. Jain, Desai, Kim, Shih, Lee, Choi, Shin, Kim, Kang, Han. NDSS. 2016.
	May 3	**Side Channels I**	Assigned: CLKSCREW: Exposing the perils of security-oblivious energy management. Tang, Sethumadhavan, Stolfo. Usenix Security. 2017.
Week 7	May 8	**Side Channels II**	Assigned: • Meltdown. Lipp, Schwarz, Gruss, Prescher, Haas, Mangard, Kocher, Genkin, Yarom, Hamburg. ArXiv e-prints. 2018. • **[Present]** Spectre Attacks: Exploiting Speculative Execution. Kocher, Genkin, Gruss, Haas, Hamburg, Lipp, Mangard, Prescher, Schwarz, Yarom. ArXiv e-prints. 2018.
	May 10	**Side Channels III**	Assigned: SgxPectre Attacks: Leaking Enclave Secrets via Speculative Execution. Chen, Chen, Xiao, Zhang, Lin, Lai. CoRR. 2018.
Week 8	May 15	**Cryptocurrencies: Intro.**	Assigned: • **[Present]** SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Bonneau, Miller, Clark, Narayanan, Kroll, Felten, Foundation. Oakland. 2015. • **[Present]** Bitcoin's Academic Pedigree. Narayanan, Clark. Communications of the Acm. 2017. Recommended: • Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto. 2008. • Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 1-5,7-8.**
	May 17	**Cryptocurrencies: Buying Physical Goods**	Assigned: Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin. Goldfeder, Bonneau, Gennaro, Narayanan. Financial Cryptography and Data Security. 2017.
Week 9	May 22	**Verifiable Computation**	Assigned: • Verifying computations without reexecuting them: from theoretical possibility to near practicality. Walfish, Blumberg. ECCC. 2013. • **[Present]** Pinocchio: Nearly practical verifiable computation. Parno, Howell, Gentry, Raykova. Oakland. 2013. Recommended: • Verifying computations with state. Braun, Feldman, Ren, Setty, Blumberg, Walfish. SOSP. 2013. • Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Ben-sasson, Chiesa, Tromer. Usenix Security. 2014. • Geppetto: Versatile Verifiable Computation. Costello, Fournet, Howell, Kohlweiss, Kreuter, Naehrig, Parno, Zahur. Oakland. 2015.
	May 24	**Cryptocurrencies: Anonymity**	Assigned: • **[Present]** Zerocash: Decentralized Anonymous Payments from Bitcoin. Ben-sasson, Chiesa, Garman, Green, Miers, Tromer. Oakland. 2014. • **[Present]** TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. Heilman, Alshenibr, Baldimtsi, Scafuro, Goldberg. NDSS. 2017. Recommended: Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 6.**
Week 10	May 29	**Cryptocurrencies: Smart Contracts**	Assigned: Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Kosba, Miller, Shi, Wen, Papamanthou. Oakland. 2016. Recommended: • Ethereum: a secure decentralised generalised transaction ledger. Wood. Ethereum Project. 2014. • Town Crier: An Authenticated Data Feed for Smart Contracts. Zhang, Cecchetti, Croman, Juels, Shi. CCS. 2016. • Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 10-11.**
	May 31	**Cryptocurrencies as a Platform**	Assigned: Blockstack: A Global Naming and Storage System Secured by Blockchains. Ali, Nelson, Shea, Freedman. USENIX ATC. 2016. Recommended: • Catena: Efficient Non-equivocation via Bitcoin. Tomescu, Devadas. Oakland. 2017. • Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 9.**