# cse 543 - course calendar



Below is the calendar for this semester course. This is the preliminary schedule, which will be altered as the semester progresses. It is the *responsibility of the students* to frequently check this web-page for schedule, readings, and assignment changes. As the professor, I will attempt to announce any change to the class, but this web-page should be viewed as authoritative. If you have any questions, please contact me (contact information is available at the course homepage).

| Date | Topic | Assignments Due | Readings for Discussion (do readings **before** class) |
|---|---|---|---|
| 08/22/17 | Introduction (Slides) | | Course syllabus. link<br>Hacked vs. Hackers: Game On - NYTimes.com.pdf link<br>Text: Chapter 1 link |
| 08/24/17 | Authentication (Slides) | Project One: Password Management System (Due: 9/20/2017, 11:59pm)link | Reflections on Trusting Trust. K. Thompson, Turing Award Lecture, 1983. link<br>Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. P. G. Kelley et al. , IEEE Symposium on Security and Privacy, 2012. link<br>Text: Chapter 7.1-7.5 link |
| 08/29/17 | Passwords (Slides) | Review for "Guess Again" paper | Pitfalls in the automated strengthening of passwords. D. Schmidt and T. Jaeger, Annual Computer Security Applications Conference, 2013. link |
| 08/31/17 | Cryptography (Slides) | | Text: Chapter 2 link |
| 09/05/17 | Cryptography (Slides) | | Why Cryptosystems Fail. R. Anderson, 1st ACM Conference on Computer and Communications Security, 1993. link<br>Chapter 3link |
| 09/07/17 | Public Key Cryptosystems (Slides) | Review for "RSA" paper | A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM, 21(2):120-126, 1978. link<br>Text: Chapter 4 link |
| 09/12/17 | Crypto Protocols (Slides) | | Using Encryption for Authentication in Large Networks of Computers. R. Needham and M. Schroeder, CACM, December 1978. link<br>Text: Chapter 5 link |
| 09/14/17 | Authentication Protocols (Slides) | Review for "Kerberos" paper | Kerberos: An Authentication Service for Computer Networks. B. Clifford Neuman and Theodore Ts'o, IEEE Communications, 32(9):33-38. September 1994. link<br>Text: Sections 10.5 link |
| 09/19/17 | Malware (Slides) | | W32.Stuxnet Dossier. Nicolas Falliere, Liam O Murchu, and Eric Chien. 2011. link<br>Text: Section 11.3 link |
| 09/21/17 | Program Vulnerabilities (Slides) | Review for "Stackguard" paper | Buffer Overflow Tutorial link<br>Text: Sections 11.1-11.2 link<br>Stackguard: Automatic Adaptive Detection and Prevention of Buffer Overflow Attacks. C. Crispin, et al. , 7th USENIX Security Symposium, 1998. link |
| 09/26/17 | Return-Oriented Programming (Slides) | | Return-Oriented Programming: Systems, Languages, and Applications. R. Roemer, E. Buchanan, H. Shacham, and S. Savage, ACM Trans. Info. Sys. Security 15(1):2, March 2012. link |
| 09/28/17 | Access Control (Slides) | | Text: Sections 8.1-8.3 link |
| 10/03/17 | Mandatory Access Control (Slides) | Review for "Lattice Model" paper | A lattice model of secure information flow. D. Denning, CACM, May 1976. link |
| 10/05/17 | Mandatory Access Control (Slides) | | Chapter 2. Access Control Fundamentals. T. Jaeger, in Operating Systems Security, 2008. link<br>Text: Sections 8.4-8.5 link |
| 10/10/17 | Operating Systems Security (Slides) | | Linux Security Modules: General Security Support for the Linux Kernel. C. Wright et al. , Proceedings of the 11th USENIX Security Symposium, August 2002. link<br>Text: Section 13.1-13.3 link |

| | | | |
|---|---|---|---|
| 10/12/17 | Network Security Vulnerabilities (Slides) | Review for "Kaminsky" paper | An Illustrated Guide to the Kaminsky DNS Vulnerability , S. Freidl. link<br>Text: Sections 9.1-9.4 link |
| 10/17/17 | Network Security Protocols (Slides) | | SSH - Secure Login Connections Over the Internet. T. Ylonen. USENIX Security 1996. link<br>Text: Sections 10.1-10.2 link |
| 10/19/17 | Firewalls (Slides) | Review for "FIREMAN" paper | The Beginner's Guide to iptables: Linux Firewall , How-To Geek. link<br>FIREMAN: a toolkit for FIREwall Modeling and ANalysis. L. Yuan et al. IEEE Security and Privacy 2006. link<br>Text: Section 8.9 link |
| 10/24/17 | Mid-term Exam (in class) | | |
| 10/26/17 | Web Security (Slides) | Review for "Browser Handbook" Chapter | Browser Security Handbook, Part 2 (Same origin policy, Life Outside Same-origin rules, Third-party cookie rules). link<br>Text: Sections 7.1 and 7.2 link |
| 10/31/17 | Web Security (Slides) | | Secure Web Browsing with the OP Web Browser. C. Grier, S. Tang, S. T. King, Proceedings of the IEEE Symposium on Security and Privacy, 2008. link |
| 11/02/17 | Intrusion Detection (Slides) | | A Sense of Self for UNIX Processes. S. Forrest, S. A. Hofmeyr, A. Somayaji, T. A. Longstaff, In Proceedings of the IEEE Symposium on Security and Privacy, 1996. link<br>The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. S. Axelsson, In Proceedings of the ACM Conference on Computer and Communication Security. November, 1999. link<br>Text: Section 6.4 link |
| 11/07/17 | Privacy (Slides) | Review for "Anonymous Routing" paper | Proxies for Anonymous Routing. M. Reed, P. Syverson, D. Goldschlag. 12th Anual Computer Security Applications Conference, 1996. link<br>The Tor Project link<br>Text: Section 10.5 link |
| 11/09/17 | Blockchains (Slides) | | The Blockchain: A Gentle Four Page Introduction. . Jan Hendrik Witte, ArXiv.org, Dec. 2016. link |
| 11/14/17 | Adversarial Machine Learning (Slides) | Review for "AdversariaL ML" paper | Machine Learning in Adversarial Settings. Patrick McDaniel, Nicolas Papernot, and Berkay Celik. IEEE Security and Privacy Magazine, 14(3), May/June, 2016. link |
| 11/16/17 | Hardware for Security (Slides) | | Design and Implementation of a TCG-based Integrity Measurement Architecture. Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn. In USENIX Security Symposium, Aug. 2004. link |
| 11/21/17 | **Thanksgiving Break - No class** | | |
| 11/23/17 | **Thanksgiving Break - No class** | | |
| 11/28/17 | Virtualization Security (Slides) | Review for "Virtualization" paper | What Virtualization Can Do for Security. T. Garfinkel and A. Warfield. ;login 32(6) 2007. link |
| 11/30/17 | Cloud Computing Security (Slides) | | AmazonIA: When Elasticity Snaps Back. S. Bugiel, T. Poppelmann, S. Nurnberger, A-R. Sadeghi, and T. Schneider, 18th ACM Conference on Computer and Communications Security, 2011. link |
| 12/05/17 | Android Security (Slides) | | AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings. Giuseppe Petracca, Ahmad-Atamli Reineh, Yuqiong Sun, Jens Grossklags, and Trent Jaeger. In 26th USENIX Security Symposium (USENIX Security), Aug. 2017. link |
| 12/07/17 | Future of Secure Programming (Slides) | | Leveraging 'Choice' in Authorization Hook Placement. Divya Muthukumaran, Trent Jaeger, and Vinod Ganapathy. In 19th ACM Conference on Computer and Communications Security, 2012. link |
| 12/10/17 | **Final Exam, TBD** | | |