CSCI 3907/6907.81
ADVANCED SECURITY SEMINAR

Course Schedule

Science of Security

Assignments: Reviews, Presentations, Project

Date	Event
01/18/12	Topic: Introduction to Science of Security Presenter: Clarkson Required reading: • none Suggested reading: • JASON. Science of Cyber-Security. Technical report JSR-10-102, Nov.2010. Sections 4 and 5 can be skimmed or skipped.
01/23/12	Topic: Fundamentals of Computer Security Presenter: Clarkson Required reading: • Fred B. Schneider. Chapter 1 of an untitled in-progress textbook, 2007. Even though this is required, you do not need to write a review of it. Suggested reading: • none
01/25/12	Class cancelled
01/30/12	Topic: Fundamentals of Access Control Presenter: Clarkson

	Required reading: • Pierangela Samarati and Sabrina De Capitani di Vimercati. Access Control: Policies, Models, and Mechanisms. In Foundations of Security Analysis and Design: Tutorial Lectures, Lecture Notes in Computer Science, vol. 2171, pp. 137–193, 2001. Even though this is required, you do not need to write a review of it. Skip the HRU formalization (pp. 5–7), because we'll discuss it in detail on 02/06/12. Also skip section 4.5, and all of sections 6 and 8. Suggested reading: • The parts you skipped in the required reading.
02/01/12	Topic: Fundamentals of Information Flow Presenter: Clarkson Required reading: • Andrei Sabelfeld and Andrew C. Myers. Language-Based Information-Flow Security. IEEE Journal on Selected Areas in Communications, 21(1):5–19, 2003. Even though this is required, you do not need to write a review of it. Skim sections 5 and 6. This is an example of a survey paper, which you need to write for your project. But it's much longer than what you'll write. Suggested reading: • The parts you skipped in the required reading.
02/06/12	Project proposal due Topic: Security Policies and Enforcement Mechanisms Presenter: Roberts Required reading:

	• Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in Operating Systems. Communications of the ACM 19(8):461–470, 1976. Suggested reading: • none
02/08/12	Topic: Security Policies and Enforcement Mechanisms Presenter: Kang Required reading: • Anita K. Jones and Richard J. Lipton. The Enforcement of Security Policies for Computation. In Proceedings of ACM Symposium on Operating Systems Principles, pp. 197–206, 1975. Suggested reading: • J.S. Fenton. Memoryless Subsystems. The Computer Journal, 17(2):143–147, 1974. • Anita K. Jones and Richard J. Lipton. A Linear Time Algorithm for Deciding Security. In Proceedings of IEEE Symposium on Foundations of Computer Science, pp. 33–41, 1976.
02/13/12	Topic: Security Policies and Enforcement Mechanisms Presenter: Kaczmarek Required reading: • Fred B. Schneider. Enforceable Security Policies. ACM Transactions on Information and System Security 3(1):30–50, 2000. Suggested reading: • Kevin W. Hamlen, Greg Morrisett, and Fred B. Schneider. Computability Classes for Enforcement Mechanisms. ACM Transactions on Programming Languages and Systems,

	28(1):175–205, 2006.
02/15/12	Topic: Security Policies and Enforcement Mechanisms Presenter: Clarkson Required reading: • Michael R. Clarkson and Fred B. Schneider. Hyperproperties. In Proceedings of IEEE Computer Security Foundations Symposium, pp. 51–65, 2008. Suggested reading: • Bowen Alpern and Fred B. Schneider. Defining Liveness. Information Processing Letters, 21(4):181–185, 1985.
02/20/12	Presidents' Day
02/22/12	Class cancelled
02/23/12	Project survey paper due
02/27/12	Project review meetings (individual)
02/29/12	Project review meetings (individual)
03/05/12	Topic: Security Policies and Enforcement Mechanisms Presenter: Hirsch Required reading: • George C. Necula. Proof-Carrying Code. In ACM Symposium on Principles of Programming Languages, pp. 106–119, 1997. • George C. Necula and Peter Lee. Safe Kernel Extensions Without Run-Time Checking. In Proceedings of USENIX Symposium on Operating Systems Design and Implementation, pp. 229–243, 1996. Suggested reading: • None.
03/07/12	Topic: Security Policies and Enforcement Mechanisms Presenter: Zhang Required reading:

	• Riccardo Pucella and Fred B. Schneider. Independence from Obfuscation: A Semantic Framework for Diversity. In Proceedings of IEEE Computer Security Foundations Workshop, pp. 230–241, 2006. Suggested reading: • Hovav Shacham, Matthew Page, Ben Pfaff, Eu-Jin Goh, Nagendra Modadugu, and Dan Boneh. On the Effectiveness of Address-space Randomization. In Proceedings of ACM Conference on Computer and Communications Security, pp. 298–307, 2004. • Nora Sovarel, David Evans, and Nathanael Paul. Where's the FEEB? The Effectiveness of Instruction Set Randomization. In Proceedings of USENIX Security Symposium, pp. 145–160, 2005.
03/12/12	Spring break
03/14/12	Spring break
03/19/12	Topic: Security Metrics Presenter: Roberts Required reading: • Sal Stolfo, Steven M. Bellovin, and David Evans. Measuring Security. IEEE Security & Privacy 9(3):60–65, 2011. • Daniel Geer, Jr., Kevin Soo Hoo, and Andrew Jaquith. Information Security: Why the Future Belongs to the Quants. IEEE Security & Privacy 1(4):24–32, 2003. • Steven M. Bellovin. On the Brittleness of Software and the Infeasibility of Security Metrics. IEEE Security & Privacy 4(4):96, 2006. Suggested reading: • None.
03/21/12	Topic: Security Metrics

	Presenter: Kaczmarek Required reading: • Kevin J. Soo Hoo. How Much Is Enough? A Risk-Management Approach to Computer Security. Working paper, Consortium for Research on Information Security and Policy, Stanford University, 2000. Suggested reading: • TBA
03/26/12	Topic: Security Metrics Presenter: Kang Required reading: • Solomon W. Golomb, Robert E. Peile, and Robert A. Scholtz. Basic Concepts in Information Theory and Coding: The Adventures of Secret Agent 00111. New York, Plenum Press, 1994. Pages 1–21. Even though this is required, you do not need to write a review of it. • Geoffrey Smith. On the Foundations of Quantitative Information Flow. In Proceedings International Conference on Foundations of Software Science and Computation Structures, pp. 288–302, 2009. Suggested reading: • William E. Burr, Donna F. Dodson, and W. Timothy Polk. Electronic Authentication Guideline, Appendix A. NIST Special Publication 800-63, April 2006.
03/28/12	Topic: Security Metrics Presenter: Clarkson Required reading: • Michael R. Clarkson and Fred B. Schneider. Quantification of Integrity. In Proceedings IEEE Computer Security

	Foundations Symposium, pp. 28–43, 2010. Suggested reading: None.
04/02/12	Class cancelled (work on project)
04/04/12	**Project midterm draft paper due** Class cancelled (work on project)
04/09/12	**Project peer reviews due** Project review meetings (individual)
04/11/12	**Project review meetings (individual)**
04/16/12	**Class cancelled (work on project)**
04/18/12	Topic: Provable Security Presenter: Zhang Required reading: • Anupam Datta, Jason Franklin, Deepak Garg, Limin Jia, and Dilsun Kaynar. On Adversary Models and Compositional Security. IEEE Security & Privacy, 9(3):26–32, 2011. Suggested reading: • Anupam Datta, Jason Franklin, Deepak Garg, and Dilsun Kaynar. A Logic of Secure Systems and its Application to Trusted Computing. In Proceedings IEEE Symposium on Security and Privacy, 221–236, 2009.
04/23/12	Topic: Provable Security Presenter: Hirsch Required reading: • Jean Paul Degabriele, Kenneth G. Paterson, and Gaven Watson. Provable Security in the Real World. IEEE Security & Privacy, 9(3):33–41, 2011. • Richard A. De Millo, Richard J. Lipton, and Alan J. Perlis.

	Social Processes and Proofs of Theorems and Programs. Communications of the ACM, 22(5):271–280, May 1979. Suggested reading: • Various authors. Comments on Social Processes and Proofs. Communications of the ACM, 22(11):621–630, November 1979. • A thread on Lambda the Ultimate about social processes and proofs.
04/25/12	Topic: The Science of Security Presenter: Clarkson Required reading: • Fred B. Schneider. Blueprint for a Science of Cybersecurity. Cornell Computing and Information Science Technical Report, http://hdl.handle.net/1813/22943, 2011.
04/30/12	Final project presentations
05/01/12	Make-up Day (no class)
05/02/12	Final project presentations (Designated Monday)
05/04/12	Project poster session. Marvin Center, room TBA, 4–6 pm.
05/09/12	roject final paper due