Advanced Topics in Computer Security (3-1)
Huffmire, Ted
07/09/2014

Course Description:
This course applies graduate-level knowledge and reasoning skills in written essays and verbal discussion of current topics in computer security. Students read academic papers regarding information assurance topics, and discuss issues that they derive from the readings. This pedagogical approach is constructivist in encouraging the students to develop their own viewpoints and conclusions. Prerequisites: CS3600 and CS4600 and CS4605, or consent of the instructor.

Course Format:
In general, each week the first class session will be for discussion of the assigned readings relative to a common computer security topic, and the second two will be for discussion of related papers you find. This reading and discussion seminar format requires grounding in information assurance fundamentals. It is assumed that you are familiar with current best practices for administration and configuration of commercial products for the day-to-day processing of information. Particular emphasis is placed on research regarding the protection of *high value data*, the foundations of high assurance policy enforcement, and the uses of multilevel security. You must have graduate level abilities to research, organize and evaluate technical problems, and to participate in related discussions (e.g., speaking, explaining, querying, and *active listening*).

Course Goal Statement:
The goal of this reading and discussion seminar is to explore current topics in computer security by reading, discussing, and writing about research papers on the protection of high value data, the foundations of high assurance policy enforcement, and the uses of multilevel security.

Learning Objectives:
- Think critically and form conclusions about security techniques
- Survey the literature in this field successfully and judge the quality of search tools
- Defend an argument convincingly and develop academic writing and speaking styles
- Revisit foundational papers and discover new ones
- Avoid common pitfalls in thinking about computer security
- Dissect a paper through purposeful, active, and systematic reading
- Categorize scientific methodologies into taxonomies and understand trade-offs
- Discover relationships between papers and judge the quality of references
- Connect research papers to one's current projects and theses as well as past experience
- Identify the fundamental engineering concepts employed in a paper

A weekly schedule is on the next page.

Topics

Week	Topic	Subtopics/Readings/Labs
1	Course Introduction	Introduction to the course and expectations Discuss tools and strategies for a successful literature search Explain LaTeX citations
2	Banking	Ancient Crypto [Singh 2000, Chapter 1] Chip & Pin [Murdoch 2010]
3	Quantum Primer	Quantum Leap [Singh 2000, Chapter 8] Survey with Timeline [Bacon 2007]
4	Quantum Computing	Limitations [Aaronson 2008] Quantum Algorithms [Bacon 2010]
5	Quantum Key Distribution	Quantum Money [Aaronson 2012] Quantum Networks [Elliott 2003]
6	Malicious Hardware	Malicious Inclusions [Karri 2010] Backdoors [Skorobogatov 2012]
7	Hardware-Oriented Security and Trust	Flash Memory [Wang 2012] PUFs [Katzenbeisser 2012]
8	Cyber-Physical Systems	Automotive Security [Koscher 2010] Smart Meters [McLaughlin 2011]
9	Cloud Computing	Amazon EC2 [Bugiel 2011] Hypervisor Attacks [Szefer 2011]
10	Mobile Platforms	Android Malware [Zhou 2012] Satellite Phones [Driessen 2012]
11	Classic Papers	Multics [Karger 2002] Compiler Subversion [Thompson 1984] Protection [Saltzer 1974]

A course bibliography is on the following pages.

Bibliography:

[Aaronson 2008] Scott Aaronson. The Limits of Quantum Computers. *Scientific American*, March 2008. URL: http://www.scottaaronson.com/writings/limitsqc-draft.pdf

[Aaronson 2012] Scott Aaronson et al. Quantum Money. *Communications of the ACM*, Vol. 55, No. 8, August 2012. URL: http://dl.acm.org/citation.cfm?id=2240258

[Bacon 2007] Dave Bacon and Debbie Leung. Toward a World with Quantum Computers. *Communications of the ACM*, Vol. 50, No. 7, September 2007.
URL: http://dl.acm.org/citation.cfm?id=1284648

[Bacon 2010] Dave Bacon and Wim van Dam. Recent Progress in Quantum Algorithms. *Communications of the ACM*, Vol. 53, No. 2, February 2010.
URL: http://dl.acm.org/citation.cfm?id=1646375

[Bugiel 2011] Sven Bugiel et al. AmazonIA: When Elasticity Snaps Back. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, October 2011. URL: http://dl.acm.org/citation.cfm?id=2046753

[Driessen 2012] Benedikt Driessen et al. Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards. *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2012.
URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6234409

[Elliott 2003] Chip Elliott et al. Quantum Cryptography in Practice. *Proc. ACM SIGCOMM 2003*, Karlsruhe, Germany.
URL: http://dl.acm.org/citation.cfm?id=863955.863982

[Karger 2002] Paul A. Karger and Roger R. Schell. Thirty Years Later: Lessons from the Multics Security Evaluation. *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Las Vegas, NV, December 2002.
URL: http://www.acsac.org/2002/papers/classic-multics.pdf

[Karri 2010] Ramesh Karri et al. Trustworthy Hardware: Identifying and Classifying Hardware Trojans. *IEEE Computer*, Vol. 43, No. 10, October 2010.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5604161

[Katzenbeisser 2012] Stefan Katzenbeisser et al. PUFs: Myth, Fact, or Busted? Security Evaluation of Physically Unclonable Funtions (PUFs) Cast in Silicon. *Proc. CHES 2012*, Leuven, Belgium, September 2012.
URL: http://www.springerlink.com/content/aw444489575214q2/

[Koscher 2010] Karl Koscher et al. Experimental Security Analysis of a Modern Automobile. *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, Oakland, CA, May 2010. URL: http://www.autosec.org/pubs/cars-oakland2010.pdf

[McLaughlin 2011] Stephen McLaughlin, Patrick McDaniel, and William Aiello. Protecting Consumer Privacy from Electric Load Monitoring. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, October 2011. URL: http://dl.acm.org/citation.cfm?id=2046720

[Murdoch 2010] Steven J. Murdoch et al. Chip and PIN is Broken. *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, Oakland, CA, May 2010. URL: http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf

[Schroeder 1974] Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems. *Communications of the ACM*, Vol. 17, No. 7, July 1974. URL: http://www.acsac.org/secshelf/papers/protection_information.pdf

[Singh 2000] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Books, 2000. URL: http://simonsingh.net/books/the-code-book/

[Skorobogatov 2012] Sergei Skorobogatov and Christopher Woods. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip. *Proc. CHES 2012*, Leuven, Belgium, September 2012. URL: http://dl.acm.org/citation.cfm?id=2240258

[Szefer 2011] Jakub Szefer et al. Eliminating the Hypervisor Attack Surface for a More Secure Cloud, *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, October 2011. URL: http://dl.acm.org/citation.cfm?id=2046754

[Thompson 1984] Ken Thompson. Reflections on Trusting Trust. *Communications of the ACM*, Vol. 27, No. 8, August 1984. URL: http://portal.acm.org/citation.cfm?id=358198.358210

[Wang 2012] Yinglei Wang et al. Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints. *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2012. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6234403

[Zhou 2012] Yajin Zhou and Xuxian Jiang. Dissecting Android Malware: Characterization and Evolution. *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2012. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6234407

From this milieu, the topic of computer securityâ€”later to be called information system security and currently also referred to as â€œprotection of the national information infrastructureâ€â€”moved from the world of classified defense interests into public view. A few peopleâ€”Robert L. Patrick, John P. Haverty, and myself among othersâ€”all then at The RAND Corporation (as its name was then known) had been talking about the growing dependence of the country and its institutions on computer technology.Â 1. â€œSecurity and Privacy in Computer Systems,â€ Willis H. Ware; RAND, Santa Mon-ica, CA; P-3544, April 1967.Â polymorphic virus, advanced persistent threat, distributed denial-of-service attack, inference and aggregation, multifactor authentication, key exchange protocol, and intru Each user of computers must decide what security means to him. For example, a defense agency is likely to care more about secrecy, a commercial firm more about integrity of assets. A description of the userâ€™s needs for security is called a security policy.Â security, and not according to how much work has already been done on that topic. To make up for this there is a concluding section that points out what technology is already in wide use, what is ready for deployment, and what needs more research. The conclusion also highlights the topics that are especially relevant to distributed and embedded systems. The careful analysis here may seem tedious, but it is the only known way to ensure the security of something as complicated as a computer system. SECTION 3: THE INTERNET 3.7 Internet security CHECK YOUR ENGLISH VOCABULARY FOR COMPUTER AND INFORMATION TECHNOLOGY.Â 3.7 Internet security. A. Choose the best words to go into each of the spaces. 1. A person who illegally accesses somebody else's computer over the internet is called a _. Introduction to the fundamentals of information security, computer security technology and principles, access control mechanisms, cryptography algorithms, software security, physical security, and security management and risk assessment.Â This unit provides an overview of information security. First, we look at the basic concepts of confidentiality, integrity, and availability as discussed in the National Institute of Standards and Technology (NIST) standard Federal Information Processing Standards (FIPS) 199. We will discuss threats, attacks, and assets in the overall context of a security management model. We will also learn about the challenges of information security and its overall scope. Completing this unit should take you approximately 6 hours. Unit 1 Learning Outcomes Page. Computing Science Department Faculty of Science. Instructor: E-Mail: COMP 3260 â€“ 3 Credits Computer Network Security (3,1,0). Fall 2015. Phone/Voice Mail: Office: Office Hours: CALENDAR DESCRIPTION. Students explore how information is exchanged on the Internet and the security issues that arise due to information exchange between different technologies.Â Students are introduced to the topics such as firewalls, public key infrastructure, security standards and protocols, virtual private networks, and wireless network security. Students also explore privacy, legal issues and ethics in context of network security. Prerequisites Â· comp 3270. Educational objectives/outcomes.