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.
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Subtopics/Readings/Labs</th>
</tr>
</thead>
</table>
| 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:


Computer security, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment, namely, serial numbers, doors and locks, and alarms. The protection of. The development of advanced security techniques continues to diminish such threats, though concurrent refinements in the methods of computer crime (q.v.) pose ongoing hazards. Learn More in these related Britannica articles Chapter 16 Advanced Security. Outline Security Requirements. Chapter 16 Advanced Security. Chapter 16 Advanced Security. Chapter 16 Advanced Security. Additional Resources. Slide Number 60. Objectives: Red Is New Since v.3.1.1 9.1 Explain why security is important 9.2 Describe security threats 9.3 Identify security procedures 9.4 Identify common preventive maintenance techniques for security 9.5 Troubleshooting security. BRK-126T New Topics in ITE PC. Use computer resources to correct a security problem in a wireless network. Lab 16.5.3RT: Remote Technician: Fixing a Security Problem (two students). The Level 2 technician, provides steps for a technician to follow.