College: College of Science  
Department: Department of Computer Science  
Syllabus Title: CS 464/564 – Networked Systems Security  
Call Number:  

1. Meet the Professor  

1.1. Instructor Contact Information:  
   Title: Assistant Professor  
   Name: Tamer Nadeem  
   Office Location: 3204 E&CS Building  
   Office Hours: Tuesday – 10:00-11:30am  
                Wednesday – 10:00 – 11:30am  
   Email Address(es): nadeem@cs.odu.edu  
   Telephone Number(s): 757-683-7718  
   Fax Number  
   Other  

1.2. Contact Policy  

1.3. About the Professor  
   Teaching and Education Background  
   Dr. Tamer Nadeem joined the department of computer science at ODU as an  
assistant professor in January 2011. He received his Ph.D. degree in Computer  
Science from the University of Maryland, College Park in 2006. Prior to joining  
ODU, he spent 5 years as a research scientist at Siemens Corporate Research  
(SCR) in Princeton, USA in which I led several research projects in the general  
areas of smart mobility for optimized intelligent transportation systems and  
dynamic radio management for enterprise and industrial wireless networks.  
Since I joined ODU, I have taught the wireless networked systems course once a  
year. I also introduced new course on application development for smart devices  
focusing on programming for Android devices and have been teaching it once a  
year. I also introduced new seminar course in Spring 2013 on physical cyber  
systems. The success of the seminar course encourage me to continue the trend  
and plan to introduce another seminar course on smart sensing in Fall 2016.  

Research Interests  
While at SCR, Dr. Nadeem led the development of several projects in the area of  
dynamic radio management for enterprise wireless networks, efficient cross  
layer protocols for vehicular networks, intelligent transportation systems,
location estimation and tracking of WLAN devices, and statistical characterization of VoWLAN. From 2004-2005, Dr. Nadeem was at Fujitsu Labs of America (FLA) in College Park, USA. While he was at FLA, he participated in designing, analyzing, and evaluating new paradigms for 802.11 wireless networks such as access points with sectorized antennas. Dr. Nadeem holds two US patents (#7,171,558, 2007 & #7,630,343, 2009) and has 15 pending patents. He has over 45 publications in peer reviewed scholarly journals and conference proceedings. He serves on the organizing committees of several conferences including recently ACM MobiCom 2013, ACM MobiSys 2013, and ACM HotMobile 2012. Recently, he served as program chair of the Ninth International Wireless Communications & Mobile Computing Conference (IWCMC 2013) - Mobile Computing Symposium, Cagliari, Italy, July 1-5, 2013. He serves as a member of the technical committees of various conferences in the areas of wireless management and vehicular networking. He also serves on several panels on vehicular networking. Dr. Nadeem's technical interests include wireless management for smart devices and enterprise networks, vehicular networks, intelligent transportation system, cyber physical systems, smart grid communication, network security, mobile and pervasive computing, and location determination systems.

Selected Papers and Publications
My [ODU CS website](http://www.cs.odu.edu/~nadeem/) has more information about me, including my research interests, research projects, and publications.

Personal Website
http://www.cs.odu.edu/~nadeem/

1.4. Teaching Philosophy

1.5. Teaching Assistant/Secretary Contact Information:

2. Student Resources

2.1. Online Student Orientation: [http://clt.odu.edu/oso](http://clt.odu.edu/oso)
2.2. Blackboard Support Web site: [http://clt.odu.edu/bb](http://clt.odu.edu/bb)
2.3. Technical Support Center: [http://occs.odu.edu](http://occs.odu.edu)
2.4. Paper Citation Styles: MLA, APA, Chicago, or CBE
   [http://owl.english.purdue.edu/](http://owl.english.purdue.edu/)

3. Accessibility Statement-From ODU Catalog

4. Course Readings

4.1. Required Materials
   **REQUIRED TEXT BOOK**

ISBN: 978-0-133-37043-0

Other readings are listed in each module of the course.

4.2. Optional Materials

5. Course Description

5.1. ODU Catalog Description

5.2. Instructor Course Description

This course is currently focused on network security. In order to understand the network security problem, the security section will begin with a review of various forms of network attacks including scanning, exploits and denial-of-service attacks. We will also review various cryptographic mechanisms like symmetric encryption, message digests, and public key crypto. Then, we will look at different security tools and protocols at different layers of network stack such as Layer 3 (IPSEC), Layer 4 (ssl) and Layer 7 (kerberos). We will also look at intrusion detection systems, viruses, firewalls VPNs and other security tools. Last but not least, wireless security issues (layer 2) will also be discussed.

5.3. Entry Level Requirements

Prerequisites

The main prerequisites for this course are CS 270 - Computer Architecture and CS 462/562 – Cybersecurity Fundamentals

5.4. Recommendations for Success

6. Course Objectives and Expectations

6.1. Course Objectives

This course gives students a strong foundation on different topics network security. Upon successful completion of this course, students will:

• Gain experience with the online course system.
• Recognize the general purpose and goals of the online course
• Gain the importance of network security.
• Familiarize with several terminologies that are used to define network, information, and computer security.
• Distinguish between different network technologies
• Identify different threats, vulnerabilities, and various types of attacks and hacks in network
• Identify the role of cryptography in network security and information security
• Gain knowledge on digital signatures, digital certificates, and the concept of a public key infrastructure.
• Familiarize with typical Authentication Systems and Human Authentication Mechanisms
• Describe IP security
• Explain different security systems to secure transport layer.
• Distinguish between different mechanisms for web security.
• Analyze the threats of intruders and malicious software
• Explain systems for intrusion detections and countermeasures for malicious software
• Identify the concept of a firewall, pros and cons, and explains how it functions.
• Explains the functioning of virtual private networks (VPNs) and how it works.
• Identify the threats and vulnerabilities associated with 802.11 wireless networks

More specific objectives for each topic are listed within each module.

6.2. Course Expectations

7. Teaching and Learning Methods

7.1. Delivery Method

This online course employs several methods of delivery and learning activities including online lectures and presentations, threaded discussions, Web sites, video clips, reading and written assignments, self-assessment checks, examinations, e-mail, and electronic access of information.

The course is divided into five units:

Introduction to Network Security
Cryptography
Network Security
System Security
Wireless Security

The course has two midterms and final exam. First midterm exam will be at the end of unit Two while the second midterm exam will be at the end of unit 3. The final exam will be at the end of the course.

Weekly Schedule

Each unit is divided into modules. Each module represents the material for one week of the course.

Monday New module begins
Wednesday Initial discussion question posting due before 11:59pm
Sunday Module ends. All materials (homework, discussion replies, reflections, feedback) due before 11:59pm.

7.2. Instructional Approach

7.3. Course Interaction
8. Course Schedule

Table/Chart showing week, class meeting days, date, topics, assignments, and due dates

<table>
<thead>
<tr>
<th>#</th>
<th>Week</th>
<th>Class Meetings</th>
<th>Date</th>
<th>Topics</th>
<th>Assignments</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>January 11</td>
<td>Module 1</td>
<td>Orientation and Introduction</td>
<td>January 17</td>
<td>January 17</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>January 18</td>
<td>Module 2</td>
<td>Network Technologies Overview</td>
<td>January 24</td>
<td>January 24</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>January 25</td>
<td>Module 3</td>
<td>Network Threats and Attacks</td>
<td>January 31</td>
<td>January 31</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>February 1</td>
<td>Module 4</td>
<td>Symmetric Encryption and Message Confidentiality</td>
<td>February 7</td>
<td>February 7</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>February 8</td>
<td>Module 5</td>
<td>Public-Key Cryptography and Message Authentication</td>
<td>February 14</td>
<td>February 14</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>February 15</td>
<td>Module 6</td>
<td>Midterm Exam I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>February 22</td>
<td>Module 7</td>
<td>Authentication Applications</td>
<td>February 28</td>
<td>February 28</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>February 29</td>
<td>Module 8</td>
<td>IP Security</td>
<td>March 6</td>
<td>March 6</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>March 7</td>
<td></td>
<td>Spring Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>March 14</td>
<td>Module 9</td>
<td>Web &amp; Transport-Level Security</td>
<td>March 20</td>
<td>March 20</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>March 21</td>
<td>Module 10</td>
<td>Midterm Exam II</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>March 28</td>
<td>Module 11</td>
<td>Intrusion Detection Systems &amp; Malicious Software</td>
<td>April 3</td>
<td>April 3</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>April 4</td>
<td>Module 12</td>
<td>Firewalls</td>
<td>April 10</td>
<td>April 10</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>April 11</td>
<td>Module 13</td>
<td>Virtual Private Networks</td>
<td>April 17</td>
<td>April 17</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>April 18</td>
<td>Module 14</td>
<td>802.11 Security</td>
<td>April 24</td>
<td>April 24</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>April 25</td>
<td>Module 15</td>
<td>(Last Day of Classes April 30)</td>
<td>Review and Conclusion</td>
<td>Review and Conclusion</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>May 2</td>
<td>Exam week</td>
<td>Final Exam</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Grading Criteria

Grading

Your grade in this class will be based on the following:

(Note that these percentages are only approximate and are subject to change, but by no
more than 10%.)

<table>
<thead>
<tr>
<th>Grading Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Discussion Participation</td>
<td>20%</td>
</tr>
<tr>
<td>Reflections and Feedback</td>
<td>5%</td>
</tr>
<tr>
<td>Midterm Exam I</td>
<td>15%</td>
</tr>
<tr>
<td>Midterm Exam II</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
</tbody>
</table>

**Grading Scale**

The grading scale is as follows:

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>94-100</td>
<td>A</td>
</tr>
<tr>
<td>84-87</td>
<td>B</td>
</tr>
<tr>
<td>74-78</td>
<td>C</td>
</tr>
</tbody>
</table>

This time limit includes weekends -- they are counted just like weekdays.

For example, most of our assignments are due on Sunday. A submission on Monday would have a penalty of 10%, and a submission on Tuesday would have a penalty of 20%. No submissions are accepted after Tuesday.

No credit is given for late discussion postings, reflections, or feedback.
I reserve the right to specify that late submissions will not be accepted for particular assignments.

10. Student Responsibilities

10.1. Managing Time
Students are expected to spend 10 hours per week on the course materials and assignments. Out of 10 hours, students are expected to spend approximately 3 hours per week to read the material, approximately another 3 hours/week for the homework and another 3 hours/week for discussions.

10.2. Understanding the Syllabus Requirements

10.3. Utilizing Online Components
Refer to the START HERE section within the Blackboard menu and the course tour

11. Course Policies

11.1. Attendance
Since this is an on-line course, there is no mandatory attendance policy. However, students are expected to actively participate in the discussions, homework submissions, reflections, and feedback. Each of these components is graded and counted toward the final grade.

11.2. Getting Help
Please use the discussion forum (on Blackboard) to ask questions about the course material or ask clarifying questions about an assignment. Feel free to answer questions that other students have posted in the Security Café.

If you need to contact the instructor about a private matter, the best way is through email (mweigle@cs.odu.edu), but do not expect or rely on an immediate response.

11.3. Tests and Make-ups
The same information for homework will apply for tests and make-up work: If a situation has occurred that requires your time and attention which will prevent submitting your work on time, please notify your instructor 24 hours before the scheduled due date.

11.4. Course Disclaimer
Every attempt is made to provide a syllabus that is complete and that provides an accurate overview of the course. However, circumstances and events may make it necessary for the instructor to modify the syllabus during the semester. This may depend, in part, on the progress, needs, and experiences of the students.

12. University Policies

12.1. College Classroom Conduct
Netiquette is the accepted behavior for online participation. Students are expected to follow good Netiquette rules. The following is a list of general guidelines for this course:

- Check your grammar and spelling
- Keep your comments focused on the topic
- Strive to write succinctly and clearly
- Share your knowledge and include supportive evidence for your comments
- Do not use all capital letters as that is viewed as shouting
- Avoid flaming—disrespectful language is unacceptable

Please read the Core Rules of Netiquette.

12.2. Cultural Diversity

12.3. Honor Pledge

By attending Old Dominion University, you have accepted the responsibility to abide by the honor code and honor pledge. This is an institutional policy approved by the Board of Visitors. If you are uncertain about how the honor code applies to any course activity, you should request clarification from the instructor. The honor pledge is as follows:

"I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member if the academic community, it is my responsibility to turn in all suspected violators of the honor system. I will report to Honor Council hearings if summoned."

Any evidence of an honor code violation (cheating) will result in a 0 grade for the assignment/exam, and the incident will be considered for further review. Evidence of cheating may include a student being unable to satisfactorily answer questions asked by the instructor about a submitted solution. Cheating includes not only receiving unauthorized assistance, but also giving unauthorized assistance.

Students may still provide legitimate assistance to one another. You are encouraged to form study groups to discuss course topics. Students should avoid discussions of solutions to ongoing assignments or exams and should not, under any circumstances, share solutions for an ongoing assignment or exam.

All students are responsible for knowing the rules. If you are unclear about whether a certain activity is allowed or not, please contact the instructor.

12.4. Special Needs

Old Dominion University is committed to achieving equal educational opportunity and full participation for persons with disabilities. It is the university's policy that no qualified person be excluded from participation in any university program or activity, be denied the benefits of any university program or activity, or otherwise be subjected to discrimination with regard to any university program or activity. This policy derives from the university's commitment to Non-discrimination for all
persons in employment, access to facilities, student programs, activities and services.
You may view the policy online: Old Dominion University Policies and Procedures 4500 - Accommodation of Students with Disabilities (pdf). For additional information visit the Office of Educational Accessibility online or at 1525 Webb Center.

12.5. University Email Policy
The Old Dominion University e-mail system is the official electronic mail system for distributing course-related Communications, policies, Announcements and other information. In addition, the University e-mail user ID and password are necessary for authentication and access to numerous electronic resources (online courses, faculty Web pages, etc.) For more information about the policy, please visit: Electronic Messaging Policy for Official University Community Policy 3506 (pdf).
For more information about student email, please visit http://occs.odu.edu/accounts/studemail/

12.6. Withdrawal
A syllabus constitutes an agreement between the student and the course instructor about course requirements. Participation in this course indicates your acceptance of its teaching focus, requirements, and policies. Please review the syllabus and the course requirements as soon as possible. If you believe that the nature of this course does not meet your interests, needs or expectations, if you are not prepared for the amount of work involved - or if you anticipate that the class meetings, assignment deadlines or abiding by the course policies will constitute an unacceptable hardship for you - you should drop the class by the drop/add deadline, which is located in the ODU Schedule of Classes. For more information, please visit the Office of the University Registrar.

12.7. Student Acknowledgement Options
“I, ________________, have completely read this syllabus and understand and agree to the course requirements.”