CISC859: Topics in Advanced Networks & Distributed Computing: Network & Distributed System Security

Introduction
General Information

- **Instructor:** Professor Rui Zhang
- **Office:** Smith Hall 448
- **Contact:** 302-831-2010, ruizhang@udel.edu
- **Office hours:** Tu/Th 9:30AM-10:30AM or appointment by email
Subject of Class

- Problems and solutions in network and distributed system security & privacy
- Focusing on unsolved problems and recent research
- Mostly on securing network infrastructure
- Not really on securing your LAN or individual computers
- Intended for graduate students with serious interest in doing research or pursing a career in network security
Class Organization

• Graduate-level seminar class
• Concerning selected topics of ongoing research in network and distributed system security & privacy
• Based around presentations and in-class discussions
  – Not formal lectures as you attended or expected
A Typical Class

• 2 papers will be presented and discussed
• Someone (usually one of you) will spend about 30 minutes presenting a paper assigned by me
• The following 5-10 minutes will be spent discussing it
• Whoever presented the paper should lead discussion
• Each student need present and lead the discussion on no more than 3 papers in the whole semester
Topics to Be Covered (Tentative)

• Telecom network security/privacy
• RFID system security/privacy
• Social network security/privacy
• Online/mobile cloud computing security/privacy
• Anonymous communications
• Location privacy
• Cognitive radio network security/privacy
• Wireless/mobile health security and privacy
• Smart grids security/privacy
• Mobile sensing system security/privacy
• Any other topic you may be interested in
Reading Materials

• No textbook required, only research papers from leading conferences and journals
• 4 papers per week
  – Papers will be made available on the class web page
• Helpful references on cryptography and security
  – “Handbook of Applied Cryptography,” by Menezes, van Oorschot, and Vanstone (Free online version is available)
  – “The Algorithmic Foundations of Differential Privacy”, by Aaron Roth and Cynthia Dwork (Free online version is available)
  – Wikipedia
Grading Policy

• Weighting factors
  – Homework: 20%
  – In-class presentation: 20%
  – Exam: 10%
  – Class participation: 10%
  – Term paper: 40%

• Attendance
  – All students must attend all the classes. Missing one class costs 1 points of the final grade in 100 scale

• Final grades
Grading Policy

\[ g = \begin{cases} 
A+, & s > 100, \\
A, & 90 \leq s \leq 100, \\
B+, & 85 \leq s < 90, \\
B, & 80 \leq s < 85, \\
C+, & 75 \leq s < 80, \\
C, & 70 \leq s < 75, \\
D+, & 65 \leq s < 70, \\
D, & 60 \leq s < 65, \\
E, & s < 60.
\end{cases} \]
Homework

- 4 papers will be assigned for each week
- You are required to read all of them and be able to competently discuss the material in class
- You are required to submit a one-page (letter size) summary for only ONE of the assigned papers
- A summary must
  - Include a one-paragraph description of the paper and descriptions of three strong points plus three weak points you discovered in the paper
  - Should be single-column, 1 inch margins, 11-point size, single-spaced, and written using text editors like MS Word and Latex.
  - Should be emailed to me in PDF/DOC before noon (12pm) every Monday with /CISC859 and HW# in the subject line
In-Class Presentation

• Presentation preparation
  – Thoroughly study the paper, read the references if necessary, prepare the slides, & practice the talk if necessary
  – The slides (MS PowerPoint) should be emailed to me before noon (12pm) of the day when you ought to do the presentation
  – You should spend sufficient time preparing the presentation and must be able to lead an active discussion as well as answering questions to the paper raised by the audience

• Leading a class discussion should focus on
  – Analysis of the problem
  – Critiques of existing solutions
  – Suggested improvements to those or entirely new solutions
Grading In-Class Presentations

• Preparation of slides (20 points)
• Clarity of the content (35 points)
  – Does the presenter discuss the basic techniques logically and clearly?
  – Introduction (10 points)
  – At least one of the main techniques (25 points)
• Clarity of the oral presentation (5 points)
  – Does the presenter speak clearly?
• Coverage (10 points)
  – Does the presenter cover at least one of the essential techniques in the paper?
• Future work (5 points)
  – Does the presenter have a clear idea what could be done based on the results in the paper?
• Questions and Answers (15 points)
  – Does the presenter give satisfactory answers to audiences’ questions?
• Leading of the Discussion (10 points)
Class Participation

• This course is designed to be a highly interactive course so that active participation in class discussion is required.

• Class participation in discussing papers (10%)
  – Very active participation (9-10)
  – Active participation (6-8)
  – Some participation (3-5)
  – No participation (0-5)
Class Projects (Term Papers)

• 40% of the final grade
• Students are required to form a team of 1-2 members to complete a term paper on one of the topics discussed in class or others approved by the instructor
• The term paper can be either a survey paper or a research paper
• Project Timetable
  – Term paper proposal (20%): due on 5pm, 4/1/2017
  – Final term paper (80%): due on 5pm, 5/16/2017 (tentative)
Term Papers: Research vs. Survey

• Research papers
  – You should focus on original research problems, and the outcome should be a paper with original technical contribution
  – Your grade will be judged on originality, soundness of the approach, and the quality of presentation
  – You are encouraged to choose this option if you are a Ph.D. student or a Master student needing to finish a thesis
  – You are encouraged to combine this effort with your current research and discuss it with me during my office hours
  – You will be rewarded by up to 15 points depending on the quality of your work
  – **Special Warning**: it is much more difficult to write an original research paper than a survey paper
Term Papers: Research vs. Survey

• Survey papers
  – You can write a paper that surveys a particular field on network security. The outcome should be a paper that summarizes the trend in the field you have chosen
  – You must survey up to most recent research results
  – Your grade will be judged on the completeness of the survey, the quality of the trend analysis, and the quality of presentation.
How to Find References

• Most relevant conferences
  – IEEE INFOCOM, ICNP, ICDCS, IEEE Symp. on Security & Privacy, IEEE SECON,
  – ACM CCS, SIGCOMM, MOBICOM, MOBIHOC, MobiSys, WiSec
  – USENIX Security, NSDI
  – ISOC NDSS

• Most relevant journals
  – ACM Transactions on Privacy and Security (TOPS)

• Google Scholar
Honor Code

• The UD Honor Code will be upheld, and any violations in homework & projects will be brought to the immediate attention of the Office of Student Conduct.
Special Warning

- You are not supposed to exploit any technique discussed in class to break into any computer system or network that is not your own.
Prerequisite

- A good understanding about computer network concepts
- Knowledge in basic cryptographic, security, and privacy concepts is preferred but not required
  - These will be reviewed in the first 6 classes
Reasons for Taking My Course

• You do not like taking exams 😊
• You do not like buy an expensive textbook 😊
• You do not like regular lecture-type courses 😊
• You want to learn something in this exciting area
• You are a Ph.D. student interested in doing research in Internet or wireless network security
• You are a Master’s student interested in pursuing a career in network security
• You want to challenge yourself
• …
Reasons for Not Taking My Course

- Do not have the pre-requisites
- You have to get a grade at least B
- You are not interested in network security & privacy, but only interested in a grade (with the hope of good grade)
- You only rely on good memory
- You do not like interactive lectures
- You prefer exams to projects/presentations
- You do not want to do your homework or projects independently
- …
Several Classes Need be Rescheduled

• Feb. 14th (next Tuesday)
• March 9th
• May 2nd
• May 4th (possible)
• May 11th