Syllabus

Course Details

Course CSC 591/791 Cellular Network Security

Meeting Location TBD

Meeting Times TBD

Credits 3 credit hours

Instructor Dr. Brad Reaves

Email bgreaves -at- ncsu.edu

Office 3256 Engineering Building 2

Office Hours TBD

Grader TBD

Course Prerequisites

Formal: A computer networking course at the undergraduate or graduate level (equivalent to CSC 401 or CSC 570) and a computer security class (examples include CSC 474, 574, 405); or permission of the instructor.

Overview

Cellular networks are essential to modern infrastructure. Not only do they power the daily communications of billions of individuals, they are and will be the primary access medium for over a billion people in developing regions. The newest generation of cellular networks (5G) will not only accelerate current uses of cellular networks, but potentially enable exciting new applications like vehicle-to-vehicle communications, IoT devices, and even remote robotic assisted surgery.

Despite their ubiquity and import, cellular networks present a number of unique security challenges. In this course, we will study in detail how these networks function and the current state of the art of their security. This course provides an in-depth investigation into security issues in areas including cellular air interfaces, core networking (SS7, IMS), cellular data networking, and mobile device architectures. In particular, we will study how these networks provide (or fail to provide) high confidentiality, integrity, availability, authentication, and privacy. A key focus of the course will be how the design philosophy of telephone networks differs from the Internet, complicating traditional security solutions. The security of these networks are poorly understood by computing professionals, making competence in this area a rare and valuable skill.

A detailed list of lecture by lecture contents, assignments, and due dates (subject to change as semester evolves) will be available on the course schedule.

This course has 2 course numbers: CSC 591 and CSC 791. While the in-class material is the same, the out-of-class expectations differ. Students in CSC 591 will be expected to demonstrate mastery of the material through out-of-class assignments and midterm and final exams. Students in 791 will demonstrate mastery through the successful execution of a novel research project in cellular security in place of a final exam.

Student Learning Outcomes

By the end of this course, students will be able to:

- Explain the design and functioning of cellular networks
- Explain and critique existing cellular network security mechanisms
- Identify, explain, and critique recent cellular security research
- Know the most important conferences and journals for network security research
- Identify some of the current trends and open problems in cellular and telephone network security research

Students in CSC 791 will additionally:

- Summarize and explain orally a research idea / contribution in a clear and appealing way
- Define a network security research problem and justify it
- Do research in network security using proper methodology
- Write ideas and results in a clear, technically appropriate way

Textbooks and Reading Material

This course will use a textbook: P. Traynor, P. McDaniel and T. La Porta. Security for Telecommunications Networks. Springer, Series: Advances in Information Security, August, 2008. ISBN: 978-0-387-72441-6.

Readings will also come from recent network security research papers. You should expect to read and review 1 chapter or two papers most class periods.

CSC 791: Course Structure and Grading

The course will consist primarily of in-class lectures, readings from recent literature, homework assignments, a midterm exam and a course research project.

Your grade will be determined as follows:

- 20% Midterm exam
- 15% Assignments
- 15% Participation
- 50% Class Project

The final letter grade will be based on the final percentage as follows:

> A+ <= 97% < A <= 93% < A- <= 90% < B+ <= 87% < B <= 83% < B- <= 80% < C+ <= 77% < C <= 73% < C- <= 70% < D+ <= 67% < D <= 63% < D- <= 60% < F

REG 02.50.03 describes the grade point interpretation of letter grades.

CSC 591: Course Structure and Grading

The course will consist primarily of in-class lectures, readings from recent literature, homework assignments, and a midterm and final exam.

Your grade will be determined as follows:

- 30% Midterm exam
- 30% Final exam
- 25% Assignments
- 15% Participation

The final letter grade will be based on the final percentage as follows:

> A+ <= 97% < A <= 93% < A- <= 90% < B+ <= 87% < B <= 83% < B- <= 80% < C+ <= 77% < C <= 73% < C- <= 70% < D+ <= 67% < D <= 63% < D- <= 60% < F

REG 02.50.03 describes the grade point interpretation of letter grades.

Assignments: The instructor will assign homework assignments on a periodic basis for topics associated with the class . These homeworks require the students to write, program, or perform other basic research. The content and due dates of these assignments will be decided over the course of the semester. If you cannot attend a lecture, contact other students to see if any assignments have been made and consult the syllabus.

CSC 791 Course Project: The course project requires that students execute research in cellular network security. The result of the project will be a complete research paper formatted for submission to a workshop of conference. Project topics will be discussed in class about 25% of the way through the class. Be realistic about what can be accomplished in a single semester. However, the work should reflect real thought and effort — projects executed in the closing days of the semester are unlikely to be well received. The grade will be based on the following factors: novelty, depth, correctness, clarity of presentation, and effort.

Class Participation: Enthusiastic, intentional class participation is an essential element of this course. To do well in this course, students must take active and regular roles in discussion and demonstrate comprehension of the reading themes. Students are required to do the assigned reading before class.

Devices Students are encouraged to use computing devices during lectures in ways that facilitate their learning and do not distract others. However, using devices for activites not related to the class (including excessive off-topic browsing, social media, or for out-of-class assignments) will result in poor participation grades.

Grading Concerns Timely and informative feedback is an essential element of effective education, and the instructional staff makes every effort to fairly and accurately grade every assignment and exam. If a student believes that a grading error has been made, they should contact the instructional staff *by email* clearly and objectively detailing the error and how the student believes it should be corrected. *Grading corrections will not be made without a request in writing.* While we are happy to correct honest errors, note that in the case of a grade dispute, the instructional staff reserves the right to regrade an entire assignment.

Weekly Course Schedule

See the attached course schedule.

Assignment Lateness Policy

Assignment deadlines will be hard. Mini-reviews submitted after class will not be graded. Other assignments, where applicable, will be assessed a 20% per-day late penalty, with a maximum of 3 days. Unless the problem

is apocalyptic, excuses will not be effective in reducing the penalty. Students with legitimate reasons who contact the professor before the deadline may apply for an extension.

Attendance Policy

The instructor will not take any formal attendance for class meetings. However, regular attendance is critical for meeting the learning objectives of the course. Students with erratic attendance will receive poor attendance grades. Students missing class should consult classmates on missed material.

The university policy on excused absences will be observed (see REG 02.20.03). Late submission of non-exam assignments due to excused absences is not subject to the policies on late assignments.

Academic Integrity Policy

Students in this class are *welcome and strongly encouraged* to discuss assignments outside of class, including to have other students review and provide feedback on all aspects of presentations or project progress. However, the actual work of the assignment should be done by the assigned parties. Mini-reviews should be completed *individually* before class. Students are explicitly forbidden from copying the work of others (with or without superficial modification). This includes Internet or text sources for code or prose.

My experiences with NC State students so far have lead me to believe that nearly every student is honorable, and I have every reason to believe that the students in this course will complete assignments in an honest fashion.

However, should an incident arise where I believe academic misconduct has occured, the university, college, and department policies against academic dishonesty will be strictly enforced. You may obtain copies of the NCSU Code of Student Conduct from the Office of Student Conduct. The instructor has a zero tolerance policy for violations of academic integrity. which include but are not limited to plagiarism and illegal collaboration. If a student is in doubt about the conduct of themselves or others, the instructor welcomes questions about this policy. In this case, it is far better to ask permission, as there will not be forgiveness of academic misconduct. The penalties for academic misconduct will include assigning at least a **negative** grade and refering the student to the appropriate University bodies for possible further action.

It is the understanding and expectation of instructor that the student's signature on any assignment means that the student neither gave nor received unauthorized aid. For additional information, visit studentconduct.ncsu.edu.

Ethics Statement

This course considers topics involving personal and public privacy and security, and this course covers topics concerning the security of many systems that are widely deployed and potentially critical. As part of this course, we will investigate methods, tools and techniques whose use may negatively impact the rights, property and lives of others. As security professionals, we rely upon the ethical use of the above technologies to perform research. However, it is easy to use such tools in an unethical manner. Unethical use includes the circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services.

This is NOT a class on hacking. Any activity outside of the spirit of these guidelines will be reported to the proper authorities both within and outside of NC State and may result in dismissal from the class and the University. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through the proper channels; however, students with any doubt should consult the instructor for advice. DO NOT

conduct any action which could be perceived as technology misuse anywhere or under any circumstances unless you have received explicit permission from the instructor.

When in doubt, please contact the course professor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from the instructor.

Resources for Support

The instructor's goal is to help students gain a clear understanding of the course material, to foster a deep interest in the topic of computer security, and develop the basic research skills essential to a career at the frontiers of technology. With security, the devil is often in the details, and crucial understanding often relies on subtleties. Accordingly, it is natural for students to struggle both with the content of this course and with requisite background material.

To this end, the instructional staff are providing a number of mechanisms for support. These include:

- **Piazza** The course will feature a Piazza message board, available here. This should be your first go-to resource for any questions about course structure, deadlines, class material, or anything else that could possibly be relevant to other students. Note that active participation in Piazza will enhance your participation grade. The instructional staff receives emails from Piazza, so any questions posted to Piazza will be addressed as fast or faster than those sent by email. *Piazza will be the main form of out-of-class communication.*
- **MediaSite** I will make recorded lectures available to you to aid in studying or to help in catching up after absences. These will be available on Mediasite. Please be advised this course is being recorded for current and potential future educational purposes. By your continued participation in this recorded course, you are providing your permission to be recorded.
- **Office Hours** The instructor will hold office hours weekly. Students are highly encouraged to come to office hours with the instructor to discuss doubts about course material, concerns about course performance, consult on the course project, or to discuss computer security beyond what can be discussed in class. No appointment is needed to attend office hours. The instructor is also available by appointment outside of office hours when meeting is impractical.
- **Email** The instructional staff strongly requests that you limit individual emails to communications regarding private questions (like grade concerns), appointment and make up exam requests, and other communications that are not suitable for Piazza. Note that emails that are of a general nature will be posted anonymously to Piazza on a student's behalf. To ensure that student emails receive a high priority, students should place the string "[CSC XXX]" somewhere in the subject line.

If at any time you have constructive suggestions about how to improve the course, feel free to share them with the instructor during office hours or via an email.

Statement on Identity

I make an effort to treat all of my students with respect, and an important part of that is correctly addressing students with correct names and pronouns. If you would like to be called by a different name or pronoun other than what is in the directory, let me know (in person or email). Also, if I mispronounce your name, please let me know – it is not intentional!

Statement on transportation

Students have to provide their own transportation for any and all class related trips.

Statement on safety and risk assumption

This course does not require activities that pose physical risk to students.

Statement for students with disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with Disability Services for Students at 1900 Student Health Center, Campus Box 7509, 919-515-7653. For more information on NC State's policy on working with students with disabilities, please see the Academic Accommodations for Students with Disabilities Regulation (REG 02.20.01).

Statement on Class Evaluation

Online class evaluations will be available for students to complete during the last 2 weeks of the semester for full semester courses and the last week of shorter sessions. Evaluations then become unavailable at 8am on the first day of finals. For full semester courses, evaluations will be available: 8am April 16th, 2018 through 8 am April 30th, 2018.

N.C. State University Polices, Regulations, and Rules (PRR)

Students are responsible for reviewing the PRRs which pertain to their course rights and responsibilities. These include: Equal Opportunity and Non-Discrimination Policy Statement, Office for Institutional Equity and Diversity, Code of Student Conduct, and Grades and Grade Point Average.

Lecture #	Topic	Reading
1	Security Basics	Traynor et al., Chapter 2
2	Security Basics	
3	Project Ideas	
4	Cellular Basics	Traynor et al., Chapter 1
5	Cellular Basics	
6	Cellular Basics	
7	Cellular Networking	Traynor et al., Chapter 3.1-3.3
8	Project Mini-presentations	
9	Cellular Networking	
10	Cellular Networking	
11	GSM Air Interface	
12	GSM Air Interface	
13	Academic Writing	
14	3G/4G Air Interface	
15	**Midterm Exam**	
16	Cellular Data Networking	Traynor et al., Chapter 3.4
17	Cellular Authentication	
18	Exam Review	
19	Classical Telco Security Problems	Traynor et al., Chapter 4 M. Sahin, A. Francillon, P. Gupta, M. Ahamad. SoK: Fraud in Telephony Networks, Proceedings of IEEE
20	Overload in GSM	Traynor et al., Chapters 5 and 6 P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. La Porta and P. McDaniel, On Cellular Botnets: Me
21	End-to-End-Authentication	V. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. Hunter and P. Traynor, PinDr0p: Using Single-End H. Tu, A. Doupe, Z. Zhao, and G. Ahn. Toward Authenticated Caller ID Transmission: The Need for a Sta
22	End-to-End Authentication	B. Reaves, L. Blue and P. Traynor, AuthLoop: End-to-End Cryptographic Authentication for Telephony ov B. Reaves, L. Blue, H. Abdullah, L. Vargas, P. Traynor and T. Shrimpton. AuthentiCall: Efficient Identity a
23	Eavesdropping and In-band Signaling	R. Rosenbaum, Secrets of the Little Blue Box, Esquire Magazine, 1971 (link) M. Sherr, E. Cronin, S. Clark and M. Blaze, Signaling Vulnerabilities in Wiretapping Systems, IEEE Secur
24	Privacy and Tracking	D. F. Kune, J. Koelndorfer, N. Hopper, Y. Kim, Location Leaks on the GSM Air Interface, Proceedings of t B. Hong, S. Bae and Y. Kim, GUTI Reallocation Demystified: Cellular Location Tracking with Changing T
25	Project Presentations	
26	Bypass Fraud	M. Sahin and A. Francillon, Over-the-top bypass: Study of a recent telephony fraud, Proceedings of ACM
27	Course Review	