Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

Week 0

Course introduction

Course Introduction

- Course logistics
- Textbook(s), other reference material
- Course requirements & Grading policy
- Course outline

Your Instructor

- Bruce McNair

Distinguished Service Professor of Electrical and Computer Engineering
Stevens Institute of Technology
Burchard B-206 Castle Point on Hudson
Hoboken, NJ 07030

Preferred means of personal contact (in order):

On-line discussion posting
Stevens email (bmcnair@stevens.edu)
Phone: 201-216-5549
Visit my office (I am generally on-campus ~9:30 - ~4 Monday-Thursday). Check www.ece.stevens.edu~bmcnair/schedule.htm for detailed times.

Background:

Stevens alum (BE - Class of ’71, MEE ’74)
7 years working in defense industry/government (wireless & security)
24 years working for Bell Labs/AT&T Research (wireless communications, system security, signal processing, data networks, analog modems, software design, system prototyping, speech processing, etc. “retired” March 2002)
Amateur radio license for 40 years
Founder/CTO: Novidesic Communications, LLC
Joined Stevens faculty in August 2002

Textbooks and reference material

- Primary text:
  - “Wireless Security – Models, Threats, and Solutions,” by Nichols and Lekkas, McGraw-Hill, 2002, ISBN 0071380388.

- Other materials
  - Links and copies of vendor materials as needed

Class interaction

- The first part of the course is lecture format – but I welcome questions to clarify material and direct discussion

- The second part of the course is team-based security assessment with Red/Blue team divisions (Problem finders/Problem solvers). I will set up on-line Discussion Boards for this class for each case study with Red and Blue team areas.

- (note – this is mainly for the benefit of students taking the on-line section of the course, but students taking an on-campus section are welcome to augment their classroom interactions with the on-line discussion groups. The 584A and 584WS sections are set up in separate shells, so there is no interaction between the two groups of students)

Grading Policy

- Participation in Class or on-line discussions: 15%
- Three papers (3-5 pages) due during semester: 15% each
- Participation in security assessments: 15%
- Final project report written: 20%
- Final project 'presentation': 5%

- All items will leave *lots* of room for extra credit

- All assignments must be emailed, not scanned handwritten pages

- For on-line section:

  FINAL PRESENTATIONS ***MUST*** BE SUBMITTED BY THE DUE DATE TO MAKE THEM AVAILABLE FOR OTHER STUDENTS TO REVIEW ON-LINE. SIGNIFICANT GRADE PENALTIES WILL BE APPLIED FOR LATE SUBMISSIONS (presentations that are N days late will be given a grade no higher than $(.9^N)^N$ times maximum possible score)

A Note on Plagiarism and Honor Code

- Plagiarism:
  - From the Stevens Honor Board web site:
    - "The dictionary defines plagiarism as the act of '...stealing and using the ideas, writings, or inventions of another as one's own' or '.... taking passages, plots, or ideas from another and using them as one's own'."
  - All work submitted for this class for credit ***must*** have a ***full*** citation of the source – enough to enable the reader to find the specific material without any additional searching.
  - Work found to be substantially identical or directly derived from a cited source or other unidentified sources will be assigned a grade of 0 **without further discussion or options for resubmission**
  - Note that significant evidence of plagiarism in ***any*** of your work will result in a maximum course grade of C. Repeated instances of significant plagiarism will result in an F in the course, independent of what grade you may have gotten on other assignments.
  - Should you find it necessary to use the words of the sources' authors unmodified, they must be specifically quoted (as I have done above). If the words aren't quoted, you are implicitly saying that they are yours; however, if a substantial portion of the paper consists only of direct quotes, you should seriously consider what the value added of your portion of the paper is
- Students taking TM584 are also bound by the Howe School Statement of Ethical Conduct

RE-READ THE LAST TWO SLIDES AND SPEAKERS NOTES

- Obviously, this slide wouldn't be necessary unless problems with plagiarism continued.

- ANY REPORT SUBMITTED WITHOUT A ***COMPLETE*** CITATION OF THE SOURCE WILL NOT BE GRADED.

- This is a proper citation of a source:
  - Clearly, Seymour, "Must The Obvious Be Restated?," International Conference on Repetitive Events, Podunk, Iowa, April 1, 2006.

    (Enough information for someone to find the material in the future)

- These are NOT a proper citations of a source:
  - Clearly, "Must the Obvious Be Restated"
  - Seymour Clearly, Obvious paper.

- If the last two examples sound silly, I can show you a few submissions for this course that have tried to pass off citations as those shown. Misleading citations (e.g., copy from X, partially cite Y) will not be viewed favorably.

And Two More Items on Plagiarism and Related Issues…

- In past semesters, I have seen most plagiarism in the form of copying large sections of text from a published paper without citation. I added this slide because I have started to see students submitting a paper that is identical to that submitted by another student in a previous semester. In case there was any question, these papers will receive a grade of 0 as well

- I teach two related courses, EE/NIS/TM-584 (Wireless Systems Security) and NIS/CpE-691 (Information Systems Security). Many students take both of these classes. Submitting the same paper for both is not acceptable (some schools define this as "self-plagiarism") – I expect original work in each class for separate grades. Besides, the specific course requirements are different for the papers and projects. If you wish to use the same source paper for both courses, I think you are short-changing yourself, but I will allow source reuse. The submitted material must, however be substantially different.

And one more note on references

- It should be clear that you need to cite your references for your work, but there appears to be a question about what sources should be included as references.

- For instance, here is an actual citation from a recent student submission:
  - D.S. Johnson, private communication (October 1975)

- How is this possible? The student was born in 1990! Has he employed time travel to go back and interview Dave Johnson? Or, MAYBE, the author of the paper the student used was the person who spoke to Johnson! I'll never know, there was no useful citation in the submission.

- Or, remarkably enough, I have seen 5 page papers that list 27 references. WOW, how did they compress all that research into 5 pages? Or, perhaps, they just thought it would be impressive to list every reference the paper or two they used cited.

- The bottom line: **DO NOT LIST A REFERENCE IN YOUR PAPER UNLESS YOU PERSONALLY ACCESSED AND READ THE REFERENCE AND EXTRACTED SOME USEFUL INFORMATION FROM IT.**

For Students Taking the TM-584 Section of This Course: Howe School Statement of Ethical Conduct

Ethical Conduct

The following statement is printed in the Stevens Graduate Catalog and applies to all students taking Stevens courses, on and off campus.

"Cheating during in-class tests or take-home examinations or homework is, of course, illegal and immoral. A Graduate Academic Evaluation Board exists to investigate academic improprieties, conduct hearings, and determine any necessary actions. The term 'academic impropriety' is meant to include, but is not limited to, cheating on homework, during in-class or take home examinations and plagiarism."

Consequences of academic impropriety are severe, ranging from receiving an "F" in a course, to a warning from the Dean of the Graduate School, which becomes a part of the permanent student record, to expulsion.

Reference: The Graduate Student Handbook, Academic Year 2003-2004 Stevens Institute of Technology, page 10.

Consistent with the above statements, all homework exercises, tests and exams that are designated as individual assignments must contain the following signed statement before they can be accepted for grading.

_____

I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination. I further pledge that I have not copied any material from a book, article, the Internet or any other source except where I have expressly cited the source.

Name (Print) _____ ***Signature*** _____ ***Date:*** _____

Please note that assignments in this class may be submitted to www.turnitin.com, a web-based anti-plagiarism system, for an evaluation of their originality.

Notes on submissions

1. Depending on the semester, I am teaching 2-3 undergraduate courses and about 4 sections of 3 graduate courses. To keep things straight, I need students to mark their submissions so I can tell them apart. Your email attachment must include your name, the course and the submission information. For instance, Sally Smith, submitting the 2nd paper to EE584 should title their attachment something like:

   Sally_Smith-Paper2-EE584.doc

   This is particularly important for students enrolled in more than one of my courses when they submit work after the due date (see next slide about due dates)
2. With hundreds of students in all the course sections, I do not directly acknowledge any submissions and cannot review drafts of papers. Instead, I use the on-line gradebook to give students feedback on the status of their submissions. Within a day or two of the paper submission, I will change the status of the assignment in the on-line "My Grades" page. Overdue, submitted, and graded work will be so marked. Work that is not due or has not been acknowledged will be unflagged.
3. When you email me an assignment, you should use Stevens email. If you send a large (>4 MB) attachment, please send a separate email to let me know you sent it, in case the attachment causes the email to get bogged down.

Withdrawals, Incompletes and Late Submissions

- Since I am invariably asked about late submissions, incompletes and withdrawals, etc. in or after the final weeks of my courses, I'll address the questions up front. I am normally sorry for making some of my policies known, but I am actually pretty lenient about late submissions. I know that there are sometimes good reasons outside the school for a student not to be able to get work in on time, so I do not penalize late submissions for ***most*** assignments. The exception for this course is the final presentation, which is heavily penalized for late submission
- A related question is about submissions after the end of the class. For this, I am restricted by school policies. I'd love to let you take an extra month to finish all your work, but consider what this would mean to the Administration. How can they send out final grade reports on time if the instructors don't turn grades in on time? For this reason, we are obligated to finalize grades within a predetermined time after the last day of the course or the final exam, whichever comes first. For this reason, I am limited in how late I can accept assignments for credit in the course.
- Finally, there is the question of Withdrawing from the course or taking an incomplete. Again, the school sets the policy. Withdrawal is permitted up to a certain date, which varies for on-campus and WebCampus classes and by semester. You can find the school policy on the school calendar on the Registrar's web site. Similarly, there are restrictions on when a grade of Incomplete can be granted. I will generally allow an incomplete if it is for good reasons, consistent with school policy. "I didn't have enough time to finish everything" is not an allowable excuse. Real, extenuating circumstances, like death (but not the student's), illness, or extreme natural calamities will generally be accepted as valid reasons to permit an incomplete. If you do receive an incomplete in one of my courses, there will always be a set date by which you will retake the course. The chances of getting permission the N^{th} time for an incomplete in a course section that you are making up an incomplete drop even faster than late presentation submissions.

Course Outline

Lecture/discussion format

Red team/Blue team Brainstorming format

On-line	On-campus		
Week 0	Week 1	Introduction, Logistics, Course structure,	
Week 1	Week 1	Basic wireless issues	
Week 2	Week 2	Continued discussion of wireless	
Week 3	Week 3	Security services, mechanisms	Assign paper on wireless
Week 4	Week 4	More discussion of security mechanisms	
Week 5	Week 5	Security issues particular to wireless, economic tradeoffs, introduction to brainstorming process and assessment process, Case study 1 – introduction, vulnerability discussion, potential improvements, tradeoffs	
Week 6	Week 6	Case study 2	Assign paper on security
Week 7	Week 7	Case study 3	Project description
Week 8	Week 8	Case study 4	
Week 9	Week 9	Case study 5	Assign paper on current wireless security issues
Week 10	Week 10	Case study 6	
Week 11	Week 11	Case study 7	
Week 12	Week 12	Course Summary, Advanced Topics, Future Directions	Presentation and Term project due
Week 13	Week 13 & 14	Presentations	

Topics - 1

- Common topics overview
  - Wireless
    - Characteristics
    - Channels
    - Propagation
    - Types of wireless systems and their parameters
      - Satellite
      - Terrestrial microwave
      - Military tactical
      - Cellular
        - » AMPS
        - » 2G – IS-136, IS-95
      - WLAN
        - » 802.11a, b, g

Topics - 2

- Common topics overview (continued)
  - Security
    - Definition
    - Services
    - Mechanisms
      - Spread spectrum
      - Frequency hopping
      - Encryption
      - Integrity check-sums
    - Assessment
    - Issues, specifically related to wireless
      - Jamming
      - DFing, geolocation
      - Interception
      - Spoofing
      - Fraud
      - Theft of service
      - Traffic analysis

Topics - 3

- Specific examples (case studies) – for each of these, the subject matter is covered as: context, issues, solutions, tradeoffs
  - Satellite
    - Jamming
    - Theft of service – entertainment services on downlink
    - Hidden signals – theft of service – uplink
    - Monitoring long distance communications
  - Terrestrial microwave
    - Jamming
    - Compromise of information and signaling
  - Military tactical
    - Antijam (AJ)
    - Low Probability of Intercept (LPI)
    - Circular Error Probability (CEP)
    - Spoofing
    - Confidentiality of information
    - Traffic analysis

Topics - 4

- Specific examples (case studies) (continued)
  - Cellular
    - Cloning of AMPs – fraudulent use/theft of service
    - Privacy issues
    - E911/Geolocation
  - WLAN
    - WEP issues
    - Managing a wireless LAN interconnected to wired LAN
- Summary - What is the general lesson learned from these case studies?
- Advanced Topics and Future Directions

Week 0 Assignment

- Under “Discussions” there is a section “Introduction”. Post a short (a few sentences) note about yourself: interests, background, what you expect to get out of the course.
- Upload a small file with your posting (a small JPEG image of yourself would be useful so others in the class can put a face with the name)
- Using Stevens email, send me (bmcnair) a message when you have posted your message or send me a message if you are having difficulty.

Note: this is for the on-line sections only