Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

This class is cross-listed as an EE, Networked Information Systems, and Technology Management course. As such, I won't be making too many assumptions about your background. For example, to discuss wireless technology, it is helpful to have an EE/ Communications Theory background, but you might not have been exposed to some of this material. Likewise, when we get into security technology, background in Information Theory (an EE subject), computer networks (CpE or CS topics), risk management (Technology Management), etc. might be useful. To deal with the broad topic areas and varied student backgrounds, I will try to incorporate most of this background material into this course. If you are taking or have taken my EE/MT/PEP-585 course (Physical Design of Wireless Communications Systems), you may recognize some of the slides with wireless material I have used with that course. However, the emphasis here is going to be on the security aspects of wireless communications, rather than what makes a wireless system work.

A major difference between this course and other EE/technology courses is going to be focus on the process, rather than the product.

Week 0

Course introduction

Course Introduction

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

Since this is an on-line course, I have to include more information about course logistics up front than I normally would. In particular, we don't have an option of physically handing in assignments or class presentation like a face-to-face class normally does. For this reason, I have to specify formats and means of delivery of materials more stringently than I would in a live class.

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

My first choice for interaction is what we would see in class – ask general questions in the discussion boards for the class in case others are interested in the question. If it is something that is not appropriate for general discussion, use the Stevens email.

If real-time interaction is needed, you can always call me or stop by my office if that is convenient.

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

When I first started preparing this course in the Summer of 2003, I couldn't find any textbook that addressed the topic fully with the technical depth I was looking for. The best book I could find is listed here. Consider this book to be a broad summary of the background material we are discussing. I don't cover every item in the book and the book doesn't provide all the background for the course, but it is a fairly good background reference. If you are particularly interested in any particular topic in the course, I can steer you to further reading, but I didn't want to create a reading list a yard (or meter) tall.

I will provide links to relevant vendor and other material on the web 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)

We will start out discussing wireless topics and security topics in a lecture format. I will pose several topics for discussion through out the weeks' material. The real value of any course, whether it is in-person or on-line is the questions that are raised and the discussion that ensues. For this reason, I grade this on-line course (as well as the live course) including class interaction. For this class, the second half of the semester is very heavily driven by class interaction. As you will see, I intend to introduce several case studies of real wireless communications systems. After I have described security issues and wireless considerations, and have provided a format to think about security issues in systems, most of the case studies will be driven by student discussion.

The case studies in the second half of the class will be run like this: I will describe the case example, defining the system, its attributes, the application, and other background material needed. I will randomly break the class into two groups: the Red team will examine how to attack the system under study. The Blue team will examine how to protect it. To enable the discussion, each team will have their own discussion areas. A common area will be used for the two teams to interact, which I will moderate. After we finish each study, we will summarize the results for all to see. I will then show how prior classes assessed security issues in these systems for comparison.

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)

There will be no exams in this class. Instead, there will be three written reports, a course project, and MANY opportunities for discussion postings. I expect all reports to be generated in a word processor and delivered in a standard format. I can read MS/Word or .pdf format. If you need to use any other format, please coordinate ahead of time. I don't want scanned, handwritten submissions. The readability and scan quality is too variable. The three written reports are due 2 weeks after they are assigned. They will be research reports on material drawn from the public literature. The first will deal with topics in wireless communications (not necessarily including security issues); the second will deal with topics in security (not necessarily involving wireless); the third will deal with topics in wireless security issues.

There will be predefined content required for the written reports and course project. Grading will be based on the quality of material presented within the categories defined. Try to make it easy for me to find the content to improve your chances of getting a good grade on any submission. All deliverables are to be ***individual*** work. This is a **graduate** course, even if you are an undergraduate taking the course as an elective. As such, neither graduate students, nor undergraduates enjoy the Honor System privileges afforded undergraduates in undergraduate courses. However, I do look to the Stevens Honor Code to define the ethical, professional behavior of students in the course. I have **zero tolerance** for plagiarism. Any failure to cite sources or blatant copying of material from cited or uncited sources will not be tolerated and may be referred to the Committee on Academic Integrity. If you draw a concept from someone else's publications, cite it. If you use the words of someone else unchanged, put them in quotes. If the words aren't in quotes I will assume you consider them to be your own.

The course project will be assigned in the 7th week of the course and will be due in the 12th week. Final presentations ***must*** be posted before the 13th week of the course so students (and the instructor) will have an opportunity to look them over and discuss them. Other than the presentation, no other submissions will be shared with other members of the class.

In the live versions of this course, students presented their class projects, which is obviously not possible here. Instead, I want everyone to prepare a brief presentation of the final report, using PowerPoint or equivalent, use speaker's notes annotations, as I have here, and send me the presentation ***BEFORE SATURDAY 11:59pm of Week 12!*** I will create the materials that get posted for the Week 13 presentation, so I need them in time. For compatibility, I will generate .pdf output and would either prefer you submit in .ppt or .pdf format. I do not use PowerPoint XP, so if you send me PowerPoint files, save them in a format no later than PowerPoint2000. If you send me .ppt format, I will be able to correct any last minute formatting problems before the presentation gets posted. If you send me .pdf format, be sure to proof read it carefully. I have found that wordy speakers notes often run off the bottom of the page and PowerPoint has no qualms about chopping off a lines at the bottom of the page when you output .pdf format.

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

I wouldn't have added this slide to the course if I didn't find it necessary. More than one student has received a grade of F in this course for submitting work that was not their own.

I thought I spelled out the issues pretty clearly on the previous slide, but in case the point wasn't completely obvious, don't even think of cutting and pasting words from one or more conference or journal papers and passing it off as your own work. It is perfectly acceptable to read several papers and summarize their key ideas entirely in your own words, but there has to be some value-added by the student for credit.

One other item: If I find substantial evidence of plagiarism in one assignment, I will generally choose to carefully re-examine ***all*** other material submitted by the offending student to see if there is evidence of plagiarism for those items also. In this case, I will similarly revise the grade for that assignment.

…. As I am revising these notes in preparation for the next semester, I feel the need to reiterate one point in bold: if you submit a paper that is plagiarized and I assign a grade of zero, don't waste my time or yours asking if you can resubmit it. Think about it this way: if I allowed resubmissions of plagiarized assignments, why shouldn't everyone see if they can get away with a plagiarized assignment. Think of the time they could save by simply copying someone else's work, rather than writing the ideas themselves. If they are successful, great. If they get caught, the ability to resubmit gives them a "Get our of jail free" card to try again.

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.

There's an expression about beating a dead horse, but just to make it perfectly clear that plagiarism will not be accepted in this course, I need to restate every possible variation. By the way, one of the first signs that a paper is plagiarized is when the source citation is unclear or ambiguous. I used to just take off points for improper citation, but that seemed ineffective, so I will simply not accept a paper for which the source is not clearly cited. Nor will I ask you to resubmit the paper. I will treat it as if you never submitted the assignment.

To be absolutely sure your citation of a source is proper, see the Library web site:

http://libraryhelp.stevens-tech.edu/cgi-bin/stevens_tech.cfg/php/enduser/std_adp.php?p_faqid=79&p_created=1049830601&p_sid=*shLNv6i&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD0xMTcmcF9wcm9kcz0mcF9jYXRzPSZwX3B2PSZwX2N2PSZwX3NlYXJjaF90eXBlPWFuc3dlcnMuc2VhcmNoX25sJnBfcGFnZT0x&p_li=&p_topview=1

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.

I can generally spot a plagiarized report pretty quickly. There are several tell-tale signs of plagiarized material that make it look very different from original student work. In Fall 2009, I started noticing a new trend – blatant copying of a previous submission. In one case the student who copied the work didn't realize that the copied Word or Powerpoint document had the original author's information still embedded in the document, but that wasn't how I found out the work was copied. I have saved every submission of every assignment for every course I have taught at Stevens. That, combined with Google Desktop (a very handy tool that everyone should try), makes it very easy for me to identify copied materials. After I identify the original source paper, WCopyFind makes it easy to see exactly how much material is original student work and how much comes from the source(s).

The bottom line: Do your own original work. You'll learn a lot more than by copying the work of others and you'll pass the course.

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.**

This slide lists only a few of the most remarkable miscitations. Here is another: a student cited a reference that properly included the author name and title, but the journal was "a prominent technical journal" and the publication date was in the future! If the student could actually see into the future, they had no place spending their time in class. They should have been trading stock based on tomorrow's values.

So what really happened? There were several papers listed as their references by the same author as the "to be published" paper. He was also the true author of the paper the student copied but did not cite. When I found the uncited actual paper, I discovered the identical list of references the student had used. They had careless copied the author's self citation of a paper the author knew had been submitted and accepted for publication, something the student could not know themself.

Improper references are signs of sloppy research and just make my job of detecting plagiarism easier.

And one last thing. I DON"T WANT A COPY OF THE PAPER YOU USED. (1) Sending it to me is not a substitute for a proper citation and (2) If I suspect plagiarism, I will be able to find it easily enough, anyway. Google, Google Scholar, Scopus, and Iexplore are more than I need.

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.

EE584
5/10/14

0-12/16

The Howe School requires that individual work be "pledged" much like work in undergraduate classes must be pledged. To meet the letter of this Howe School requirement without undue burden on students, please physically mail me a copy of the pledge when you electronically submit the first assignment. On the signed statement, reference the electronic copy and on the electronic copy, reference the signed statement. For subsequent electronic submissions, I will accept a 'typed' "I pledge on my honor…" with your 'typed' initials below the phrase.

I find that original work, no matter how poor the writing skills of the author, is much easier to grade than work that is clearly not the students. When I see work that is clearly not a student's own words or writing style, I am likely to be annoyed - I have to waste my time to identify the actual source of the words in order to justify to myself my decision to assign a zero grade. This often motivates me to examine other work of the student more closely, looking for other evidence of plagiarism.

While I reserve the option to use turnitin.com, I have found that Google™ searches of the web and previous submitted papers (using Google™ Desktop) work quite well. Various online databases are usually sufficient to identify plagiarized work, so please make everyone's life simpler and only submit your own original work.

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.

I am constantly obsessed with the risk of losing a homework submission, so I never delete anything. Unless I know where to file it, however, the chances of misfiling a submission and marking it as unreceived are pretty good. It would not be a bad idea to indicate the information above in the attachment as well as the subject of the email.

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.

I know everyone at Stevens has a heavy course load and would like to have a life. I try to be as flexible as the school allows, but there are limits! Familiarize yourself with the school policies and due dates for assignments in my course(s). Let me know ***in advance*** if you expect to have a problem and we can work something out.

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	

As you can see, the first 5 weeks of the course will consist of my “lectures” in the form of heavily annotated PowerPoint slides. I will finish

Week 5 with Case study 1, where I will go through the overall security assessment process that will be followed for the remainder of the class.

In Weeks 6-11, we will examine six different types of wireless communications systems, using the security assessment technique introduced in Week 5. The case studies were chosen to illustrate different types of real communications systems and to investigate a variety of security issues that might exist in those systems.

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

This is a list of the various topics to be discussed in the course. We start with a discussion of wireless communications – what is a wireless system, what are its characteristics, why is security an issue in particular.

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

We then spend a few weeks talking about security – what is security, what are the capabilities that could be built into a system, what are the security issues that are either unique to wireless systems, or might be exacerbated in wireless.

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

And finally, the case studies.

For each case study, the process is the same: I will define the system, the context and the application, the red team will describe possible attacks on the system, and the blue team will describe how to protect the system. We finish with a discussion of tradeoffs.

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

Email and discussion posts will be the primary means of communications for this course, so it would be a good idea to test it out before you really need to be using it. The Week 0 assignment is designed to exercise basic communications for the course, besides providing an introduction mechanism.