4005-747 Intelligent Security Systems

Hi guys,
Welcome to my Intelligent Security Systems class!

This class is a bit non-conventional in different aspects.

First of all, it merges together, or spreads across if you prefer looking from this angle, two clusters: intelligent systems, and networking and security. I believe this wide spectrum provides more opportunities for the curriculum, bringing it closer to the real life that usually does not recognize set-up borders, and for you as students giving more options to prepare yourself for your future work or study. On the other hand, methods of artificial intelligence open novel options for the development of the computer security tools. This area is growing up very quickly and according to the current predictions will continue to grow even faster.

Second, this class is designed as a "blended" course. It means that I will try to employ novel methodologies in teaching this class, again combining traditional teaching deliveries like lectures and class discussions with more work you will be required to do on-line.
The class time in this course will be reduced. **But you will have to spend more time on your independent study and on-line work.** This way you will have more flexibility with your study: you can do it any time, day or night and any place: the classroom or a sofa in your friend's apartment, wherever, whenever, whatever it will help you to study more efficiently and achieve better results!

The first thing you have to do is to read this letter and to follow up the instructions. Please, go to the course page on mycourses.rit.edu as soon as the ITS makes it available to students. Make sure that you do have an access to this page. If you do not and you are enrolled in this class, please, contact ITS immediately. This course will have a lot of activities conducted through mycourses. If you click on the Content bar you will see that all my lecture notes as well as project and assignment descriptions are already there. I am planning to conduct most tests online also. This class is designed as more oriented towards practical work and will have a big project. BUT so far I am not planning the final exams in this class. Please, think about it and get back to me by Thursday first week if you do not like it and want to get your finals back on schedule. I am sure we will be able to fix it.

One of the reasons why I selected the blended mode for this class is that I expect to have here the students with various backgrounds. Some of you have taken artificial intelligence classes, some have not. For those who are missing this knowledge I will deliver a refresher class. I will give you some background information about expert systems and neural networks, which you might need in order to do your project work and study of firewalls and intrusion detection systems. I am not requiring other students to attend these classes but of course, you are very welcome if you want to refresh your knowledge or to learn some more.

As you see from the content list on mycourses after refreshing some fundamental computer security concepts and terms, we will devote our time in this class to four main topics in computer security, or I should say four major topics in PRACTICAL computer security:

- Intrusion detection systems

- Firewalls,

- Virus detection and protections, and

- Biometrics access control.

(We will NOT study cryptography in this class. We have at least two other courses on this topic in our department, which I would definitely recommend taking to those who are interested in crypto). I believe that above topics cover almost the whole domain of practical computer security or I should say its major part. That is why I believe they will prepare you for your possible future work in security the best possible way. These four computer security mechanisms have something else in common: their tool's designs are commonly based on an application of AI methods. This is another major reason for me to design this course the way of merging intelligent systems and computer security. And there is another reason, as you see all those mechanisms are designated to protect the computer systems from the attacks. Those attacks may have different origins, both natural and artificial, but even with artificial tools used by hackers nowadays, at the end of the chain one can find a natural intelligence piece. And even if it belongs to a "script kid", the origin definitely has some intelligence. And it will become smarter and smarter with time. In order to compete with them in your job of a system and network protection, you will need a strong assistance of artificial intelligence methods.

Let us start our course discussion from the goals. Please, click on Learning outcomes and assessment on the content. You will see that my first intention is to advance your AI knowledge in computer security applications and in a practical security system design. We will use our lectures and your design and home work to achieve this goal. You will learn the structure and design of major computer security systems and tools. In this part, you will have to learn at least one tool and present it to the class. Your presentations will be scheduled over the first few weeks. Please, read below about it. This activity will help you to advance your presentation and communication skills also.

As you see I did not specify any required textbook for this class. My another goal is to promote more professional, not undergraduate student's, habits in your learning. I will try to encourage you to start moving from the use of textbooks to reading and using professional documents, like government and professional standards and other papers. This is the kind that you will be mainly reading and using in your professional life, not the textbooks. As you see I put a few of them on mycourses including four standards issued by the US National Institute of Standards and Technology (NIST) and others. I will require you to start reading them ASAP and I will encourage you to look for more information in computer security tools manuals and descriptions also. I do recommend you to start this reading even before out class begins. However, I realize that many of you might benefit from using a computer security textbook. I recommend J.M. Kizza Computer Network Security, Springer, (see some text and more info at books.google http://books.google.com/books?id=HsawoKBLZOwC&dq=Kizza+Computer+network+security&printsec=frontcover&source=bn&hl=en&ei=UTR8TN-pDMX6lwef0cnsCw&sa=X&oi=book_result&ct=result&resnum=4&sqi=2&ved=0CDIQ6AEwAw#v=onepage&q&f=false) or M. Bishop Computer Security, Art and Science, Addison-Wesley. The first book will be the closest to this class curriculum. I do not want you to spend much money on buying new books. If you have a book on computer security and it has chapters on intrusion detection, firewalls, access control and virus protections (practically all of them do), you are welcome to use it in this class.

In your first assignment, which is due VERY SOON, by the beginning of the second week (please, see mycourses for the exact date) you will have to review a few documents: the State of the Practice of Intrusion Detection that was published by the computer Security center at the Carnegie-Mellon University in 2000 and the Computer Crime and Security Survey conducted by the Computer Security Institute and FBI last year. My main goal for you in this assignment is reviewing the development of the both computer security violations and the protection tools available over the last decade. I want you to review some more information on computer security tools you can find on Internet.

PLEASE, START WORKING ON THIS ASSIGNMENT ASAP! Again, I am giving you some time later next week but please, download the assignment and the related documents from mycourses and start working!! There are five sections in this assignment. Please, complete all of them. In your answers, please, address all the questions specified in the corresponding part. Please, be specific and brief. In your answers, I am interested in YOUR analysis and opinions which should be based on your reading, not the quotes copied from the documents. The assignment will bring you up to 8 points in the course assessment.

Now please, download the assessment document on mycourses. You see that this class will be project oriented with half of all the points assigned for your **project** work. This project is designed as a **group project** but you can do your project either individually or in small groups of two-three students. The requirements for individual and group projects may differ slightly but generally will be very similar. Naturally, I will be expecting a higher quality submission from a group. Penalties for late submission/resubmission will be different: for individual projects it will be 5% grade reduction per day and for group projects it will be 10% grade reduction per day. As soon as you decide how you will do the project, go to the Groups on mycourses, select Projects and enroll yourself into one group. All group mates should select the same group number. Please, enroll yourself into a group even if you do the project individually. Otherwise, you will not be able to submit your work. If you do your project in a group, please, coordinate your efforts and do it on time. I suggest you to have an initial discussion about your work assignments and to schedule your work the way in order to finish at least a few days before the deadline. However, I am leaving all organizational aspects to you to decide. I have put the project description online. Please, read it and have your questions ready for me. This short quarter you will run ONE project, which consists of five parts. You will have to submit all the parts separately. Those parts will be assessed separately also. However, unless and until you finish part 1, you will not be able to start part 2, so PLEASE keep your work on schedule. The submissions deadlines will be distributed between weeks Three and Nine. Commonly, you will have about one week to finish up the next part after submitting the previous one. The first part is due by the beginning of the third week. I suggest you to start working on it very soon. In your project description first ten pages give you a general description. The requirements for part 1 starts on page 11.

As I said, you will be required to prepare and present to the class one computer security tool of your choice. Please, read Tools document from mycourses. You can prepare and run your presentation in small groups of two-three students. As you see there are a few groups. What I want you to do first is choosing the topic and your partners. First two groups will have to present SNORT. This is a very important and widely used computer security tool. This is why I want to spend more time on it and there are two groups, one and two, assigned to do it. These two groups will have to divide all presentation materials and subtopics between them and decide who presents what. And I want to have this presentation in week 2. Other topics will have a bit more flexibility with their choice. After you choose your presentation, please, enroll yourself into the corresponding group on mycourses. I want to start your presentation in week 2. So I want you to

finish choosing your topic and enrollment by Thursday in week 1. To do it click on the Group bar, then select Tools category (**not** projects at this stage), check the group you have chosen and do not forget to click on the save button. If there are already three students enrolled in this group, please, choose another one. You can do it any time from the time you are reading this letter. **Please, enroll yourself.** To help you to make your decision I have put more information into the Tools document on different tools and also some advise how to prepare your presentation. Your presentation will be worth of 5 points.

One of the features of this blended class will be on-line discussions, which you will be required to participate in. Your participation will be evaluated as a part of your assessment in this course. Please, remember to post your submissions here EVERY week. Do not wait until the end of the quarter. Your late submissions may not be accepted for grading. All discussion topics are divided into two groups:

1) Discussions of student's TOOLS presentations: there are seven topics here. Every student has to submit his/her contribution within FOUR days after the presentation

2) Project discussions –I am expecting your participation while you are doing a specific project part. You have to submit at least one entry to each project part discussion group. Your participation will be graded as a part of the project assessment. If you do not participate in a particular project part discussion or your contribution is not adequate, your grade for this project part will be reduced.

Please, read on the Discussions document for more information.

The last assessment component is the tests. Again, I am not planning the finals in this class and I am planning to conduct most tests online that might save you some time also. Our first test is currently scheduled on the second week Thursday. It will be devoted to computer security basics and quiz you on your knowledge of the basic concepts and terminology. This quiz tests an introduction (topic 3) and also is based on three documents given on mycourses in the assignment 1 section. You really need to study those documents to complete your assignment and to pass this test.

As you might expect from a blended course, all the submission will be done online through mycourses. PLEASE, PLEASE submit on time in order not to loose any point and please, do not wait until the last minute to avoid any problems with the network traffic and the mycourses server bandwidth.

Finally, please, look at the Schedule document, which lists almost all activities. As you see in week 2 you will have to take your test 1 and to submit the assignment 1. Also two groups will have to present on Snort.

And yes, you are right: There are **NO FINALS** in this class.

Please, start working NOW.
Please, contact me with any questions, suggestions, etc.
See you in my class.
Good luck!
L.Reznik