Project: Collaborative Techniques for Intrusion Detection in Ad-Hoc Networks

Main Assignment: Document, analyze and apply collaborative techniques for intrusion detection in Ad-Hoc networks

Task 1: What is Intrusion Detection?

Possible questions you can answer are:
1. What are the challenges and possible solutions of security in ad-hoc networks?
2. In general, what is Intrusion Detection? What is the problem that Intrusion Detection tries to solve?
3. What are the reasons behind the idea of Intrusion Detection?
4. What are the applications of such technology?
5. Provide a brief explanation of attacks commanded by intrusion detection.
6. How is intrusion detection different for ad-hoc environments?
7. How is the collaborative part carried out? How does it benefit the detection process?

Objectives of the task:
- To recognize specialized primary and secondary information resources.
- To access specialized information efficiently and recognize the kind of information obtained (conference, journal, book, book chapter, technical report, etc.)
  Why?
  o You must be able to distinguish the library resources specialized in the area of expertise in order to carry out effectively information searches for your research.
  o You must be able to list the specialized digital resources of the area
  o You must be able to list the journals or conferences that present a thorough treatment of the area
  o You must be able to recognize and give value to the information obtained through these searches
- To introduce you to the area of collaborative intrusion detection
- To examine and analyze information in order to compare and see opportunities for improvement of the solutions encountered
- To describe collaborative intrusion detection identifying functional blocks
- To identify processes involved in collaborative intrusion detection where systems or techniques need to be developed to become a reality
- To communicate your findings in a written and oral way.
- To organize and elaborate writing reports with your own ideas
  Why?
  o You must be able to communicate your ideas in a clear manner to an audience
  o You must be capable of writing a research report explaining concepts thoroughly.
You need to develop the skill to divide a whole into its parts in order to be analyzed or introduced to an audience or a reader.

Elaboration:

- You must research 3 to 5 papers on the concept of collaborative intrusion detection from academic journals searched through the Monterrey Campus library resources. No conference papers are accepted for this point.
- You can include books, or book chapters.
- If your discussion in the report follows a citation trail, extra points will be considered for your grade
- No WWW sources will be accepted.
- Elaborate a report where you answer the questions presented at the beginning of this document and also the questions that you formulate on your own. Organize such document according to the general instructions for the report.
- For the entire document, you must provide the bibliographic citations using the IEEE format. Download the document for this, and check page 4, Section IV.D http://www.ieee.org/portal/cms_docs_iportals/iportals/publications/authors/transjnl/auinfo07.pdf
- You will make a short powerpoint presentation in the classroom on a date indicated during the class sessions.

Reading and analyzing such information, you can answer the questions provided at the beginning of this activity. **Formulate your own questions.** For this you must choose one seminal source of the topic from the papers you researched. Provide the list of your own formulated questions in an appendix of your report. Your research on the topic of collaborative intrusion detection needs to be organized in a report of no more than 7 pages, with figures included, and organized and presented as described in the course web page in the general instructions for the term project: http://www.mty.itesm.mx/dmti/materias/e5051/projs.htm.