Andres Arjona

Topic 1
Authorization and Authentication Issues in The Generic Access Network (GAN/UMA)

The Generic Access Network, also known as UMA (Unlicensed Mobile Access) is a technology that enables interworking between WLAN networks and GSM cellular networks. The standard AAA model is based on SIM card. However, in order to make different models and flexible charging systems, authorization can be based on more information sent by the mobile client. Such data might include MAC address, GSM cell id, etc. When access to the system is made flexible in this way new problems arise that might include MAC spoofing, denial of service attacks, etc.

The purpose of this study is to pin point some of the security flaws that a flexible authorization model might be subject to. The topic is suitable for anyone interested in WLAN - cellular interworking. The standards are public and are available from 3GPP and UMA forum.

http://www.umatechnology.org/
http://www.kineto.com

Topic 2
Intrusion Detection Systems in Wireless Ad-hoc Networks - An Evaluation of Different Models

With so much advancement in hacking, attackers can eventually succeed and infiltrate the system. It is therefore important to monitor what takes place on a system and look for suspicious behavior. Intrusion Detection Systems are designed for that purpose.

The topic aims at making a survey of the work that has been done on the topic and provide a comparison of such systems and a potential recommendation based on what was learnt from the research.

A student who has at the least taken basic security courses might understand the schemes and their pros and cons better.

S. Axelsson, “Intrusion Detection Systems: A Taxonomy and Survey”, Tech. report no. 99-15, Dept. of Comp. Eng.,Chalmers Univ. of Technology, Sweden, Mar. 20, 2003.pp. 153–58.
http://www.cs.chalmers.se/~sax/pub/taxonomy.ps

http://www.ietf.org/html.charters/OLD/idwg-charter.html

Y. Zhang, W. Lee, and Y.-A. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM J. Wireless Net., vol. 9 ,no. 5, Sept. 2003, pp. 545–56.

http://www-static.cc.gatech.edu/~wenke/papers/winet03.pdf

Topic 3
RFID Security and Privacy Implications

Radio Frequency Identification (RFID) are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years—and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers.

The purpose of the study is to examine some of the approaches proposed for privacy protection and integrity in RFID systems and explain in what social contexts can they be applied.

The topic is not difficult and there is extensive material available. However it requires the student to be creative at the time of selecting the security approaches and finding different scenarios in which privacy is affected.

Privacy and security in library RFID: issues, practices, and architectures
http://delivery.acm.org/10.1145/1040000/1030112/p210-molnar.pdf?key1=1030112&key2=3539297511&coll=GUIDE&dl=GUIDE&CFID=404971&CFTOKEN=86769960

Security and trust in mobile interactions: A study of users’ perceptions and reasoning,
http://www.hpl.hp.com/techreports/2004/HPL-2004-113.pdf#search=%22Security%20and%20trust%20in%20mobile%20interactions%3A%20A%20study%20of%20users%E2%80%99%20perceptions%20and%20reasoning%22