****

Prof. J.P. Hubaux Addressed topics:

According to most technology pundits, progress in wireless and sensor networks will lead us into a world of ubiquitous computing, in which myriads of tiny, untethered sensors and actuators will communicate with each other. Information technology will thus deliver its most encompassing and pervasive accomplishment to mankind, promptly taking care of the needs and wishes of everyone.
Or maybe not. The described evolution is driven primarily by market forces; it vastly ignores the user intentions. Yet the recent history of the Internet has shown that these intentions can have devastating effects: for example, spam, viruses, "phishing" and denial of service attacks have unfortunately become commonplace; the misbehavior of a relatively small number of users is leading to a substantial inconvenience to the whole community. Similar or even worse misdeeds are and will be perpetrated in wireless networks.
Anyone would agree that forecasting the attacks against a network before its deployment is a very difficult task, and that the countermeasures are not purely technical, as the human dimension needs to be taken into account.
Yet the current practice consisting in patching the problem a posteriori, once it has been detected, is of course not acceptable; after all, we should be able by now to draw the lessons from many years of Internet security experience.
An additional problem is that the speed to the market is in contradiction with the design of a well-thought (and possibly standardized) secure architecture; the solution to this recurrent problem probably resides in the evolution of the designers' attitude, and therefore in appropriate education on this issue.

In this course, we will review the fundamental questions related to this problem:
How are users and devices identified? How to establish a security association between two wireless peers? How can packets be securely and cooperatively routed in a multi-hop network? How to guarantee the fair share of bandwidth between nodes located in the same radio domain? And, above all, how is privacy protected?
We will treat each of these questions from a theoretical point of view and illustrate them by means of concrete examples such as mesh, vehicular, and sensor networks. Whenever necessary, we will introduce the security and game theoretic concepts we will need.

The material for this course will be extracted from research papers and from a book in preparation
with Levente Buttyan, from Budapest University of Technology and Economics.

****

Prof. G. Tsudik Addressed topics:

This short course will touch upon several aspects of timely and interesting security issues in wireless and mobile networking.

Human-Assisted Wireless Security

We will start by discussing the seemingly trivial problem of securely associating or pairing wireless devices (e.g., sensors, phones, and PDAs). Since this almost always involves a human user, we will consider the user impact/burden as well as various issues in usability of security-related HCI. On a related note, many security and privacy proposals for wireless RFID tags, while ostensibly aiming to help the users (consumers), have not considered user perception. It is a sad but incontrovertible fact that most people consider security to be a burden and a nuisance; moreover, they consider "invisible" (wireless) security measures to be dubious in nature since, especially, in the context of sensors and RFID tags which have no user interfaces whatsoever. We will consider human involvement in security-related activities such as device pairing and RFID privacy, among other things.

Privacy in Wireless Networks

Much of the research in security for wireless and mobile networks focused on traditional security issues such as authentication, key distribution, certification as well as securing applications such as routing and location verification. However, comparatively little has been done in terms of privacy. In the electronic society where privacy is continuously under assault from Big Government, Big Business and Spammers/Phishers/Hackers, we need to consider privacy implications of all services and applications. In the wireless/mobile world, privacy is even more fragile than in wired networks. We will first examine how familiar everyday techniques and protocols inadvertently (or by design) reveal too much information. Next, we will attempt to construct and evaluate privacy-preserving counter-measures.

Re-considering Secure Routing

Within the last decade, secure routing in wireless MANETs has been a fruitful and popular research topic. Many efficient and interesting protocols/techniques were designed which are appropriate for different types of routing protocols. One of the key concerns and priorities was the minimization of cryptographic overhead, especially that stemming from public key cryptography. (Bandwidth and storage were not treated with the same priority.) We will investigate prior work in light of bandwidth overhead and recent developments inc faster/cheaper/shorter public key primitives, especially, digital signatures. We will discuss new trends in MANET routing and a closely-related topic -- secure location verification.

****