

Erasmus Exchange ETH Zürich, Switzerland

September 2015 - February 2016

Security of Wireless Networks

prof S. Capkun

Covers everything about wireless networks: from WiFi till GPS. The course itself focuses on how attackers can break confidentiality/integrity in wireless networks and how they can interrupt connection (p.e by jamming). As you are going to study the behaviour of radio signals, it might be useful to have some basic knowledge about Fourier Transformation and the behaviour of a wireless signal in space (eg. lower frequencies reach farther than higher frequencies), but it is in general not required for the course itself. Topics covered: round-trip delay (eg. passive entrance systems), GPS spoofing/secure localization, GPS jamming, physical layer security, anti-jamming broadcast, broadcast authentication, key distribution, secure routing, GSM & UMTS, WiFi (IEEE 802.11) security.

Together with the course mandatory lab sessions are organized where theory is applied in practice. One of the project you pe. have to do is creating a directional WiFi antenna.

System Security

prof S. Capkun, prof A. Perrig

This courses is target on the security of a system on it's whole (pe. a laptop). Different crypto algorithms (AES, RSA, Triple DES) will be discussed and how they can be broken. The course itself starts with side-channel attacks (p.e. timing attack on RSA and cache-time attack on AES). After that, you'll dive deeper into the internal working of operating systems on assembler level. Here you'll see how buffer overflow and ROP attacks can be applied to get root access. Every week you'll get an assignment in which you'll have to get under the skin of a potential attacker. Creativity is very useful here.

Network Security

prof S. Frei, T. Dübendorfer, A. Perrig

A very general course covering a lot of topics without going in too much technical detail. Topics like botnets, malware, identity fraud, DNS spoofing, firewalls, SQL-injection, XSS attacks, etc. will be covered. A must if you like some general knowledge about potential vulnerabilities in networking, websites, etc. without having to sort out and deal with technical details.

Mobile and Personal Information Systems

prof M.C. Norrie

Is a course for creative people. *"This course examines the impact of the different forms of mobility and collaboration that systems require nowadays and how these influence the design of systems at the database, the application and the user interface level. For example, traditional data management techniques have to be adapted to meet the requirements of such systems and cope with new connection, access and synchronization issues."*

The course starts with all the different forms of context-awareness, which is way more than location-only CA. Based on CA, the course elaborates further on how that CA can be used in the environment surrounding us. For example on Ambient (informing a user in a non-intrusive manner) and Pervasive (= public) displays. The course is mostly about abstract ideas and how to apply them in current/future environment. As such more technical topics (such as a database for moving objects) are also covered. Every now and then a break-out session is held where you and your team can brainstorm about possible solutions (pe. what to display on a pervasive display given the current context).