Date of Issue 10th May 2006.

Bachelor Assignment

University of Twente (EWI/DACS) and Twente Institute for Wireless and Mobile Communications BV (WMC)

Experimental Analysis of a Secure Bluetooth PAN Formation Protocol (PFP)

This bachelor's assignment will be done in the context of Personal Networks. A Personal Network is a new concept related to the field of pervasive computing. It comprises a core consisting of a Personal Area Network (PAN), and is an organization of all computers, devices, and network services used by an individual in a *single* logical network.

The first step in creating a Personal Network is therefore to build the PAN. The Bluetooth PFP protocol provides a secure means to create this PAN. The goal of this assignment is to setup and analyze the security and performance aspects of the given PFP protocol. The test bed will consist of a number of devices, using BlueZ, the well known Linux Bluetooth protocol stack. Although the student is not expected to write C code, having a good understanding of the C language is a plus. The PFP protocol to be analyzed consists of a client/server PFP module which uses authenticated Diffie-Hellman.

The aim of this assignment is to analyze the given PFP protocol, and produce a prototype for demonstration. As such the assignment has both theoretical and practical components. The student will get a chance to study relevant aspects of Cryptography, Bluetooth, and Personal Network features such as device imprinting. Finally, depending on the outcome, there may be an opportunity to continue related work for a Masters thesis.

Duration : 3 Months
Location: WMC Enschede (http://www.ti-wmc.nl)

For more information, please contact: Simon Oosthoek: simon.oosthoek@ti-wmc.nl
Assed Jehangir: a.jehangir@utwente.nl