Research report for the STSM of Patrick Maillé
Host: FTW Vienna, Austria (Peter Reichl)

The STSM has been devoted to ideas exchanges regarding security issues in telecommunication networks, and possible modeling of those situations using the framework and tools of noncooperative game theory.
The main outcomes of the STSM can be summarized into three points.

1) ***State-of-the-art***: Patrick Maillé and Peter Reichl (together with Bruno Tuffin, French MC member) have carried out a survey work on the literature applying game theory to network security. The STSM has enabled to improve the efficiency of that work, which was a first necessary step toward further research work on that topic. The literature survey has been submitted as a chapter proposition for a book "Performance Models and Risk Management in Communication Systems", to be edited by Nalan Gulpinar (UK MC member) and published by Springer. The title of the proposed chapter is “Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management”.

2) ***Discussions with FTW security specialists***: Peter Reichl and Patrick Maillé had very instructive and insightful discussions with several researchers of FTW that work in network security (Andreas Berger, Ivan Gojmerac, Esa Hyytiä, Oliver Jung). The objective was to get an overview of some possible attacks, and pick out some trade-offs in the strategic choices of attackers and defenders in those situations, that we could afterwards represent in a game-theoretical model. Those discussions highlighted for example the attacks based on “botnets” (networks of computers –“bots”- hijacked by an attacker, that can be used as an “army” to launch a distributed denial of service attack). To carry out an attack, one entity may rent a given number of bots at a given price. Such an economic model from the attacker point of view does not appear in the security literature, and can be used in a game-theoretic model.

3) ***First steps toward a new model***: Peter Reichl and Patrick Maillé spent some time together to define a game-theoretical model of botnet attacks, where the attacker’s utility would be a trade-off between the damage done to the target and the cost of renting the bots (the strategic variable being the number of bots to use). From the defender’s point of view, the strategy would consist in investing on security protection, and the objective would be to minimize the suffered damage and investment costs. A sequential game model played over several time periods was discussed, where each participant can update its strategy based on the observations of the previous periods. Such a model seems quite difficult to solve, we still need to refine it to represent some realistic situations, while possibly being solvable analytically.