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

The STSM has been devoted to developing models on network economics focusing on security aspects, and exchanging ideas about anomaly detections. The main outcomes of the STSM can be summarized into three points, and can be seen as a follow-up to Patrick Maillé's STSM last December.

1) ***Designing a game-theoretic model for providers preventing intrusion***: Bruno Tuffin and Peter Reichl (together with Patrick Maillé, member of WG4) have defined a mathematical model describing the competition between security service providers. In that model, users choose their provider from a combination of price charged for the service and expected loss in case of intrusion. In that model, the probability of intrusion depends on the popularity of the applied security (the so-called externality). The distribution of users among providers follows Wardrop's principle (taken from transportation theory), and is shown to exist and be unique. On top of that user equilibrium, the pricing and quality of security game is defined and can be solved. The model (the above two steps game) is explicitly defined and should result in a common publication.

2) ***Designing a game-theoretic model against malware***: similarly to the above case, the partners have defined a two steps game between providers looking at defenses against worm propagation. In that specific situation, the externalities are different, because they depend on propagation speed, and recent results characterizing them (making use of random graph theory) can be used. Here too, he whole model has been explicitly defined during the STSM.

3) ***Discussions with ftw. on anomaly detection***: An additional security-related discussion with security specialists at ftw. was focussing on anomaly detection based IDS/IPS for SIP/IMS networks. Based on the recent development of a flooding detector at ftw. which uses the so-called Hellinger distance as a metric for measuring the difference between regular traffic as collected during a training phase and operational traffic which might be subject to a flooding attack. As, however, the Hellinger distance approach requires careful finetuning of the corresponding parametrization, the discussions during the STSM have led to identifying potential further candidate metrics which could be more robust and will be further explored for potential integration into ftw.'s flooding detector.