## Session 11 Discussion
## Recorded by Lionel Montrieux, NII, Japan

Requirements-Driven Mediation for Collaborative Security by Amel Bennaceur:

Amel talks about collaborative security, i.e. the use of everyday technology to improve security.

One of the challenges of collaborative security is to make multiple, heterogeneous, software-intensive components collaborate with each other to meet security requirements, even though they may not have been designed for it. This situation is typical in ubiquitous computing.

Collaborative security builds on two research areas: adaptive security, and collaborative adaptation. The former allows her to reason about assets, threats, attacks and vulnerabilities. The latter allows her to reason about dynamic discovery and composition. She tries to unify these two areas, using an approach based on mediators.

Her framework (available on github) uses feature models, behaviour models, and KAOS models. Features and behaviour are strongly coupled, in the sense that a particular feature configuration will allow only a subset of behaviours. This allows her to simplify the components' behaviour depending on the feature selection, before using mediators to combine them in a way that satisfies the requirements.

Amel concludes with a few open questions related to her framework. Is it only applicable to security, or can it be generalised? What are its limitations, especially around mediators? How about users? Should they just be considered as another component? How to explain the framework's decisions in a meaningful way?

An Adaptive Framework for Individual Privacy by Nobukazu Yoshida

Yoshida-san starts off with a description of the Android application security model, and points out how it does not give users sufficient control over their data. Specifically, users cannot finely control their data according to their own privacy preferences.

He proposes a privacy-aware framework that allows users a better level of control over how their data is used. He illustrates his framework with an example, where health and fitness data is collected by a service, and used to provide users with expert guidance from personal trainers, monitoring and evolution of the measurements taken, etc. In Yoshida-san's example, users are able to select how much data they want to share, with whom, and at which granularity level. It is understood that sharing more, and more fine-grained, data will make the service more useful, but also expose the user to more potential privacy breaches. Yoshida-san seems to consider privacy breaches to be the result of misuse by third parties of data they had access to or were able to infer, as opposed to data "stolen" by malicious agents

exploiting the system's vulnerabilities.

In Yoshida-san's framework, context is important. Changes in context may have an effect on users' privacy, and hence the framework is able to react to that.

The framework is based on risk assessment, where the likelyhood and consequences of breaches are assessed in order to produce privacy requirements for each user. Users need to input their privacy preferences, where they describe (on a scale) how much they would be impacted by the disclosure of a particular piece of information to a particular category of third parties. A service specification is then selected, where a high value service will carry more privacy risks, and a low value service will carry less privacy risks.

The framework is adaptive in the sense that, from a service specification, a controller measures changes in risk for each user, and produces service behaviour models.