ADaCoR Panel Discussions

Day 1: Risk Management

Duration:	15:50 – 16:50
Moderator:	François Thill
Participants:	Carlo Harpes (*itrust consulting*), Christian Probst (*Technical University of Denmark*), Sjouke Mauw (*University of Luxembourg*), Axel Tanner (*IBM*), Alexandre Dulaunoy (*SMILE G.I.E.*), Gérard Wagener (*SMILE G.I.E.*)

The discussion started with the question whether the presented methodologies are able to describe, or even detect, absurd attack scenarios. Indeed, underlying models and frameworks usually expect an attacker to act rationally, and as such, might not be able to understand the situation if he does not. As a (humorous) illustration, F. Thill chose the example of the scene from "Monty Python and the Holy Grail (1975)", where King Arthur and his companions were puzzled by the attacking mechanisms, a cow catapult, of the French castle.

The panel members admitted that their models would not yield the 'cow catapult' as a potential threat, unless the risk assessor has identified the risk of cow catapults, but argued that they focus on more general risk scenarios, which a security expert would then have to interpret appropriately. In fact, the actual goal of a methodology is to systematise risk management; it is the individual risk analysis that will be specific to a given organisation, not the framework. In other words, tools such as Attack Defence Trees, *ADTool* or *TRICK Service* are only means to support the risk assessor to identify the 'cow catapult' threat, but will probably never identify it on its own.

Similarly, attack trees are not a direct mean to find threats, but are part of a larger brainstorming process, paving the way for a subsequent risk analysis. In fact, attack trees permit to highlight the technical details of an attack, assisting in the understanding of the attack, but clash with the fact that risk analyses operate on a much higher level.

The participants all agreed that *collaboration* and information sharing is the key point for achieving a high security level. Some organisations, especially those that are not specialised in the security domain, are often unaware of the risks they are facing. Nevertheless, (large) companies do not always have or see the interest in publishing security information, especially if it comes to *how* to implement security. To a certain extent, their behaviour is comprehensible, since providing security is often part of their business strategy (this is especially true about data centers). The question arises whether the public sector (or even the legislator) should intervene in this case to assist SME's in the securing process.

Another huge problem which currently persists is the overestimated trust in black-box security appliances, which often turn out to be not so effective. In fact, they sometimes even introduce new vulnerabilities, so that one would be better off by dumping them.

Moreover, the diversity of security appliances is generally very low, which cause bugs in these implementations to have a huge impact, because everyone is using the same product. Famous examples include OpenSSL (think of *Heartbleed*) and operating system kernels.

F. Thill concludes by thanking the panellists and the audience for the very interactive discussion.

By Steve Muller, *itrust consulting*.