File 20110118.1950: Notes from Shamal's paper 'Bringing mis-usability home: finding and resolving mis-usability with Mis-usability Cases' [2].

Value scenarios [4] '...vignettes which describe the systematic effects of a system to both direct and indirect users over an extended period of time. Value Scenario [*sic*] describe both the positive and negative systematic effects of a technology without considering users as malevolent; they do so by describing negative impact of forgetting about certain values, such as prejudice and inequality.' [2, p. 2].

'Not all software systems are as divisive, pervasive, or long-running as those typically described by Value Scenarios.' [2, *ibid.*].

'...elicitation of vulnerabilities...' [2, handwritten note, §2.3, p. 2].

'Misuse cases act as validation for this risk analysis exercise. If a risk is valid then a believable Misuse Case can be written which describes how the attack associated with the risk exploits the risk's vulnerability to harm the endangered or exploited assets.' [2, p. 2] I have to say that sounds exactly like something Dr Ivan Fléchais would say.

There were a few bits in this paper that I wanted to remember for later use in my dissertation:

1. 'Explicitly assigning the Obstacle to a Role mitigates the possibility of *diffusion of responsibility*, where unresolved problems are ignored because no single agent is responsibility [*sic*] them' ([1], cited in [2, p. 4, § 3.2]).

2. Use this way of rationalisation in the methodology section of your dissertation:

   > Ideally, both security and usability should be designed into a system at a very early stage. Our involvement with the project commenced not at its initial inception, but once the main architecture and component sub-systems had been outlined. Moreover, despite the fact that empirical data from representative stakeholders could have made an invaluable contribution to the analysis to be carried out, the project scope was such that data could not be collected from prospective researchers or Data Managers. It was, therefore, necessary to use the portal development team, who had spent considerable time working with the different user communities, as proxy users. Therefore, in lieu of access to real users, we made best use of the design artifacts and project developers that were available.

3. I thought the following Mis-usability case was written in an interesting style. This is the *Batch import sensitive meta-data* Mis-usability Case:

   > Brian had spent most of the morning preparing data-sets ready for export to various sources. Some of the meta-data was for deep [sensitive] metadata for local databases, while others were shallow [summarised] meta-data targeted for the MDR. He hoped to use standards and guidelines on the gateway, but he was disappointed by the lack of anything useful that would help him. Nevertheless, Brian managed to organise his meta-data into the layout he managed to induce from some the XSLT scripts he was able download. After finally finishing the preparation of his data-sets and meta-data, Brian created the mapping files needed for the data import process. Fortunately, most of them were very similar so most of the files he used were based on an initial template he created for one of his datasets. Brian entered a URI he had been provided for uploading meta-data to the MDR, and logged in using his Data Manager credentials. Brian then specified the mapping file corresponding to the meta-data he wanted to upload and hit the Upload button. Several minutes after clicking the Upload button, Brian received a message from the portal indicating that the meta-data had been uploaded.

   [Emphasis in original]

   'Although not written in the Mis-usability Case itself, Brian accidentally uploaded a mapping file for public meta-data, which points to sensitive meta-data. As a result, sensitive meta-data has been made publicly available on the portal.' [2, pp. 5–6]

4. And finally, on the topic of **risk management**, the following information from [3] is highly relevant:

   > 'Although risk management approaches deal with the idea of *transferring* unmitigated responses to one or more agents...' ([2, p. 7], citing [3]).

and this:

> ‘Flechais [*sic*] and Sasse (2009) argue that assigning liability motivates the assigned stakeholders. . . ’ [2, § 5.2, p. 7].

References

[1] J. M. Darley and B. Latané. Norms and normative behaviour: field studies of social interdependence. In L. Berkowitz and J. Macaulay, editors, *Altruism and Helping Behaviour*. Academic Press, 1970.

[2] Shamal Faily. Bringing mis-usability home: finding and resolving security mis-usability with mis-usability cases. In preparation for BCS HCI (submission deadline: 21st January), 2010.

[3] I. Fléchais and M. A. Sasse. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-science. *International Journal of Human–Computer Studies*, 67(4):281–296, 2009.

[4] L. P. Nathan, P. V. Klasnja, and B. Friedman. Value scenarios: a technique for envisioning systematic effects of new technologies. In *CHI '07: extended abstracts on Human factors in computing systems*, pages 2585–2590, New York, 2007. ACM.