An Introduction to IRIS

Shamal Faily, Ivan Fléchais
Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD, UK
{shamal.faily,ivan.flechais}@comlab.ox.ac.uk

I. Overview

Media reports suggest that, despite recent advances in software, security, and usability engineering, we remain unable to design and build systems which meet their specified functionality, are usable by their intended operatives, and remain secure in the face of unintentional and intentional changes to the environment.

The IRIS (Integrating Requirements and Information Security) framework was devised to address the problem of designing systems which are both secure and situated for their operational environments. This framework consists of two components:

- An integrated usability, security, and software engineering design process,
- Tool-support to support this process.

II. The IRIS Design process

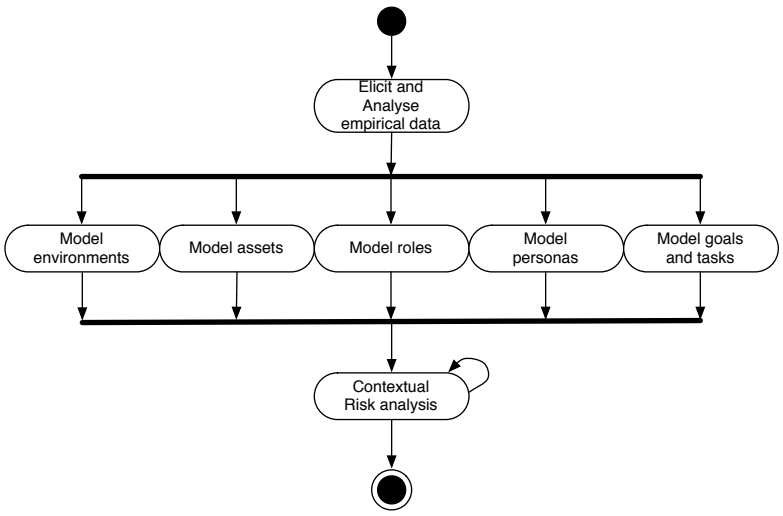

Fig. 1. IRIS Design Process

The design process, illustrated in figure 1, begins by eliciting data about the following concepts

- Operational environments,
- Organisational assets,
- Roles held by participants within the system,
- Personas of participants carrying out these roles,
- Goals held by personas, together with the tasks carried out to achieve these goals.

Some of this data is elicited from an initial 2-3 hour scoping workshop. While primarily a brainstorming session, the objective of this workshop is two-fold. First, by identifying key assets, roles, goals, and tasks, participants will guide where, when, and who will take part in subsequent elicitation activities. Second, differences of opinion between participants can be identified at an early stage by exploring the perceptions held about these concepts.

Following the scoping workshop, *contextual interviews* are scheduled for selected participants within their work setting. Contextual interviewing involves observing participants as they undertake everyday work and, periodically,

asking questions to gain a better understanding of the tasks being carried out. The interviewer makes notes and an audio recording of each interview, which lasts approximately 2 hours. Within 48 hours of each interview, an interpretation session is held, where the interview data is analysed and categorised to determine assets, roles, and tasks.

The remaining stages take place during a number of facilitated workshops, supported by the IRIS software tool (section III). During these 3 hour workshops, the results of previous analysis are presented and validated with participants who, like the scoping workshop, are representative of different environments of use. The IRIS software tool models the results of this analysis, and guides the process of risk analysis, risk management, and security countermeasure design for these different contexts. Because countermeasures introduce assets into one of more contexts, risk analysis continues until participants are satisfied that all major risks have been appropriately mitigated.

III. IRIS Tool Support

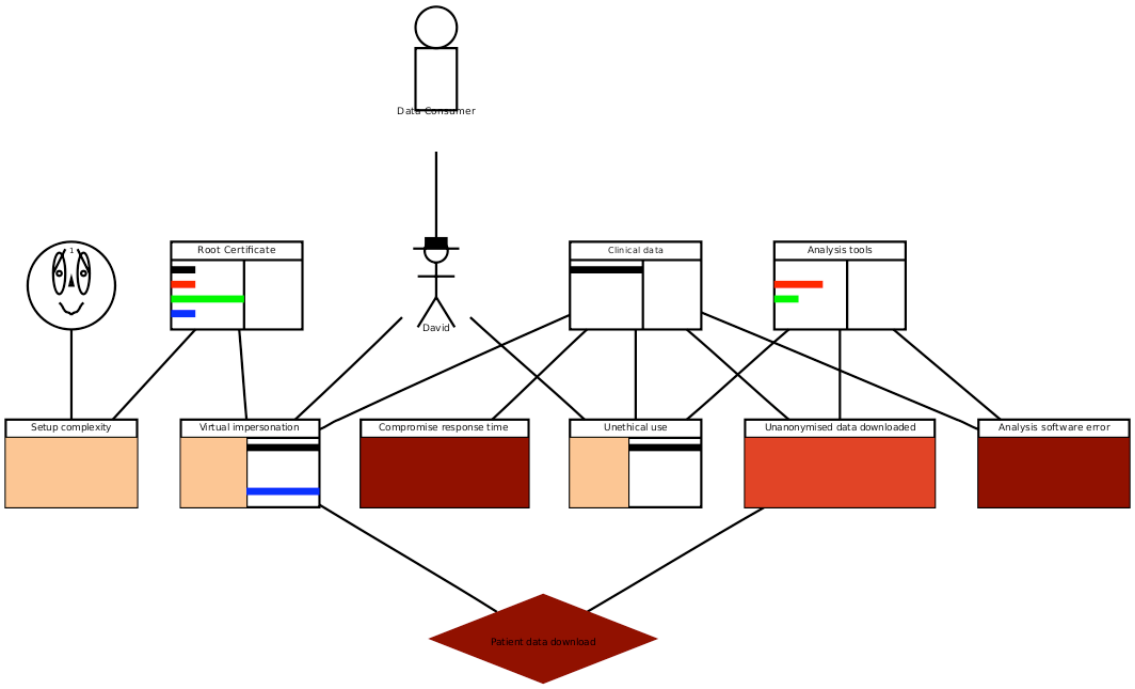

Fig. 2. Visualisation of risk analysis within IRIS

As contexts of operation are explored, an increasing number of security and usability concepts must be modelled and analysed. Without tool-support to do this, identifying the security and usability impact of design changes will become an unsustainable.

As well as providing a management tool for data elicited by the design process, the IRIS software tool (figure 2) can generate visual models showing the relationship between the different usability, security, and requirements artifacts within each context.

The tool can also visualise multi-attributes nodes within these views. Shades of red are used to visualise the properties and impact of threats, vulnerabilities, and risks; shades of blue are used to visualise the usability of a task. The quality of a requirement is codified using Chernoff Faces [1]. These allow multiple values to be encoded by exploiting the human ability to detect small changes in facial characteristics. Eye brows are used to represent the completeness of a requirement, eye shape is used to represent the presence of an imperative mood in the description text, and the mouth is used to indicate requirement ambiguity. The more ‘friendly’ the face looks, the higher the quality of requirement.

References

[1] H. Chernoff, “The use of faces to represent points in k-dimensional space graphically”, *Journal of the American Statistical Association*, p. 68, 1973.