2009 17th IEEE International Requirements Engineering Conference

Context-Sensitive Requirements and Risk Management with IRIS

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

Abstract

Many systems are not designed for their contexts of operation. Subtle changes to context may lead to an increase in severity and likelihood of vulnerabilities and threats. The IRIS framework integrates the notion of context into requirements and risk management, by means of an integrated meta-model, design method, and software prototype. By applying this framework, requirements and risk analysis can be better situated for system contexts of operation.

1 Introduction

Many systems have not been designed for their *contexts*, their environments of operation; this is evident from regular media reports on security failures. Defeating system attacks in one physical location is no guarantee of success when the system is physically situated elsewhere. Similarly, a vulnerability may only become evident by considering the system in another temporal or cultural context, such as several years after initial commissioning, or testing with different communities of users. Risk analysis can be used to inform security requirements and design, and techniques exist for eliciting and reasoning about assets, threats, and vulnerabilities within a given environment. Unfortunately, such analysis is difficult, not only because of the sheer number of variables contributing to a single risk, but also because contexts of use can be combined. Maintainers of the Vélib' public bicycle rental programme in Paris discovered this when, despite the success of a similar system in Lyon, theft and vandalism became endemic after 18 months of operation [1].

Elicitation techniques exist for exploring system contexts and eliciting requirements about them, together with security engineering approaches for designing for threats, vulnerabilities, and risks within these contexts. However, approaches for integrating techniques from these disciplines into a coherent, practical framework remains an active research topic. The elements for such an approach exist, but without explicit support for the notion of context, reasoning about changes introduced by controls within these information-rich environments remains a challenge.

2 Our approach

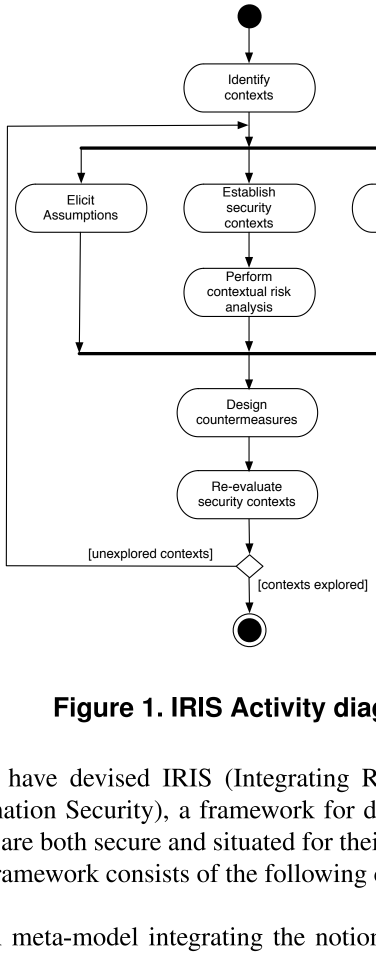

Figure 1. IRIS Activity diagram

We have devised IRIS (Integrating Requirements and Information Security), a framework for designing systems which are both secure and situated for their contexts of use. This framework consists of the following components:

- A meta-model integrating the notion of context with concepts from requirements and risk management.

1090-705X/09 $25.00 © 2009 IEEE
DOI 10.1109/RE.2009.54

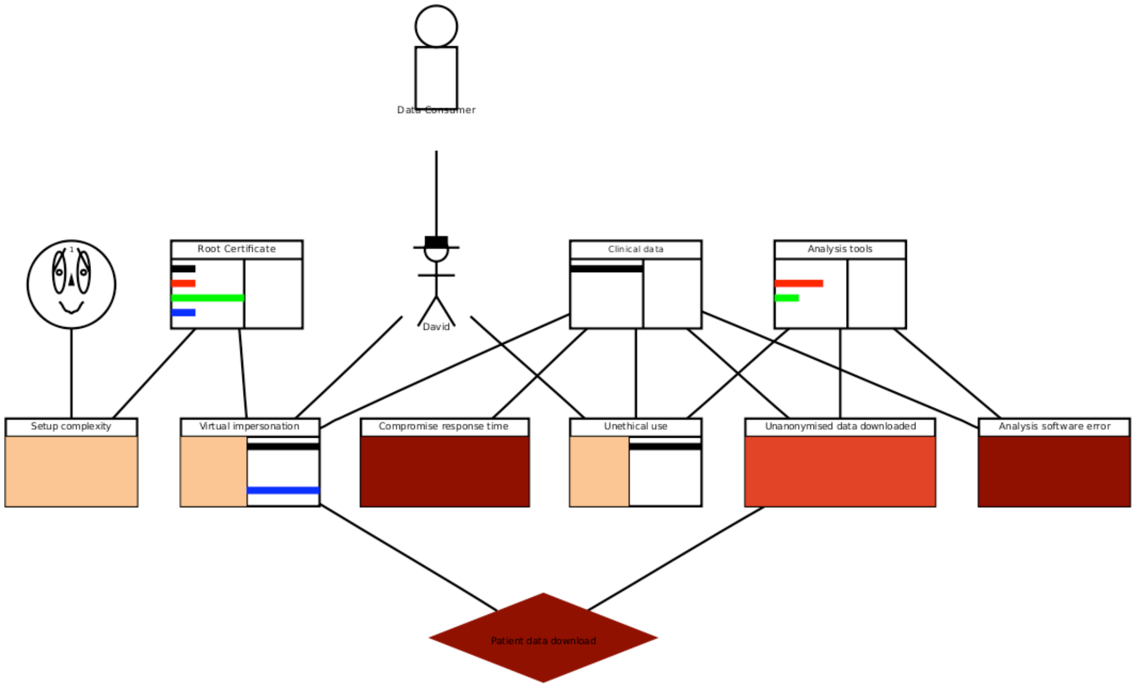

Figure 2. Requirements and Risk visualisation

- A user-centered design method for eliciting requirements and designing security controls situated for their contexts of use.
- A software prototype which implements the IRIS meta-model, and supports the associated design method.

The IRIS meta-model builds upon existing security requirements engineering meta-models in several ways. First, allowing confidentiality, integrity, availability, and accountability values to be associated with assets, threats, and countermeasures, we can examine how these vary between contexts, and multiply when different contexts come together. Second, we support the association of roles to both stakeholders and attackers in different contexts. To these roles, responsibility for responding to risks or managing countermeasures can be assigned. By allocating responsibilities to roles, and tracking these in different contexts, stakeholders with an excessive number of responsibilities can be identified, together with roles dispersed among several stake-holders, and roles shared by both attackers and stakeholders.

The IRIS design method, illustrated in figure 1, builds upon previous work on user-centered security design. IRIS incorporate processes of eliciting empirical data about contexts of operation, to support development of stake-holder and attacker personas. These personas enliven narratives exploring instances of system use and misuse within the various contexts. Therefore, rather than using scenarios to explore branches from the normal-course, alternative courses are considered as scenarios within a given context of operation.

The IRIS software prototype supports integrated and visual requirements and risk management. The tool dynamically generates a visual representation of the requirements and risk management artifacts, together with the traceability relations between them; this is illustrated in figure 2. Information visualisation techniques are used to code nodes within the visual model. For example, the quality of a requirement is codified using Chernoff Faces [2]. 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] BBC News. Thefts puncture Paris bike scheme. `http://news.bbc.co.uk/1/hi/world/europe/7881079.stm`, 10 February 2009.

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