Formal evaluation of persona trustworthiness with EUSTACE.

FAILY, S., POWER, D., ARMSTRONG, P. and FLÉCHAIS, I.

2013

Formal Evaluation of Persona Trustworthiness with EUSTACE

(Extended Abstract)

Shamal Faily, David Power, Philip Armstrong, and Ivan Fléchais

Department of Computer Science, University of Oxford
Oxford UK OX1 3QD
firstname.lastname@cs.ox.ac.uk

Abstract. Personas are useful for considering how users of a system might behave, but problematic when accounting for hidden behaviours not obvious from their descriptions alone. Formal methods can potentially identify such subtleties in interactive systems, but we lack methods for eliciting models from qualitative persona descriptions. We present a framework for eliciting and specifying formal models of persona behaviour that a persona might, in certain circumstances, engage in. We also summarise our preliminary work to date evaluating this framework.

1 Motivation

Personas —narrative descriptions of fictional users based on archetypical user behaviour — are commonly used when building interactive systems [1]. However, many insights about these personas may be hidden in these description or related qualitiative data. When properly identified and analysed, this data might suggest untrustworthy behaviour that personas might engage in. Unfortunately, the volume of data underpinning personas means we cannot rely on casual inspection alone to find such behaviour. Moreover, given that personas are grounded in qualitative data, devising formal models of interactive behaviour that software tools can verify is difficult.

Although usually used as a verification technique, Communicating Sequential Processes (CSP) [2] has also been used for modelling patterns of interaction at higher levels of abstraction. It is precise enough for its specifications to be formally checked, yet also expressive enough to deal with the nuances of human interactions. Jirotka and Luff [3] have demonstrated how CSP can be used for modelling and reasoning about interactions and behavioural norms associated with multiple people. Using model checking technology, it is possible to verify such interactional specifications modelled in CSP to determine whether these are valid refinements of a secure system specification. Deriving behavioural characteristics of personas using such refinements should allow us to investigate whether their behaviour satisfies a system's safety and liveness properties, or are free from divergent behaviour; this may indicate behaviour that betrays the trust placed by the system on the user.

2 Approach and Preliminary Results

We devised the EUSTACE (Evaluating the Usability, Security, and Trustworthiness of Ad-hoc Collaborative Environments) framework to formally identify untrustworthy behaviour hidden in persona descriptions. This entails checking whether CSP descriptions of persona behaviour are valid refinements of a CSP system specification. To apply the EUSTACE framework, we carry out four steps. First, we create an initial CSP system specification satisfying an agreed requirements of interest. Second, using the Persona Case framework [4], we code persona data based on the specified events, and elicit new events that personas might engage in. Coding is guided by Riegelsberger's trusted interaction framework[5], which provides sensitising questions about intrinsic and contextual trust properties. We also draw relationships between codes which, in turn, may lead to the elicitation of new codes in addition to relationships between existing ones. Third, cogent fragments of persona behaviour elicited from these relationships are annotated using CSP process descriptions. Finally, to evaluate whether persona behaviour in a specific context diverges from the system's intended behaviour, these implied descriptions are refinement checked against the system specification. These disparate CSP descriptions are combined based on specific context events of interest present in the individual implied specifications.

We extended the open-source Computer Aided Integration of Requirements and Information Security (CAIRIS) requirements management tool to support the first three steps of the EUSTACE framework. We have also built an interface to the FDR model checker to automate refinement checking against the implied specifications generated by CAIRIS. We have validated the feasibility of the framework by analysing personas of application developers and end-users to identify ways installing apps on mobile phones might be exploited.

3 Acknowledgements

The research was funded by the EPSRC *EUSTACE* project (R24401/GA001).

References

1. Cooper, A.: The Inmates Are Running the Asylum: Why High Tech Products Drive Us Crazy and How to Restore the Sanity (2nd Edition). Pearson (1999)
2. Hoare, C.A.R.: Communicating sequential processes. Prentice-Hall, Inc. (1985)
3. Jirotka, M., Luff, P.: Representing and modeling collaborative practices for systems development. In: Social Thinking–Software Practice. MIT Press (2002)
4. Faily, S., Fléchais, I.: Persona cases: a technique for grounding personas. In: Proceedings of the 29th international conference on Human factors in computing systems, ACM (2011) 2267–2270
5. Riegelsberger, J., Sasse, M.A., McCarthy, J.D.: The mechanics of trust: A framework for research and design. International Journal of Human Computer Studies **62**(3) (2005) 381–422