# Security Lessons Learned Building Concept Apps for *webinos*

Shamal Faily
Software Systems Research Centre
School of Design, Engineering & Computing
Bournemouth University
Poole, DH12 5BB
UK
*sfaily@bournemouth.ac.uk*

John Lyle
Department of Computer Science
University of Oxford
Wolfson Building, Parks Road
Oxford, OX1 3QD
UK
*firstname.surname@cs.ox.ac.uk*

**Concept applications provide a means for tackling security infrastructure problems. Not only do they provide feedback to infrastructure design, they can also inform subsequent research activities. However, to directly influence the architectural design of infrastructure, designers need to engage in the engineering of apps, rather than just their broad design. By doing so, additional problems can be identified that might otherwise be missed using human-centered design alone. In this paper, we describe four security lessons learned from engineering the *Kids in Focus* concept app for the EU FP 7 *webinos* project. These illustrate how detailed design activities can highlight broader infrastructure problems that might otherwise have gone unnoticed.**

*webinos, concept apps, personas, access control*

## 1. INTRODUCTION

As we become more reliant on mobile apps, it is easy to forget how dependent they are on software infrastructures. Infrastructures like App Stores are not prominent, but are becoming increasingly important for fostering software ecosystems. Other examples include the software libraries connecting end-users to remotely connected services. Our dependency on such infrastructures is not purely functional; we also have implicit security and privacy requirements that we expect to hold when directly or indirectly using them.

Software infrastructures are difficult to validate without creating apps that use them. Even then, while missing or broken functionality might be easy to spot, security problems are harder to identify. Security vulnerabilities in apps may not properly reflect vulnerabilities in the infrastructure they use. Moreover, the absence of known security problems in an app today does not mean latent vulnerabilities in the infrastructure won't be found by an attacker tomorrow.

Concept applications are useful for providing feedback to the design of infrastructures (Edwards et al. 2003). Additionally, as concept designs such as Dynabook have suggested, even if these applications are never built, they can still influence other design activities (Stolterman and Wiberg 2010). Concept app design focuses on the interfaces between infrastructure and application, and the match between conceptual models and functionality (Edwards et al. 2010). However, Edwards et al. claim that directly influencing the architecture of the infrastructure requires engagement with the technical specialists that have traditionally led design discussions. This engagement includes addressing quality concerns, such as security, that are often sacrificed during the early stages of design. One approach for doing this is to try engineering, rather than lightly prototyping, a concept app. Attempting to develop non-trivial applications not only exposes some of the user and application developer expectations of infrastructures, it also suggests further opportunities for tackling broader problems that may not have otherwise come to light.

In this paper we describe four security lessons learned from engineering the *Kids in Focus* concept app for the EU FP 7 *webinos* project. These illustrate how detailed design activities can highlight broader infrastructure problems that might otherwise have gone unnoticed.



*Proceedings of BCS HCI 2013 Workshops*
*Human Aspects in Mobile App Engineering*

## 2. INTRODUCING *WEBINOS* AND *KIDS IN FOCUS*

*webinos* is a software infrastructure for running web applications across different device platforms (Fuhrhop et al. 2012) including mobile handsets, TVs, in-vehicle infotainment systems, and Internet of Things devices. The specification of *webinos* was informed by human-centered design activities, such as the creation of personas (webinos Consortium 2011b), scenarios (webinos Consortium 2012), and the integration of these activities into the specification of *webinos* (Faily et al. 2012).

To further manifest ideas about how *webinos* might be used by the personas, we developed a concept app called *Kids in Focus*. This app is a children's card game designed to be played on in-vehicle, mobile devices, and TVs. The game involves a child playing cards with a remotely connected babysitter. By playing with the child, the babysitter ensures that a parent or guardian driving the car will not be distracted during long car journeys.

Once a specification for *Kids in Focus* had been created (webinos Consortium 2011a), development was carried out by a small team of developers and user interface designers. This team was supported by security and usable security researchers involved in both the human-centered and architectural design of *webinos*. The source code for *Kids in Focus* is available online via GitHub (webinos Consortium 2013c).

## 3. LESSONS LEARNED

*Kids in Focus* has been developed in parallel with other *webinos* project activities since November 2011. The sections below summarise four security lessons learned so far in building this concept application.

### 3.1. Children are security stakeholders too

Surprisingly for a concept app designed for children, there were few insights available to developers about how children might be affected by *webinos*. Moreover, although a persona – Helen (webinos Consortium 2013b) – had been created to represent the mother of a young child, the development team had nothing other than assumptions to guide their thinking about child-game interaction. In hindsight, this was a surprising omission because children and cars are two of the most precious things an average person is likely to be responsible for.

Because none of the developers involved with concept app development were parents, we created a new persona to understand how children might interact with *Kids in Focus*. After interviewing project team members who were also parents of young children, we quickly developed a persona for Eric: the youngest son of Helen (webinos Consortium 2013a). By using both this persona and a premortem scenario (Faily et al. 2012) to envisage ways that Eric might be harmed as a result of a *Kids in Focus* security breach, we identified vulnerabilities in the way the concept app captured and managed analytics data.

### 3.2. Security helps envisioning

The developers found it easy to envisage Helen driving a car, and Eric playing a game in the back seat; several scenarios describing the parent and child interaction with *Kids in Focus* were described in (webinos Consortium 2011a). However, many unexpected aspects of how *Kids in Focus* might be used were not apparent until people considered the security and privacy implications of setting up and playing games. For example, we envisaged that, before starting any game, *webinos* would check a remote player had permission to access the resources necessary to interact with a *Kids in Focus* game. However, it wasn't until this precise detail was specified that it occurred to the developers that the setup might be too involved for Helen.

Given all the issues Helen needs to address at home before setting out on her journey, methodically following this process in advance seemed unlikely. Instead, we concluded that Helen would instead let Eric watch a movie or play with a more traditional, physical travel game instead; *Kids in Focus* would then only be setup on an ad-hoc basis some way into a journey once Eric was bored of his planned activities.

### 3.3. User accounts are dead, long live user accounts

*webinos* facilitated the setup of a "personal zone" of different devices. This allowed Helen to use her mobile phone to control settings on the in-vehicle system Eric used to play *Kids in Focus*. Conceptually, *Kids in Focus* also provided a vehicle for thinking about how devices in Helen's personal zone might interact with devices used in the personal zone of the remote babysitter Eric was playing with.

Tablets and other mobile devices tend to assume that one person is the owner and user of the device at all times. However, when devices are shared between parents and children, this is not the case. User authentication solutions are slowly appearing in mobile handsets, but not in a standardized manner, and not in a way that is well understood by users or developers. As we discovered when

building *Kids in Focus*, this meant that a cross-platform application needed to be designed with no assumption about who the current user is. This did, however, present opportunities to think about how local device authentication might be tailored to the application in question, to afford a more usable authentication experience.

### 3.4. Convention is sacrificed for innovation

Developing concept applications highlighted unconsidered security issues. The development process also indirectly introduced tensions when deciding how limited security manpower should be spent.

At a project review where *Kids in Focus* was presented, an idea for modifying the *webinos* access control framework was proposed. The proposal entailed re-directing permission prompts that might otherwise appear on Eric's tablet to Helen's phone instead. This idea drove discussions within the project about analogies between this approach and "Bring your own device" policies found in commercial environments, and possible solutions for implementing this idea. Tackling the problems would have led to security innovation; this excited many on the project who wanted to develop prototypes to explore the options available.

Dedicating resources to building these prototypes would not have been possible without spending manpower earmarked for implementing other planned security functionality. However, while the idea *appeared* to be neither urgent nor important, it was impossible to say if this was actually the case. This was because the idea was not found using the security and usability design methods used to elicit, analyse, and mitigate other risks addressed by the *webinos* architecture. Retrospectively analysing the design of *Kids in Focus* was also infeasible because the manpower was unavailable for carrying out this work.

This lesson reinforces not only the disruptive nature of security (Faily and Fléchais 2010), but also the value tensions between security innovations and secure systems.

## 4. CONCLUSION

Software infrastructures are difficult to envisage without the aid of concept applications. However, when designers and developers join forces to tackle implementation problems in their construction, additional insights can be gleaned about the human implications of such systems.

In this paper we presented four security lessons learned developing the *Kids in Focus* concept application for *webinos*. These lessons have subsequently been used to inform the design of *webinos* platform. For example, we are currently informing the security testing for the *webinos* policy management architecture (Lyle et al. 2012) based on how Helen and Eric interact with *Kids in Focus* during a long car journey.

## 5. ACKNOWLEDGEMENTS

The research described in this paper was funded by the EU FP7 *webinos* project (FP7-ICT-2009-05 Objective 1.2).

## REFERENCES

Edwards, W. K., V. Bellotti, A. K. Dey, and M. W. Newman (2003). The challenges of user-centered design and evaluation for infrastructure. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 297–304. ACM.

Edwards, W. K., M. W. Newman, and E. S. Poole (2010). The infrastructure problem in hci. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, New York, NY, USA, pp. 423–432. ACM.

Faily, S. and I. Fléchais (2010). To boldly go where invention isn't secure: applying Security Entrepreneurship to secure systems design. In *Proceedings of the 2010 New Security Paradigms Workshop*, pp. 73–84. ACM.

Faily, S., J. Lyle, and S. Parkin (2012). Secure system? challenge accepted: Finding and resolving security failures using security premortems. In *Designing Interactive Secure Systems: Workshop at British HCI 2012*.

Faily, S., J. Lyle, A. Paul, A. Atzeni, D. Blomme, H. Desruelle, and K. Bangalore (2012). Requirements sensemaking using concept maps. In *Proceedings of the 4th International Conference on Human-Centered Software Engineering*. Springer. To Appear.

Fuhrhop, C., J. Lyle, and S. Faily (2012). The webinos project. In *Proceedings of the 21st international conference companion on World Wide Web*, WWW '12 Companion, New York, NY, USA, pp. 259–262. ACM.

Lyle, J., S. Monteleone, S. Faily, D. Patti, and F. Ricciato (2012). Cross-plaform access control for mobile web applications. In *Policies for Distributed Systems and Networks (POLICY), 2012 IEEE International Symposium on*, pp. 37–44.

Stolterman, E. and M. Wiberg (2010). Concept-driven interaction design research. *Human-Computer Interaction 25*(2), 95–118.

webinos Consortium (2011a, October). Specification of webinos Proof of Concept Applications. `http://www.webinos.org/content/webinos-ProofOfConceptApps-PUBLIC.pdf`.

webinos Consortium (2011b, February). User expectations on privacy and security. `http://webinos.org/content/webinos-User_Expectations_on_Security_and_Privacy_v1.pdf`.

webinos Consortium (2012, May). Updates on Scenarios and Use Cases. `http://www.webinos.org/wp-content/uploads/2012/06/D2.4-Updates-on-Scenarios-and-Use-Cases.public.pdf`.

webinos Consortium (2013a, April). Eric persona. `https://github.com/webinos/webinos-design-data/blob/master/personas/eric.xml`.

webinos Consortium (2013b, May). Helen persona. `https://github.com/webinos/webinos-design-data/blob/master/personas/helen.xml`.

webinos Consortium (2013c, January). Kids in Focus Concept Application. `https://github.com/webinos-apps/app-kids-in-focus`.