To Market, To Market: Human-Centered Security and LotusLive™

Mary Ellen Zurko
IBM
Littleton, MA
USA
mzurko@us.ibm.com

ABSTRACT
In this paper, we discuss several techniques that were useful in injecting usable security as a quality into the LotusLive™ cloud collaboration offerings. We relied on having people responsible for both usability and security on the project. We aligned usable security with the specific business needs of the market being targeted. We developed some principles early on to guide the motivation and placement of features considered to provide usable security. And we aligned specific process for ensuring usable security with the process of the overall project.

Keywords
Usable security, Technology transfer.

1. INTRODUCTION
Almost from its inception as an early advanced development experiment, the LotusLive™ team has had a commitment towards not just enhancing our security as a quality, but to enhancing usable security as a quality. LotusLive™ is the brand that covers the offerings in the IBM® Software as a Service, multi-tenant cloud collaboration platform. This paper discusses the aspects and approaches we found successful in driving usable security as a quality into products, one form of technology transfer of usable security.

2. Putting usability and security together
Nothing gets done without someone to drive it. The importance of security to the cloud market meant that I was brought in early on (iteration 3) as the point for security. For Lotus collaborative products, user experience is always of primary importance, with early user experience and design work driving both initial vision and early functional direction. The UX lead and I were certainly familiar with each other. But we had never attempted a tight cross discipline collaboration within a project between security and usability. I reached out to the user experience lead, proposing that we work on usable security together, finding appropriate ways to inject it into his designs

3. Matching the business need
Initial advanced development work focused on collaboration needs of Small and Medium Businesses (SMBs), particularly in terms of file sharing. Market data and research showed that one of the major inhibitors of uptake of cloud by SMBs were security concerns. More specifically, some of those concerns were around user error; that hosting end user applications in a public cloud would give the user more opportunities that they did not understand for inappropriately exposing business and company data to people outside of the company (friends, competitors, the web as a whole).

Knowing and citing the market research and issues provided a platform to drive the right kind of usable security into early file sharing designs. Given the concerns for user error leaking data across the organizational boundary, we took the organizational definition and perimeter within LotusLive™ as a core concept at both the user experience and functional level. We were unaware of any other public cloud collaboration or social networking system that has done the same. We provided an option to share a file with the entire organization, easing the task of predetermining who within the company should get access to the information while still honoring the potential for company confidential information. We restrict display of email names, which are attractive targets for spammers and personally identifiable information, to the users in the organization and users outside the organization that the owner has explicitly connected to.

Determining the market drivers for usable security in the enterprise market is our next challenge. The increased scale of the challenge at the enterprise creates a number of differences in the business requirements. One is the requirement for oversight and control by enterprise compliance and administrative staff. The norm on human processes is that there are technical controls in place, or regular reports or checks that are available. We see this as an extension of the original principles put in place for end user usable security, transparency and control, into the realm of the administrator and organization. The definition of the organizational boundary in the cloud will also help, as it enables us to focus those techniques on those boundaries, which are of most interest to the organization. An additional challenge is that market drivers are usually framed in terms of established market categories. Usable security has not aligned or defined itself as a market category, or other sort of item that can be easily defined and compared in a purchasing decision (such as a standard). Data Leak Prevention is the category most easily aligned with one aspect of LotusLive™ usable security (controls and design around organizational boundaries and information flow).

4. Principles
There are a number of operational methods to drive something into a product. If it can be put in as a concrete component of the architecture, the process is in some sense straightforward. The process for driving a quality, such as performance, usability, security, or usable security, can be more variable. As the usability field matured, a number of papers on successful (or somewhat successful) methods for incorporating usability into products were published in conferences and journals. Often the process must align with the overall technical and business process for a product.

Early in the design, we knew we wanted to drive usable security into all aspects of the collaboration functionality, but were challenged by questions such as "What exactly is usable security?". We decided to start with a number of guiding design principles that any design could be checked against. For the cases around injecting and ensuring the appropriate user security mechanisms, we were guided by "Transparency and Control". For all scenarios where humans interacted with other humans, directly or through artifacts, we wanted to ensure that security state information was transparently obvious, at a glance, and available to the users involved. In addition, artifact owners should be able to control how their artifacts are shared, and organizational owners should be able to control what owners can do. The second principle was "No Surprises". Owners and administrators should not be surprised by any particular turn of events; they should know what's going on, and what could happen. "No Surprises" covers transparency, but also the potential for confusion and mistakes. These initial principles provided a grounding for both user experience and security for initial security aspects of the design of the user facing functionality of LotusLive™.

5. Process

Next we needed to figure out how to appropriately synchronize usability and security in the development and delivery process to ensure usable security of the LotusLive™ functionality. The project was based on the agile methodology, with all initial processes focused on four week iterations. The user experience group would have design tasks for the iteration, and the designs were reviewed by the developers impacted, along with other stake holders such as product management and development management. Security was initially handled as a cross cutting concern, with some tasks tagged as security related tasks, which could be assigned to whatever component had the most affinity. There was a single point person responsible for security overall, and over time some developers started specializing in security. Carefully placed security themed iterations focused the entire development team on security issues in design, coding, testing and review. Given that initial set of processes, the best place to bring the user interface and security teams together was in the per iteration review of the new user experience functionality. Security attended the reviews, giving feedback on security related considerations in the proposed user functionality, and with suggestions about issues in usable security, particularly on the agreed upon themes. For security specific features (usually administrative in nature), the user experience team did the design, so user experience and security were naturally working together.

Over time, user experience design cycles were more organic, and less tightly tied to the iteration schedule as the UX designers began to work on design challenges further out than the current iteration. Also, security specific reviews for all substantial components and tasks were instituted. Some usable security considerations were injected into the security review checklist. Security team members were called in to review substantial user experience work after it had gotten a round or two of review from other stakeholders. Since the usable security principles had become ingrained in both the process and the software, different stake holders at different times were able to call out potential issues (user experience, developers, and security). At times when a new member of one of the teams came on, they were surprised by the need for integration between user experience and security, since they had never experienced it before. In addition, as LotusLive™ user experience personnel spent time on other products and projects, they brought their usable security experience with them, injecting it into other efforts. We consider that sort of transfer of expertise and knowledge to be a huge success.

The process was not without its challenges, as with all new things. Since interpersonal social networks have less of an emphasis on the user experience around security, there were several discussions about the difficulty and issues with that emphasis, and how it impacted more direct transfers of well known forms of interactions from personal social networks to collaboration for business. Some of the going in positions from the security side were mostly informed by more traditional, less usable security approaches, placing the burden on the user experience team to attempt to drive to better integrated solutions. With practice, that got easier. There are still some thorny areas that are not as close to our principles as we'd like. In particular the indirection of groups raises some opacity issues that we continue to grapple with.

6. Conclusion

In the case of LotusLive™, we found that identifying point people and teams responsible for usability and security, targeting specific market requirements with a usable security approach, developing principles that could be used during the early design phase, and integrating usable security concerns with existing processes produced a successful technology transfer that enhanced the usable security of cloud collaboration offerings. We hope that others will share their technology transfer stories so that a richer picture of approaches and pitfalls can be developed.

7. Acknowledgements

Special thanks to Chris Paul for his teamwork, expertise, and proof reading.