

The paradox of usable security

By Andrew Swartz, (first published 17 August 2004, UsabilityNews.com)

I have a friend in the States who lives in a big city, and like all big city dwellers she has a healthy concern for safety. Her front door has a deadbolt, a latch, a chain, an extra deadbolt, sliders top and bottom, kick plates, an intercom system, and a high-tech peephole. It can take two minutes to vet the pizza delivery guy and permit access for a pepperoni with extra cheese.

But when she takes out the rubbish or goes to the kerb to get the morning paper, more often than not she leaves the front door wide open. It's too much trouble to deal with all those latches and locks, codes and keys. Good technology, but sometimes security can make things less secure.

The same is true when designing online applications. Often, the more technically sophisticated the security, the more users will thwart the security, creating a paradox for those who don't take human limitations into account: The more secure the technology, the less secure the system.

*My colleague at Serco Usability Services, **Simon Herd**, has been working on banking applications for over a decade and has been considering the implications of security usability. I'd like to share his thoughts on the subject with you. Here is Simon's article.*

In November 2003, MI5 was revealed to have infiltrated the Pakistani High Commission in London. Their job was made surprisingly easy as High Commission staff had left the code for their cipher machine on a yellow Post-It note stuck to a wall next to the machine. The most elaborately engineered authentication system turned out to be insecure in the light of some rather human traits – the need of humans with fallible memories to write down complex passwords.

To be secure, any authentication method must identify authorised users in a way that considers how real people work and think. There are a number of approaches to authentication. How do usability considerations affect these approaches?

Passwords

If you use online banking, or indeed almost any computer-based application, you will be familiar with passwords of varying formats. I've mentioned a rather extreme example of what can happen with complex passwords, but this is just one example of a wider issue. As humans, we are not built to instantly recall complex and non-meaningful strings of words and numbers on a periodic basis. When we are forced to by technology, we will often opt not to use it or adopt (possibly Post-it based) workarounds.

This problem is compounded when a user has to remember passwords for all the software packages that they use and compounded further when they are made to change passwords on a regular basis. In visiting one workplace recently I noticed that there was a big red notebook on the desk with the words "Password Book" written in rather large letters across the front. Staff happily admitted that they could not keep up with all the password formats and password changes for the software that they had to use.

We often see that the tolerance to password complexity can vary with the relative importance of the software and indeed, it can vary over time. For example, we've seen a greater tolerance of it with online banking and it is possible that attitudes may shift further given the press attention that this area has recently had. However, in a competitive market the user always has options and if

authentication for one online banking application is felt to be less onerous than another without compromising the desired security of the user, then real competitive advantage is lost. Users have told us they have quit using online systems that were too difficult to log in to.

To provide real security, password strategies need to match user capabilities. If they do not, the user will either not use the software at all or find a workaround which may be dangerously insecure.

Chip and PIN

Personal identification numbers (PINs) are another common authentication method. There are big changes happening in the UK that will directly impact how we access technology, whether on the Internet or elsewhere: the credit card industry is moving from the magnetic cards that have been in use since the early 1970s to smart cards using Chip- and-PIN authentication. Again, it is important for online security to be both easy to use and only allow access to those intended.

Putting chips into plastic cards means that a more secure alternative to passwords may be offered. In the longer term we are going to see card readers in PCs, TV set-top boxes and other devices to make payment easy, but the rate at which people change their hardware is always slow (for most of us anyway). In the shorter term chips can be read by small standalone card readers the size of a key fob. This can generate a random PIN to be used to access Online Banking or other applications. A similar approach to this is widely used in Scandinavia, where small tokens are used to generate PINs for online banking. While potentially more secure than using the same passwords every time, there are human factors to consider. Are users willing to carry a small device with them to generate secure PINs when they are needed? As we have seen with passwords, software is not used in a vacuum. What happens when users have accounts with more than one organisation? This approach has been very successful in Scandinavia, where the users appear to be placing a higher value on the security provided. However, this may not be guaranteed to work in other cultures. As we've seen with Account Aggregation, what works in one country may not in another.

Where these cards are being used for off-line payment rather than just on-line access, standalone keypads will be used increasingly in the place of signatures. Such devices are already highlighting usability concerns, in particular over accessibility. For example, significant issues have been identified with PIN entry devices in Post Offices for blind users, which the Post Office is currently having to (expensively) address. As new authentication possibilities arise due to the advent of Chip- and- PIN, both on the Web and beyond, usability will continue to be an important consideration in how successful they are.

Biometrics

Biometric security is another area where new technology opens up new possibilities. Identification by unique personal characteristics such as fingerprints or iris patterns initially seem ideal from a usability perspective. Technical capabilities are increasing and it does seem to be the most inherently natural (and highly secure) method of authentication, requiring little effort from the user.

However, even this approach requires careful consideration of the way users think and react to technology. For example, a high level of validation will result in false rejections: a hung over or ill but otherwise authorised user with bloodshot eyes might be rejected. This technology also raises potential accessibility issues and contextual factors such as the physical environment and cultural context can be important. For example, people from certain cultures may be reluctant to press their fingers/palm on a biometric device due to concerns over hygiene. So even the most seemingly natural method of authentication raises potential usability issues that must be considered.

Conclusion

Common threads run through the various methods of authentication. Any method must provide the level of security that the user feels is appropriate for that type of software, and it must do so in a manner that is as natural as possible to the user. If ease of use is not considered, users are likely either to consider dropping a service or adopt insecure workarounds. Security is not just about technology; it is about the users who want to access the technology. Applications must get the balance right between security and usability.

We would be interested in hearing your stories about the trade-offs between security and usability. Please feel free to contact Simon at simon.herd@serco.com.

About ExperienceLab

ExperienceLab (formerly Serco Usability Services), are a global experience design research agency. They help organisations optimise their customer experiences, from web to TV and mobile, from advertising to physical environments. They've been doing this for a while, pretty much since the first computers and networks were created, so they know a thing or two about how to make people, processes and technologies work in harmony.

ExperienceLab use a wide range of techniques to tailor a research solution that fits your business objective, including ideation sessions, proposition analysis, customer needs mapping, usability testing, benchmarking and touch point integration studies. As a co-founder of the UXalliance we also provide research on a global scale.

Why not visit the ExperienceLab blog (www.experiencelab.info), which features the latest thinking on experience design issues.

Serco ExperienceLab

22 Hand Court
London
WC1V 6JF

+44 (0)20 7421 6499

info@experience-lab.co.uk

www.serco.com/experiencelab