Andrew Zurn

Reading 4

Summarized Article: <http://online.wsj.com/article/SB10001424127887323585604579008620509295960.html>

Other Article:

<http://dl.acm.org/citation.cfm?id=945074.945125&coll=DL&dl=ACM&CFID=248587646&CFTOKEN=17738074>

In Andrew Blackman’s article “Say Goodbye to the Password,” Blackman describes the areas of research that many companies are looking into to replace the traditional password with some sort of human augmented component. He opens his article by saying that the “fundamental problem with passwords is they are most effective in protecting a company when they are long, complicated and changed frequently. In other words, when employees are least likely to remember them.” This, to us as computer scientists and technicians of the IT industry, is less than a problem, as we generally know password best practices, and choose easy enough be complex-like passwords to protect our private data. But for everyone else, I can see it be quite the challenge to both find a complex enough password, remember it, and have some sort of a cycle to change passwords to when companies or organization put in place password recycle rules.

Here comes in the various companies that are trying to replace and fix the problem of the non-savvy user forgetting their password. Apple just implemented a finger print reader into their iPhones that were just released in the past week, and Google, Paypal, Lenovo, and Microsoft are also all into this area of altering the password landscape. Be it from fingerprint readers, to plug-in tokens, to short range communication tokens that authenticate users.

Although as I stated above, the problems with passwords do affect those of us that are not tech-savvy, and thus the products that these companies are trying to create to have a solution for this problem is worthwhile in doing. However, I do have some worries about some of the solutions these companies are coming up with. The first, I worry that those building biometric readers might begin collecting biometric data from users without their consent, and might sell it or hand it over to different organizations. I’d rather not let the NSA have my fingerprints, or let them have any other personal data that might be abused. Also, if the tokens and such are lost or stolen, breaking authentication for users that lost them becomes easier for abusers, and systems then become insecure. Although these approaches might be good for the masses, better thought and securities need to be put into place before they go into mass production, not only for the sake of company security, but also our personal privacy.