# Facebook's Battle Sign

November 16, 2009, Michael Lissner
Privacy, Security, and Cryptography
University of California, Berkeley

**Battle's sign** is commonly the only outward sign of a skull fracture. In fact, this type of fracture may go undetected even by skull X-rays. If left untreated, it can be fatal...

– Handbook of Signs and Symptoms[1]

## 1 Security is Economics

In class, we discussed a set of thirteen principles for the design of secure systems. Applying these to Facebook is a task that somebody ought to do at some point, for it seems clear that Facebook has not taken security particularly seriously for some time.

Probably the most important of these 13 principles is the first, which states that, "Security is Economics." Unlike the other principles, this principle speaks to the *motivations* for the design of a system, not the design of the system itself. In the case of Facebook, the economics are rather complicated, however few would argue that, regardless of their business model, their most important method of guaranteeing revenue is to attract more users, and to create an environment where users spend more of their time logged into the system. To do this, Facebook must entice users to the site and keep those users pleased with the site. As a result, when it comes to security, they must walk the line between what is acceptable to the users, and what is cost effective for their bottom line.

When weighing this balance, Facebook must analyze the threat model and determine what security threats might result in loss of users or of their users' time. In order to lose users, a threat must be public (so the users know about it), and must be drastic and obvious (so that ordinary users can understand the

1 Springhouse, ed., *Handbook of Signs & Symptoms*, Fourth Edition. (Lippincott Williams & Wilkins, 2009), 78.

threat). As we have seen over the past several years, such a confluence of factors is rare in the security arena. As we discussed in class, even the most flagrant of security errors – the insecure login – is not enough to create an exodus of users. As a result, it is not surprising that Facebook does little to ensure that their system is secure, and major data leaks and problems are frequently discovered.[2, 3, 4]

For now, the average user does not understand the risks that Facebook places on their data, and so Facebook is not at a great risk of losing their patronage. Economically then, these users do not affect Facebook's security decisions. However, as more data is lost, their economic mandate for better security waxes, and soon we should begin seeing the effect of this mandate.

It thus seams clear that the threat is huge, and the financial impact could be devastating for their organization. They do not, however, take reasonable precautions against this threat.

## 2 Psychological Acceptability

A principle of secure systems that is hinted at above is that of "psychological acceptability." This principle states that for a system to be secure, it must be fitting with the psychological abilities of those people that will be using it. In the case of Facebook, the average user has very little understanding of security threats, and is thus unconcerned with the security and privacy of their data. As a result, Facebook has the challenge of creating a system where security is a psychologically appealing decision for users.

---

2 achille, "Facebook FAIL: A misconfigured webserver has leaked notes for 16,000 accounts with privacy settings turned on. (Mine was one of them) : programming," September 11, 2009, http://www.reddit.com/r/programming/comments/9jn8i/facebook_fail_a_misconfigured_webserver_has/.

3 Dennis Yu, "How To Spam Facebook Like A Pro: An Insider's Confession," November 1, 2009, http://www.techcrunch.com/2009/11/01/how-to-spam-facebook-like-a-pro-an-insiders-confession/.

4 Jason Kincaid, "Massive Facebook And MySpace Flash Vulnerability Exposes User Data (Updated)," November 5, 2009, http://www.techcrunch.com/2009/11/05/massive-facebook-and-myspace-flash-vulnerability-exposes-user-data/.

In some regards, Facebook does a reasonably good job executing this principle, but this is largely a result of lax security rules in the first place. As discussed in the next section, because Facebook does not enforce strict rules for strong security upon any of the programs or users of the system, it avoids those problems where users circumvent the system's security mandates.

One area where Facebook may encounter some push back from the users is with regards to the HTML autocomplete attribute which, on the login page, is set to off. Turning this attribute off prevents password managers from storing a user's password after they login, which is a good thing on shared or public computers. However, for those users that prefer to use password managers, this attribute is frustrating since it forces them to remember a password, and popular scripts have been written to circumvent it.[5]

A further problem related to the psychological acceptability of Facebook's security measures relates to their mechanism of allowing outside applications (such as popular photo applications or external websites) to integrate with their site. The current system utilizes the user's password, encouraging them to use a password that is easy to remember or else one that is written down. In either case, there is a disincentive to using strong passwords, which is detrimental to the security of their system.

## 3 Usability

A related principle to psychological acceptability is the principle of usability, which states that a system must be usable by its intended audience. In the case of Facebook, it can be presumed that the users are a lay population, and so security features and settings must not be overly complicated or convoluted.

This is an area where Facebook abjectly fails. Although it has reasonable privacy mechanisms in place, finding, understanding and adjusting these settings is a difficult and time consuming task. As an example, to find the page

5 Indeed, in the case of the author, I have disabled this feature altogether by altering my browser's code.

where an application's permissions can be revoked, a user must browse to Settings > Privacy Settings > Applications, and then find the link (within a large block of text) to the application settings. Because this link is four levels deep within the settings, very few users will be able to find it, even if they seek it out. For those users that do not seek it out, it's quite likely that it will never be found.

A similar problem can be identified when examining the system's ability to place "friends" into groups, and for groups to have certain levels of access to a user's information. While this is a laudable and powerful approach to privacy, it fails because it is overly complicated, forcing users to create taxonomies for how they categorize their friends. A simpler system consisting of only loose, medium and strict privacy settings would make grouping friends into categories more intuitive (close friends into loose, distant ones into strict, etcetera).[6]

## 4
## Least Privilege

A fourth principle for the design of secure systems is that of "least privilege." This principle requires that for any user or system component it is important that they only have enough privileges to legitimately accomplish what they were intended to do.

How is Facebook's example of this principle? In a word: Bad. It's very difficult to know how well Facebook handles this principle with their internal programs. Their Achilles heel can be found however by examining Facebook Applications, and the API upon which they rely.

These applications are constantly running into problems due to the fact that the API is more permissive than the web interface. As an example, a popular hacker magazine, there is an article that describes how to spoof a message from one Facebook user to another.[7] Similarly, the ACLU has created an application

---

6 For an at-length discussion of this concept, see: Michael Lissner, "Rethinking Facebook Privacy Settings | Michael Lissner," *Rethinking Facebook Privacy Settings*, August 17, 2009, http://michaeljaylissner.com/blog/rethinking-facebook-privacy-settings.

7 stderr, "Facebook Applications Revealed," *2600: The Hacker Quarterly*, Winter 2007.

which demonstrates the privacy problems with the permissiveness of the API.[8] In their application, the ACLU demonstrates that not only can it access information about you, but it can also access information about your friends – despite and regardless of their privacy settings. Clearly, this is not the intention of the Facebook API, however to date, they have not fixed this privacy hole.

A second area where their security is unreasonably weak is with regards to the pictures that are hosted on their site. As the largest photo site on the web,[9] it's rather unfortunate that the only thing preventing your picture from being displayed publicly is a thin veneer of obscurity. Further, lacking a way to meaningfully delete photos makes such problems doubly dangerous.[10] The following scenario should exemplify the problem:

1. On 21 May 2009, your "friend" posts an embarrassing photo of you on Facebook.
2. Another friend right-clicks that photo, copies its location, and then posts a link to it on his/her website within an HTML <img> tag. This defeats the veneer of obscurity.
3. The world can now see that photo, not just those people designated within Facebook.
4. You ask the friend to delete the photo from Facebook, and they do.
5. That photo is never actually deleted from their servers, and if the article mentioned *supra*, is accurate, the photo would still be there to this day.[11]

---

8 ACLU Northern California, "What Do Quizzes Really Know About You? on Facebook," http://apps.facebook.com/aclunc_privacy_quiz/.

9 Erick Schonfeld, "Facebook Photos Pulls Away from the pack," *TechCrunch*, February 22, 2009, sec. Tech, http://www.techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/.

10 Jacqui Cheng, "Are "deleted" photos really gone from Facebook? Not always," *Ars Technica*, July 3, 2009, http://arstechnica.com/web/news/2009/07/are-those-photos-really-deleted-from-facebook-think-twice.ars.

11 In an effort to verify this data, I have begun my own investigation into the cache lengths of various online photo services. The ongoing results of this experiment can be found here: http://michaeljaylissner.com/blog/testing-deletion-speed-of-online-photo-sites.

## 5 Ensure Complete Mediation

This touches on another principle of secure systems which dictates that complete mediation must always be ensured. In other words, when caching information on any computer, revocation is vital. If you are unable to or simply do not revoke information, it can remain a problem for the security of the system. In the above scenario, the photo is placed on Facebook's photo server, but they lack a true method for deleting that information upon a user's request. As a result, the photo remains viewable even after its owner has attempted to delete it.

To my knowledge, outside of this error though, Facebook does an excellent job of revoking caches. It's quite likely that they use caching on many of their machines for various efficiency purposes, but I have not identified or found any additional criticism of these mechanisms.

Outside of their servers, the other place that information might be cached is in the user's browser. Generally, such caches are not a huge liability, since they are refreshed at page load, and only contain the information that the user was allowed to see in the first place. Facebook also uses the browser's cookie mechanism to cache a number of small pieces of information. These can be revoked by the user or by Facebook as needed, and I have seen no evidence that they are not properly handled by Facebook when they need to be deleted.

## 6 Don't Rely on Security Through Obscurity

A final principle which I will address here is that the principle of not relying on obscurity as a form of security. Although it may seem obvious that reliance upon an obscure method or secret would undercut the security of any system, in practice, many systems use such methods as a norm. As was mentioned above with relation to pictures that a friend or enemy might post, Facebook is no exception.

Facebook does not, however use obscurity for many other areas of the site. For example, although each comment and each post has a unique identification number, these numbers are not used as a form of security, but solely as a form of

identification. This is good. Elsewhere in the site, identification numbers are used to identify each user, but again, obscurity is not used in any significant way as it relates to security.