

Creating Safe and Trusted Social Networks with Biometric User Authentication

Ho B. Chang and Klaus G. Schroeter

BioID AG
Bruenigstrasse 95, 6072 Sachseln, Switzerland
info@bioid.com, <http://www.bioid.com>

Abstract. Many people are concerned about engaging in social networks or allowing their children to do so, because the anonymity and perceived lack of security puts them at risk of identity theft and of online contacts who misrepresent themselves, such as sexual predators and stalkers. Current password-based authentication neither adequately protects users' accounts from being compromised, nor helps people to trust that people they contact really are who they say they are. Strong multimodal biometric authentication, which can conclusively link a real person to a digital identity, prevents unauthorized account access and ensures that only the person who created the account can use it. At the same time, it offers an extra level of trust in the identity of other members, and provides a deterrent against potentially criminal abuse of social networks.

Key Words: multimodal biometrics, authentication, security, social networks

1 The Advent of Social Networks

A social network service is a website intended to build communities based on common interests and activities. Typically users can create profiles with selected personal information and interests, search or view parts or all of the profiles of other users, connect with old friends and make new ones.

Social networking websites such as Facebook, MySpace, LinkedIn, and Twitter have become a popular channel for communication, meeting people, and self-expression, and usage is growing rapidly. According to a June 2009 survey by research group The Conference Board, 43% of US internet users participate in social networks, up from 27% only a year earlier.¹

¹ <http://www.portfolio.com/news-markets/local-news/atlanta/2009/06/16/conference-board-43-of-internet-users-now-in-social-networks>

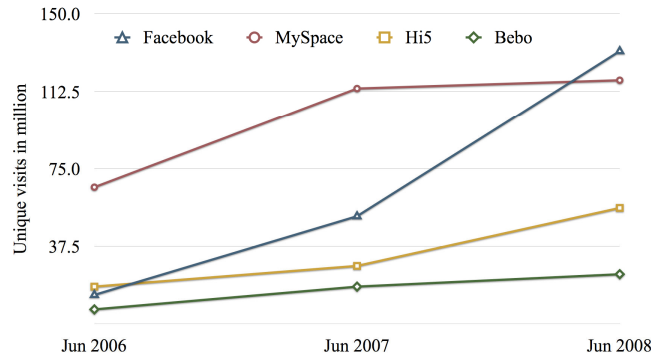


Fig. 1. The global growth of social networks.

Young people, in particular, have taken to it rapidly; a 2008 study by the Pew Internet & American Life Project found that 65% of US teens (12-17) use online social networks.² The demographics of several German social networks were analyzed by the AGOF internet facts 2009-I study.³

Table 1. Demographic profile of German social networks, March 2009.

Age of User	myspace.com	schueler.cc	stayfriends.com	studivz.net
14-19	23%	56%	4%	17%
20-29	31%	13%	17%	56%
30-39	18%	10%	29%	11%
40-49	16%	14%	27%	7%
50-59	7%	3%	12%	6%
60+	3%	2%	7%	1%

2 The Real Dangers of Social Networks

The anonymity and physical distance can lead to a false sense of security, so that users give out too much personal information. Even mature adults who should know better are not immune. Take the wife of the newly appointed head of the British Se-

² <http://www.pewinternet.org/Presentations/2009/17-Teens-and-Social-Media-An-Overview.aspx>

³ <http://www.agof.de/studie.583.html>

cret Intelligence Service. She posted personal information on her Facebook page, accessible to 200 million users, which compromises the new chief's security and could easily put the family at risk.⁴

The lack of control mechanisms makes it easy for malicious users to misrepresent themselves and gain other users' confidence. For example, in 2006 a 14-year-old girl committed suicide after having sex with an older man she met online. Her family has sued MySpace for facilitating the relationship.⁵ The case highlights one of the most serious dangers of social networks.

In 2009, MySpace confirmed that they identified user profiles belonging to over 90,000 registered sex offenders⁶ – and that only includes those who registered with their real names. Their accounts were blocked, but nothing prevents them from creating new accounts under false names.

Social media presents other dangers as well. Since there is no identity check, anyone can set up a fake profile in someone else's name, to post embarrassing and slanderous content. Add to that the prevalence of spam and offensive comments, for instance the spammer who tricked MySpace users into giving away login information, then sent over 730,000 spam messages to their friends, including links to gambling and pornography sites.⁷

Given this environment, is social media too dangerous? Or is there a solution to make virtual socializing safe?

3 Social Networking Today

Most major social networking sites today operate on the honor system. While many sites' policies require members to use their real name and age and to open only one account, there is no verification. Users can easily lie about their identity, with no traceability in case of a serious complaint.

The large member base and wealth of personal information makes social networks a magnet for unscrupulous people. Many users, wanting to express themselves or forgetting that strangers can also see their profiles, give out too much personal information. Add to that the tendency to use weak passwords – which can sometimes even be drawn from information in their profile – and the success of “phishing” at tricking users to give away their login information and you have a great recipe for abuse.

With access to someone's account, it is possible to spam their friends; to post embarrassing or incriminating information on their profile or elsewhere; and to gather additional private information leading to identity theft or even physical harassment.

Password-based protection is simply too easy to compromise. The average user today has 25 password-protected accounts; most people tend to use weaker passwords and to use the same one for several accounts [1]. Besides, even the strongest passwords still do not conclusively identify the user.

⁴ <http://www.timesonline.co.uk/tol/news/uk/article6639521.ece>

⁵ <http://www.wired.com/threatlevel/2008/02/myspace-sued-ov/>

⁶ <http://www.nytimes.com/2009/02/04/technology/internet/04myspace.html>

⁷ <http://www.ecommercetimes.com/story/63012.html>

4 A Potential Solution: Biometric User Authentication

A password (something you know) cannot prove a user's identity. Only one form of identification truly does. It must be something that cannot be guessed, lost, or stolen – something the user is, a unique feature that is part of the user. Such features are called biometric traits; they could provide a strong foundation for social network authentication.

A biometric authentication solution for social networks would need to provide highly accurate analysis of unique biometric features to reliably determine if the person logging in is the same one who registered. Capture of more than one trait would increase accuracy and security, assuming the results were properly fused [2]. At each log in, live traits would be captured and compared with the reference data, which could either be stored on the social network database, at an independent party such as a trust center, or by the user on the local PC or on a token or smart card.

Since users of such networks have greatly varying degrees of familiarity and comfort with technology, it should be easy to use in a way that is natural to the user and requires no memorization. Use of built-in or common, off-the-shelf equipment would reduce costs. A traceable audit trail at every login (privacy laws permitting) would further increase security.

In case of a crime, an accused person would only need to prove to law enforcement personnel, through biometric verification, whether the user data on file “belongs” to them. This model would not only increase the chances of successful prosecution, but would also provide a strong deterrent – who would commit a crime knowing that they could be identified through biometrics?

Finally, such a system could be even more effective and trusted with a reliable means to link the user with a legal identity. Registering with a government-issued identity document, such as a biometric passport or national identity card, could provide this link.

5 Biometrics for Social Networks: How it Might Work

The technology for such a system already exists, with a combination of human traits well-suited to a social networking application. Biometric identification of face, voice, and iris, individually or in any combination, using standard computer webcam and microphone, such as the biometric technology developed by BioID, has been available for some time [3].

5.1 Basic User Experience

Registration. To register for the first time, users can verify themselves against the biometric data (face and/or iris) stored on their biometric passport or national identity card [4] using a USB e-passport reader. The user can simply look at the screen while a webcam captures their face and/or iris in a video stream. Each trait is preprocessed separately, and unique features are extracted and compared to the biometric data on

the passport or identity card. A user registered in this way would be regarded as a “trusted” user.

Users who do not have a biometric passport or national identity card or who cannot access the data on their passport can be cross-verified by a “trusted” user. The new user can then enroll their face/iris biometric data using a webcam. The process is the same as described above, except that the unique biometric features are used to create a reference file to be used for later verification.

To make it even more secure, the user can be prompted to say a phrase, such as their name, while looking at the screen. While the webcam captures face and/or iris, a microphone captures a brief audio stream with the user’s voice, and added to the biometric reference file.

In any case, the biometric reference data can be stored on the social network server, at a trusted third party, or locally on a computer or token for later use. Only digitally signed snapshots of face/iris/voice, in a standard, non-proprietary format, are maintained. A digital signature includes a time stamp and provides a means to verify if a snapshot has been tampered with. To enhance the user experience, the biometric data can be updated as often as needed to adapt to the user’s usage behavior and environment, as well as aging.

Verification. The same simple capture process is repeated every time the user logs in. Biometric algorithms compare the new data with the reference data stored either on the biometric passport or identity card, on a token, on the local computer or on a server, and determine whether the newly captured data matches the reference data. In this way, every session is protected with a reliable login, ensuring that only the owner of the account is able to log in to the network and increasing trust in user identity.

In practice, user acceptance of this type of biometric login process is very high. They have nothing to memorize – no complicated passwords to be forgotten. Users do not have to touch a sensor or hold still. They simply do one of the most natural of human actions: look the camera in the “eye” and optionally say their name. Most people who have used this type of solution for other applications welcome its simplicity; the login process is completely natural and takes virtually no thought. The process has a certain “cool” appeal that especially younger people, the majority of social network users today, may appreciate.

5.2 User Experience Versus Security

System settings represent a trade-off between high security (low false acceptance) and greater convenience (low false rejection). The key here is to select a method that is best suited to the particular application. In some cases it may be necessary to use a stricter method [5], with which more attempts may be necessary, while in other cases a looser method might be more fitting, if the security concern is not so critical. For instance, acceptance might require that only two of the three traits reach a certain threshold score, or all three might have to meet a minimum. Alternately, the scores could be mathematically combined to meet a single combined threshold.

In a social networking application, while it is vital to keep users enthusiastic and the experience positive, security, as mentioned earlier, is becoming a critical issue which urgently requires action. In the extreme case, if a user had repeated problems

logging in they would probably become frustrated with the service. Particularly for some of the most popular social networks, even a relatively low rate of false rejection could mean a large number of complaints to customer service. Likewise, a minor security breach could trigger negative publicity for the whole community. Considering all of this, the decision method for a social network security solution should lean towards user-friendliness, while maintaining a strict configuration.

Fortunately, when combined and configured properly, the use of multiple biometric traits results in superior overall performance compared to a single trait, enabling suitable results even for very large social networks.

5.3 Continuous Session Protection

In addition to protecting login to the social network, using face recognition the system can continuously check for the presence of the active user's face in front of the screen throughout the entire social networking session. If the user steps away for a while, the system can automatically log out or inform any corresponding parties that the user is currently away, preventing unauthorized access of the user's account by other people with access to the same computer. In this way, the entire duration of the session is protected. Upon return, the user is either automatically recognized or is prompted to login again, and the system will automatically inform any corresponding parties that the user is back.

Such a process would offer multiple layers of protection for social networks. First of all, because a new video and voice are obtained at every login and throughout the session and are compared with the original registration data, only the registered user is able to log into a social network account or to take any actions during an active session. In this way, the dangers of unauthorized account access or impersonation described above can be avoided. It makes a truly "user-managed" social networking experience possible, because the user is the only one who can access the account, and so is in full control over it. It also greatly increases trust within the community; because the entire session can be trusted, other parties communicating through the service can be confident that they are communicating with the actual "trusted" user.

5.4 Duplicate Account Detection

Biometric authentication would also make it possible to detect if the same person is trying to open multiple accounts under different names. During registration, the new reference file can be compared with those of all existing accounts. If a match is found, it means the user may be trying to open a duplicate account, and registration can be denied or linked internally to the other accounts. This same method can be used to prevent users whose accounts were closed for policy violations from opening a new account under another name.

5.5 Traceability and Deterrence

Because the user's biometric data is kept on file, and is compared against at every login, all account activity can be traced to the identity established at registration. If

privacy laws and storage capacity allow, additional data from subsequent logins could also be stored, providing further accountability.

Perhaps the greatest benefit of biometric authentication for social networks would be the potential deterrent power. For a normal user, it assures that access to their social network account is securely protected. The fact that the user must provide biometric information such as their face and voice in order to register for a social network will make anyone think twice before harassing someone or committing a crime. Furthermore, a link between their online identity and their legal identity should make them think three times. Thus, such a solution has the potential to significantly reduce the incidence of the abuse previously described. And when abuse does occur, such a solution can make it easier to find out who is responsible.

6 Conclusion: A Safe and Trusted Social Network Community

Privacy and data protection is, then, possible for social networking. The technology described here could have a considerable effect on user satisfaction and the reputation of social networks. Stories such as those previously cited have made many people hesitate about social media, or at least about their choice of networks. A network that implements a strong identification infrastructure like the one described here would signal that the security of its members is a top priority. As a show of good faith this should help to protect against lawsuits when problems do occur. Furthermore, it should strengthen the trust of its members and potential members, increasing membership and overall activity: the factors most necessary for the success of a social network community. In this way, more people can safely reap the many benefits of social networking.

References

1. Florencio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Sixteenth International World Wide Web Conference (WWW 2007), pp. 657 – 665. IW3C2, Banff (2007)
2. Daugman, J., The Computer Laboratory, Cambridge University, <http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html>
3. Frischholz, R., Dieckmann, U.: BioID: A Multimodal Biometric Identification System. In: IEEE Computer, Vol. 33, No. 2 (2000)
4. Lion, R.: E-Credentials and Identity Management. In: Keesing Journal of Documents & Identity, Annual Report E-Passports 2008-2009, pp. 17 – 20. Keesing Reference Systems (2009)
5. Frischholz, R., Werner, A.: Avoiding Replay-Attacks in a Face Recognition System Using Head-Pose Estimation. In: AMFG 2003: IEEE International Workshop on Analysis and Modeling of Faces and Gestures (2003)