

The Case for a New Social Authentication Era

Larissa G. Rosa¹, Gustavo Zambonin¹, and Jean E. Martina¹

Universidade Federal de Santa Catarina, Florianópolis, SC, Brazil
{larissa.gremelmaier.rosa,gustavo.zambonin}@posgrad.ufsc.br
jean.martina@ufsc.br

Abstract. Even though we live in a connected society, there is a growing tendency to distrust the virtual world. This is largely due to the advent of deepfakes and other artificial intelligence capable of emulating various human characteristics, including voice, video, personal expressions, and writing styles. It is, therefore, imperative to develop secure and effective authentication and authorization methods that can be deployed against these systems. However, using passwords, biometric data, and possessions presents many problems exacerbated by this new paradigm's advent. We defend that this context requires a rethink of social authentication methods, although we first need to gain insight into their low uptake. In this context, we posit that the characteristics of the Internet at the time of the method conception, the temporal distance separating authentication, and the lack of transparency in updating items such as security contacts are likely contributing factors. Furthermore, we argue that it should be integrated with the individual's offline social sphere to foster greater trust in networked systems. Finally, we leave potential modifications and questions for further discussion.

Keywords: Social Authentication · Offline-Online Integration · Trust in Networking Systems.

1 Introduction

We are approaching a crucial point in the evolution of authentication methods. The academic community has long been critical of authentication methods based on passwords, citing various usability issues [1]. Furthermore, these methods are susceptible to significant vulnerabilities, including brute force attacks, data breaches, and other security risks [13]. Similarly, despite being widely used in critical banking applications, biometric authentication faces new threats. As AI models become more sophisticated, emulating voice, writing patterns, and even videos becomes easier. This highlights potential weaknesses in biometric techniques, particularly those that depend on particular hardware or highly confidential user information [2].

While the use of keys stored on personal devices shows promise, there are instances where the loss or theft of the device has resulted in users being unable to access their systems [10]. Furthermore, a reliance on a single device can present both usability and security challenges. In light of these considerations, it is clear

that there is a need to rethink authentication methods to align them with the demands and technological realities of 2025.

We believe this is the ideal time to re-evaluate social authentication methods. Although they gained attention with the advent of social networks [8, 6, 15], these methods have never achieved widespread adoption. The rise of deepfakes and AI technologies underscores the urgency of new virtual identity authentication, enabling safe real-world actions. Previously limited by the tech and social context, social authentication now faces a more favorable landscape for adoption.

Recently, the SOAP protocol was proposed based on identity providers [12]. If a user possesses multiple digital identities, their real identity can be confirmed. The authors define social authentication as a process based on online impressions, negating the necessity for links to the real world. While this approach has positive implications in situations like whistleblowing [7], social authentication should also consider a broader range of social factors beyond verifying multiple accounts with different identity providers. These factors could be leveraged for authentication purposes and to authorize actions that integrate the digital and physical worlds.

We show two examples of this: SIM Swap and porting. In both cases, there is a procedure to transfer the phone number to a new SIM card or another mobile network operator [9]. These cases involve a combination of virtual and real-world identity authorization and are susceptible to various scams exploiting current authentication models [11]. As we explain later, social authentication can also benefit professional environments. *But what are the reasons for the lack of popularity of social authentication? What steps can be taken to develop protocols that implement it more efficiently, considering usability and security? Would it be appropriate to use this approach in all cases?*

Our position paper examines state of the art in social authentication and defends the following points: ① the need for real-time adaptation, with a certain amount of privacy, due to the challenge of maintaining trust-based social authentication that accurately represents volatile human relationships; ② a greater focus on the amount of time expended in the authentication process is needed to solve usability issues, and ③ the effectiveness of social authentication is directly related to collaborative access and fraud prevention, exemplified by SIM swap cases. We sketch protocol enhancements to integrate authentication and authorization across physical and digital contexts.

2 Barriers of Social Authentication

We identified two main categories of social authentication in the literature: knowledge-based and trust-based [3]. Knowledge-based authentication requires users to provide information about their contacts and online interactions. Conversely, trust-based authentication relies on social validation from the user's contacts. Furthermore, research is being done to extract the user's social context to validate their permissions [4].

An example of a knowledge-based authentication implementation is shown in Figure 1. In this process, ① represents a user initiating authentication on a system. To verify the user’s identity (or as part of a multi-step authentication journey combined with other methods), ② the system randomly selects a security question from a pre-defined set. The corresponding answer is then ③ retrieved from a dataset of social data collected from the user. This dataset ④ returns a set of possible answers, which the system presents to the user in ⑤. If the user provides the correct response in ⑥, access is granted, and the system is unlocked.

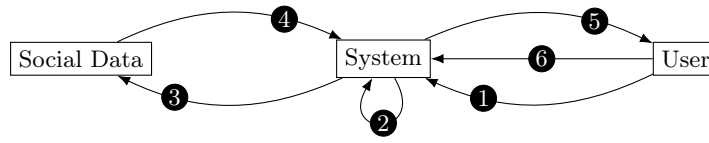


Fig. 1. Example of a knowledge-based social authentication flow and its entities.

One challenge in knowledge-based social authentication is analyzing individual contexts, identifying information users can recall from photos, and understanding the uniqueness of social data [3]. In the current context of language and image recognition models, this data is often publicly available on social networks, making it susceptible to interpretation from attackers.

While these methods have several shortcomings regarding security and usability, they offer an advantage concerning authentication distance. The time required for authentication is a key benefit of these methods. For instance, when suspicious activity is detected on a user’s account, Facebook halts the process and requests that the user identify individuals in photos of friends on the network. Upon successful identification, the system is immediately released [8].

Looking at trust-based methods, a security ceremony involving the concept of vouching is introduced in [5]. This type of authentication is based on the definition of a list of trusted contacts later used to validate the user’s authentication by sending confirmation codes. This scheme may differ in the mechanisms used to set up, send, and collect verification codes [3]. However, defining the list of contacts is mainly manual and depends on the user’s remembering to update it; this problem relates to point ①.

An example of this authentication method is shown in Figure 2. In this approach, the user pre-registers a list of trusted contacts in the system through an out-of-band process for future authentication. When authentication is required, ① the user initiates the process within the system, ② which then selects a trustee from the list and ③ sends them a message containing a one-time PIN through SMS. The user ④-⑤ must then communicate with the trustee to obtain the code and ⑥ enter it into the system to verify their identity.

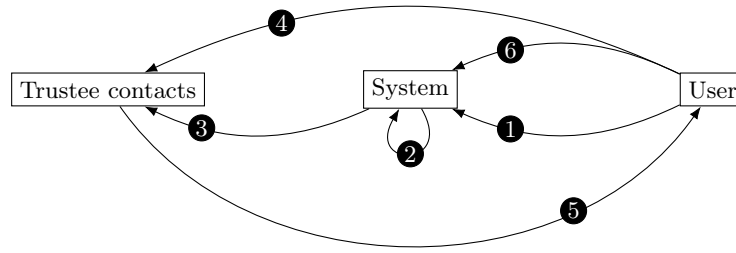


Fig. 2. Example of a trustee-based social authentication flow and its entities.

Although these methods have fewer problems related to public data, as with the knowledge-based method, they have attacks demonstrated in the literature, such as the forest fire attacks [6]. This attack consists of fooling one of the security contacts and then sequentially confusing the others to make them accept a false authentication. Naturally, such an attack is complex and involves the manipulation of several human nodes.

In addition to the attacks, two usability issues are raised: the distance of authentication and the automation of the processes involved. In the first case, since authentication depends on confirming the user’s identity with each of the contacts required for authentication, and given the current existence of deepfakes, there is a delay between starting and completing the authentication process. This problem is related to point ②. Similarly, handing over authentication responsibility to humans reduces automation and makes it difficult to measure trust in social relationships and reflect it in authentication schemes [3].

Also, we have the system based on the results of the i-Contact and k-Contact subsystems [4]. The first subsystem asks users to confirm the identity of neighbors based on eye contact. It then passes this contextual information to k-Contact, determining the users’ authenticity level. As more reports are collected, users gain access rights to more resources. This system may have problems with the authentication distance and the integrity of the reported information.

3 What should social authentication have?

In light of the methods mentioned earlier and the SOAP protocol [12] explained in Section 1, social authentication presents an intriguing fundamental concept: leveraging the credibility of a known individual based in the society around them. However, it also raises concerns regarding conceptualizing the underlying principles and defining the relevant properties, which must be adapted to align with the current authentication needs.

For instance, the methods outlined in Section 2 leverage users’ social and individual contexts to facilitate authentication and authorization. However, in SOAP, this same authentication is shown to have the objective of verifying the authentication of a prover using one or more of their digital identities. This

introduces a divergence in approach: *should we rely on an individual’s real social contexts or the possession of anonymous digital identities?*

We believe that integrating with the real world offers a more advantageous approach in some cases. In addition to the growing difficulties in trusting digital networks, there is also a significant human aspect to consider. *Could a system that mimics or understands the real social fabric, even if only in the context of authentication, foster collaborative benefits?* Such a system would align with how people interact and build trust daily, using the fundamental nature of human relationships to create a more intuitive and effective model.

However, the methods developed thus far based on these concepts lack the mechanisms mentioned above. To illustrate, although trustee-based models are established on real security contacts, they do not automatically adapt to an individual’s social changes. Instead, users must update their contacts manually for this to occur. In conjunction with the authentication distance, this harms the method’s adherence.

In this context, we argue that a social authentication model should ideally be capable of **transparently updating security contacts** without requiring user intervention, ensuring a **short response time**, and maintaining robust **privacy guarantees**. At the same time, it should not rely on easily found information as knowledge-based approaches nor depend on continuous human intervention as in the current context-aware methods.

4 Connecting Physical and Digital Authentication

Given the defined properties and constraints, we are looking for possible modifications to the current implementations and the possibility of new deployments. Note that the ideas discussed here do not necessarily cover all the restrictions and properties we are looking for simultaneously, as reconciling them is a work in progress. In the following, we discuss examples related to point (3).

We recall that the SIM swap procedure involves changing SIM cards while maintaining the same number. It requires user authentication to proceed. However, passwords are an ineffective solution in this case, as SIM swap occurrences are rare, and users cannot recall passwords that are seldom used [14]. Authentication in this context relies on user biometrics or personal information, frequently relying on publicly available data, which has been subject to numerous attacks related to social engineering [9].

We believe that this is an ideal case for trustee-vouching-based authentication since there is no need for the authentication distance to be instantaneous. However, it is essential to develop a mechanism for updating these security contacts that is transparent to users. We propose the following solution to this problem. Given a particular device, a user generates a secret and distributes parts of the secret in pieces across several geographical contexts. Defining temporal and repetition patterns for secret distribution can be achieved via Bluetooth without requiring the user to act. It is necessary to define a way to check the correctness of the assembled secret, which may use asymmetric encryption.

Here, we outline two options for updating contacts based on the chunks distributed. The first option is for the user to receive a notification at regular intervals containing the potential security contacts to select. Only with their approval is this sent to the network operator. The second option is that the operator receives the potential contacts for each context at regular intervals. This could present privacy and tracking issues. Following the initial biometric or knowledge-based authentication, the user must confirm a subset of the secret information to form the split secret.

Figure 3 illustrates the update mechanism as follows: **1** the system generates a key pair and sends the public key to its server; **2** the private key (or secret) is divided into N parts, which are distributed across specific contexts; **3** each part of the secret is assigned to a specific user cluster, requiring the user to collect a subset of k parts (where $k \leq N$) to reconstruct the secret (Shamir’s Secret Sharing); and **4** when authentication is needed, such as in the case of a SIM swap, the user must retrieve at least k parts of the key to successfully reconstruct the secret and regain access to their account. The utilisation of this mechanism is illustrated in Figure 2.

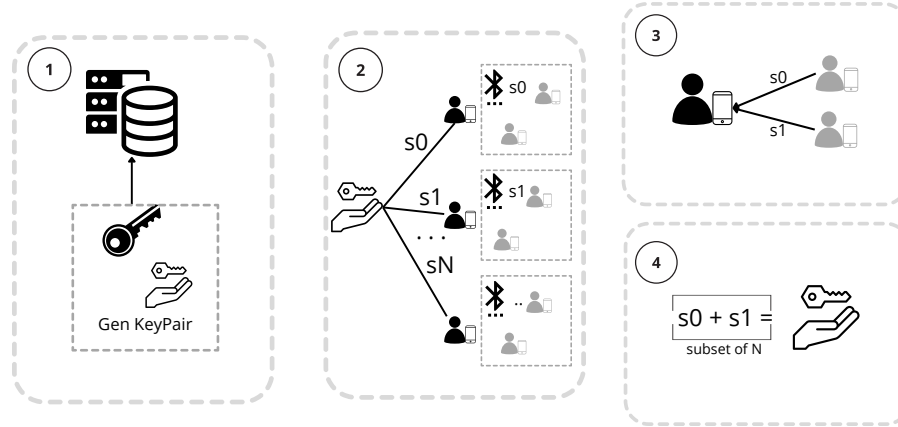


Fig. 3. The following example illustrates the process of updating trustee contacts in the absence of any deliberate initiation of the flow by a human.

This type of authentication can be a valuable tool in corporate access control since managing permissions in large organizations is challenging, creating unnecessary bureaucracy. One potential approach to authorization could involve using social authentication in conjunction with job analysis and creating pseudo-contexts for conversations. To illustrate, a user could add keywords that, if mentioned in a chat, do not require encryption and confirm that they have obtained

another user's permission or identity for access. An authorization may be granted to a user u if they have the support of a number n of other users with permission.

5 Conclusion

The solutions presented above can function with one of the properties identified as crucial for the success of social authentication: transparency of the security contact updating process. Nevertheless, there is still a need to reduce the authentication distance and increase transparency in part of the process. The challenge remains in identifying a generic social authentication process that can be used on smaller scales of authorization. One of the key issues we aim to address is whether social authentication should be based on an entirely online model, with no reference to real-world circumstances, or whether it should be integrated into the existing framework.

Moreover, whether the properties and restrictions raised here truly reflect the characteristics needed to define a good implementation is worth questioning. *Is it feasible to develop a generic framework to facilitate the adoption and popularity of these methods in different contexts?* Ultimately, *when is social authentication the optimal choice over other forms of authentication?* It seems an ideal solution in cases where SIM swap is a factor. Other similar cases can be mapped out, and whether it can be used as the first authentication factor can be answered. These questions are the foundation of our work and the focus of our discussion.

References

1. Adams, A., Sasse, M.A., Lunt, P.: Making passwords secure and usable. In: People and computers XII: proceedings of HCI'97. pp. 1–19. Springer (1997)
2. Alazwari, S., Alsamri, M.O.J., Alamgeer, M., Alabdan, R., Alzahrani, I., Rizwan-ullah, M., Osman, A.E.: Artificial rabbits optimization with transfer learning based deepfake detection model for biometric applications. *Ain Shams Engineering Journal* p. 103057 (2024)
3. Alomar, N., Alsaleh, M., Alarifi, A.: Social authentication applications, attacks, defense strategies and future research directions: a systematic review. *IEEE Communications Surveys & Tutorials* **19**(2), 1080–1111 (2017)
4. Arimura, S., Fujita, M., Kobayashi, S., Kani, J., Nishigaki, M., Shiba, A.: i/k-contact: A context-aware user authentication using physical social trust. In: 2014 Twelfth Annual International Conference on Privacy, Security and Trust. pp. 407–413. IEEE (2014)
5. Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-factor authentication: somebody you know. In: Proceedings of the 13th ACM conference on Computer and communications security. pp. 168–178 (2006)
6. Gong, N.Z., Wang, D.: On the security of trustee-based social authentications. *IEEE transactions on information forensics and security* **9**(8), 1251–1263 (2014)
7. Häring, M., Grohs, J.A., Tiefenau, E., Smith, M., Tiefenau, C.: Can johnny be a whistleblower? a qualitative user study of a social authentication signal extension in an adversarial scenario. In: Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). pp. 259–278 (2024)

8. Jain, S., Lang, J., Gong, N.Z., Song, D., Basuroy, S., Mittal, P.: New directions in social authentication. *Proc. USEC* (2015)
9. Kim, M., Suh, J., Kwon, H.: A study of the emerging trends in sim swapping crime and effective countermeasures. In: *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*. pp. 240–245 (2022). <https://doi.org/10.1109/BCD54882.2022.9900510>
10. Lal, N.A., Prasad, S., Farik, M.: A review of authentication methods. *Int. J. Sci. Technol. Res* **5**(11), 246–249 (2016)
11. Lee, K., Kaiser, B., Mayer, J., Narayanan, A.: An empirical study of wireless carrier authentication for {SIM} swaps. In: *Sixteenth symposium on usable privacy and security (soups 2020)*. pp. 61–79 (2020)
12. Linker, F., Basin, D.: Soap: A social authentication protocol. *arXiv preprint arXiv:2402.03199* (2024)
13. Orman, H.: Twelve random characters: Passwords in the era of massive parallelism. *IEEE Internet Computing* **17**(5), 91–94 (2013)
14. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* **19**(3), 122–131 (2001). <https://doi.org/10.1023/A:1011902718709>, <https://doi.org/10.1023/A:1011902718709>
15. Soleymani, B., Maheswaran, M.: Social authentication protocol for mobile phones. In: *2009 International Conference on Computational Science and Engineering*. vol. 4, pp. 436–441. IEEE (2009)