Evolutionary Consideration on User Authentication: Security, Privacy, and Safety

Chalee Vorakulpipat and Ekkachan Rattanalerdnusorn, *Information Security Research Team, National Electronics and Computer Technology Center*

User authentication needs not only to negotiate with security, privacy, and legal issues through functionality and usability, but also to address safety issues caused by sudden and unexpected changes due to the COVID-19 crisis. This article discusses three generations of user authentication with an emphasis on its technology and human factors. Especially during the crisis, digital transformation moves fast; therefore, the acceptable level of security is more flexible while privacy is still preserved. New technologies and applications such as blockchain, digital identity, 5G/B5G, and SDN/NFV underpinning user authentication will become more practical.

USER AUTHENTICATION: FROM THE PAST TO PRESENT AND FUTURE

User authentication is used to identify a credential and control a user's access to an information system. In fact, we have adopted user authentication in many businesses for decades. However, the objectives and trends of usage have gradually changed. Some new issues have arisen, resulting in an evolution of user authentication. Security is definitely the first reason to authenticate users, but later privacy and legal issues, such as personal data protection, control the use of the authentication mechanism. These days, the COVID-19 pandemic situation has inexorably and radically forced us to be concerned about health and safety in addition to security and privacy.[1]

THE FIRST GENERATION: SECURITY COMES FIRST, BUT FUNCTIONALITY AND USABILITY ARE MAINTAINED

Access control is one of the most important domains in information security to preserve the confidentiality. Identifying users is a must before giving access to authorized persons. Security professionals have tried to develop security mechanisms in different effective ways, and also to increase usability.[2] Multifactor authentication is widely accepted as one of the best methods of user identification. This method confirms at least two factors from a user, ensuring that a thief cannot steal any credentials from the user. The classic multifactor authentication includes something you know (e.g., password, personal identification number), something you have (e.g., key, smart card, token, RFID), and something you are (biometric data, e.g., fingerprint, face, vein). Another recent factor is where you are, which is the user's location detected by a tracking device such as GPS, WiFi locator, etc. Despite having an acceptable level of security, functionality, and usability are other concerns raised by end users, management, and even nonsecurity persons.[3] Having too high security level while lacking risk analysis may lead to degraded functionality or the system becoming unusable.

The use of effective authentication, e.g., multifactor authentication, also needs to balance security and usability (ease of use and time consumed). People need a high level of security, whereas security implementation and risk evaluation consume much effort and time.[4] A conference and exhibition organizer initiated an innovative idea: to use face recognition for participant registration instead of QR codes. The development team, however, was worried about accuracy. Face recognition technology today still shows a high error rate since facial data are not stable and can change with age and face expression compared to other more-stable and more-sensitive biometric methods including fingerprint and iris recognition.[5] Alternatively, using additional factors such as National ID

1520-9202 © 2021 IEEE
Digital Object Identifier 10.1109/MITP.2020.3034617
Date of current version 12 October 2021.

smart cards could be proposed, but having too many factors leads to excessive time commitment.

Similarity, such good authentication methods and the perception of them in the past can be obsolete today due to external factors. In Internet banking, some login mechanisms such as locking accounts after a three-time attempt limit for wrong password or using a one-time password (OTP) from the user's mobile device have become impractical. It is possible that the user has a lot of different passwords used for many systems, resulting in forgetting passwords. Also, if the user is living abroad, a nonroaming mobile is unable to receive the OTP. Many Internet banking developers have reverted to a classic method like passwords or PINs. In fact, in the security field, false negative errors are equally as important as false positive errors. However, in many cases, such as using machine learning to send alerts, false positives can be better addressed.[6] In some situations, authorized users cannot use the system when needed even if it is perceived that the opportunity of being hacked by unauthorized persons is low.

Another example reveals the need for speed over the complexity of security. Recent research on mobile-based time attendance systems using four-factor authentication confirms that despite using four factors, the system must be seamless to the extent that a user should not have to take up to four actions.[7] The system checks all four factors, including passwords from the active directory, devices from International mobile equipment identity (IMEI) or Unique Device Identifier (UDID), facial data from the user's camera, and locations from Service Set Identifier (SSID) or WiFi locator. In actual use, the user only scans his/her face for verification. Simultaneously and automatically, the system checks the password (after the first use), device (after device registration), and location. This system requires four factors, but in fact the user perceives that the system requires only one factor.

Public-key infrastructure is used for authentication, data confidentiality, data integrity, and nonrepudiation. It is one of the most effective security mechanisms. Besides the hardware-based key generation, the software-based one is currently deployed due to its lower cost. In fact, the software-based method is regarded as not truly random, as keys are produced by deterministic software algorithms;[8] the higher secure method, quantum key distribution, has been introduced as a secure solution to the privacy amplification process.[9] Nevertheless, public-key infrastructure is regarded as one of most complicated methods and is the long-term security strategy.[10] From the management viewpoint, it requires a high investment to handle the key, and the cost is iterative.

In this generation, security level is initially indicated as the most important. However, the utilization should be based on the consensus of all stakeholders in the system and business. Functionality and usability are iteratively considered with security mechanisms throughout the life cycle of the system.

SECOND GENERATION: THE ERA OF PRIVACY AND LEGAL ISSUES

Personal data protection has been part of privacy issues in information security for decades, but it has recently become even more essential after the introduction of personal data protection regulation (e.g., General Data Protection Regulation (GDPR) in the EU and Personal Data Protection Act in many countries). Privacy here is the privacy of users who gives or are required to give their personal information to the system for a security reason. Generally, these privacy laws share common practices such as employing a need-to-know basis in which only necessary data can be collected, asking for consent, declaring objectives, and duration of data collection, allowing right-to-be-forgotten policies, and punishment in case of failure to act. System hardening and data encryption play an important role to comply with the law, ensuring that personal data are not disclosed to unauthorized persons. Moreover, a software platform is needed to provide functionalities that data controllers request for supporting the law, e.g., the DEFeND EU Project's platform for supporting GDPR compliance.[11] However, in many cases, this readiness preparation activity for personal data processing is a radical change for SMEs, for which insufficiency of budget is the main problem.

Not only is personal data collection a privacy concern, but its data analysis must also be taken into account. ML/AI-based security mechanisms that come up with user behavior or data models can breach user privacy. Biometric authentication (e.g., face recognition) is still in dispute, particularly today when someone asks for consent even for a CCTV. The privacy acts in many countries state an exemption to bypass consent when used for a homeland security purpose. Nevertheless, it is unclear how exactly to ensure that a security system is intended for homeland security and is thus entitled to this exemption. The development of new technology today has included privacy into its requirements. For example, a study on mixed reality technology (MR) indicates that actions in MR involve personal data, flow, or process,

thus confidentiality, anonymity, and pseudoanonymity should be considered.[12]

In healthcare sectors, security mechanisms to preserve privacy are more complicated. Many systems use a user (patient)-unique ID to identify or authenticate the patient. Although aspects of patient identity like name and hospital number (HN) are not disclosed and are well preserved, some related data such as disease, drug, and date and time can be further analyzed to identify a specific patient. For example, in case where the disease is rare in a community (e.g., COVID-19 or HIV), it is not difficult to recognize a patient. System developers often fail to practice data sanitization because they are not aware of this risk. This mostly happens to in-house developers who provide unsanitized data to outsourced developers.

Importantly, all of these sensitive data assets should be identified by stakeholders, especially physicians, and should be sanitized when being disclosed. In some countries, unique national identification numbers such as Social Security Numbers in the United State, Social insurance Numbers in Canada, and National Identification Numbers in Thailand are regarded as confidential. Not only are these data confidential to the public, but it is also considered not a good practice to store these data in plaintext in data storage. Moreover, despite the uniqueness, these data should not be used as a primary key and foreign key in databases, to prevent increasing the risk of data leakage. All these are related to data governance in which data privacy is included in the system framework in terms of technical aspects and organizational and legal aspects. For example, an event-driven mobile app for tracking patients' activities in a hospital, called EasyHos, is designed to preserve patients' privacy in network layer and application (or data) layer. It does so by a) employing a server storing only need-to-know data to be shared with patients from the main server for the hospital information system (HIS) database that is to be used in-house and b) anonymizing patients' identity throughout the entire system.[13] This concern is also confirmed in a study on privacy in a cloud environment, CloudDLP. It emphasizes automatic data sanitization while not affecting functionalities and scalability for cloud applications.[14]

In this generation, the high level of security with acceptable functionality and usability is still unavoidable, but issues of privacy and law are added and indicated as equally important. Data governance focusing on privacy has played an important role. This has resulted in a number of major changes in terms of modification of infrastructure, data storage, data collection processes, and data handling processes.

THE NEXT GENERATION: SAFETY, RADICAL CHANGES, AND WHAT MANAGEMENT NEEDS TO TAKE INTO ACCOUNT

Digital transformation has been continuously promoted, but it is often not quick as expected due to constraints related to law and people's perceptions; all of these involve information security. The COVID-19 pandemic crisis has radically challenged and stimulated people to drive global digital transformation in many industries.[1] For safety reasons, they fully accept working and meeting virtually through a digital platform (e.g., Cisco WebEx Teams, Microsoft Teams, Google Meet, and Zoom) instead of in person. Despite this, security is still maintained, but the acceptance level of security may be lower without any formal written documents if this can help business to continue as usual. For example, in a formal face-to-face meeting, the presence of participants is an obvious method of authentication. However, during the COVID-19 situation, many arranged face-to-face meetings quickly change to a virtual method where participants only present their faces via their camera to check in.

In the past few years, many governments have created regulations, guidelines, or requirements for video conferencing. In Thailand, the teleconferencing guideline previously required that at least one-third of the quorum must physically attend the meeting at the same venue, and that all attendees must be in Thailand at the time of the meeting.[15] This guideline had since become impractical. Therefore, the government decided to release an updated law to remove the requirements above. However, due to the COVID-19 crisis, the country is on lockdown; thus a formal e-meeting is unavoidable and a new method of authentication for a virtual team has been adopted and accepted. Selfies are increasingly used as a mean of unique ID verification, combined with other factor (s) of authentication.[16] A new norm in e-meetings today is that participants are required to keep their cameras open throughout the meeting. This is for authentication by policy enforcement and also for reasons of "etiquette."

This radical change in business procedures may confirm the flexibility of the acceptance level of security, as mentioned earlier. This change was unanticipated and happened fast; people and even governments have not had enough time to make a long-term plan. However, they have to ensure that business continues seamlessly as soon as possible. Usability is more important than security.

Since the beginning of 2020, the e-meeting platform Zoom has been criticized for its lack of security (Zoom bombing) leading to its ban by governments in some countries. Other threats and vulnerabilities during the crisis include spyware, malware, COVID-19 phishing attacks, and network attacks.[1] Although groups are aware of this, including government sectors, universities, webinar organizers, health support services, and English Certificate test centers, they tend to use Zoom anyway and accept the risks (e.g., low opportunity of being hacked and little damage caused by threats) and usable functionality (e.g., availability, speed, familiarity, compatibility, stability, and seamlessness). Face-to-face transactions, previously indicated as one of the most secure methods of authentication, is now replaced by online face verification. Face recognition with masks becomes an increasing issue due to the requirement to wear masks. The accuracy of the algorithms on occluded faces varies with a number of factors such as coverage, shape, and color of the masks.[17]

Another example is that, despite the acceptance of Internet banking, some sensitive and risky transactions such as opening a bank account still require physical customer authentication (face-to-face) and a national identity smart-card with a unique number. It is perceived that this kind of physical authentication is the most secure method to confirm identity, and other forms of authentication cannot be substitute. Since today people are forced to do social distancing or physical distancing, they do not come to a bank because they want to avoid crowds.

Many banks offered a new, completely online method. It can be a multifactor authentication (e.g., face captured with a video camera and a unique national identity number). This new method is definitely riskier than the traditional one, but both are still a multifactor mechanism. As mentioned earlier, people who work from home are still required to check in. They also authenticate using a new online but weaker-than-physical method. It is interesting that many weaker methods have been quickly accepted that would not have been acceptable before the crisis. An organization needs to determine which transactions require e-authentication, and it is suggested that the selection of the methods be based on the four levels of assurance (from Level 1: little or no confidence to Level 4: very high confidence).[18]

The flexibility in security in authentication methods is based first on safety and then hygiene. A number of vendors have offered an all-in-one multifactor authentication machine including PIN pad, RFID reader, fingerprint, and camera for face recognition. People are required to submit one or more credentials for authentication. It is interesting that at present, they prefer to use contactless methods instead of finger-touching any part of the machine.[19] In fact, this practice was initiated in Asia after the global spread of the 2009 swine flu pandemic, and today it has become the new normal. A number of recent research studies introduce innovative biometric authentication methods such as heartbeat, ear acoustic, external ear, etc. However, all of these need contact and are likely to create a privacy issue, as discussed in the previous section.

Although security level is flexible, privacy is less so, as people are aware of recent privacy laws. During the pandemic crisis, a number of apps have been introduced with the aim of tracking users who were in close contact with infected people and thus prevent the virus from spreading to healthcare workers. These have been criticized regarding the accuracy of the authentication system and user privacy. It has been suggested that the use of these apps should be optional. Nevertheless, the safety factor can influence the adjustment of privacy level, which is contradictory. Previously, some patient data could be anonymized, but now in many countries, patient data are required to be disclosed (internally) due to the epidemic. The security design is more complicated. For example, it is suggested that metadata of an image of a part of the patient's body (e.g., EXIF in jpeg) can be used to identify a patient for further disclosure when requested, but if the data are accidentally intercepted, the data must not be understandable to unauthorized persons.

These flexibility needs and changes open large opportunities for technologists. New integrated technologies to support digital transformation have been quickly deployed in real time,[1] as opposed to the situation before the crisis, in which these were slowly adopted due to the lack of motivation. For example, blockchain-based digital identity has been deployed as a new form of user identification, even in many developing countries.[20] This helps preserve security and privacy in electronic transactions. Government and business sectors have attempted to conduct pilot projects using digital identity for voting (elections) and verifying documents (e.g., contracts and student transcripts). Additionally, Interactive Voice Response (IVR) with one- or two-factor authentication has been recently adopted for mobile voting in areas where Internet connection is limited. Other technologies like software-defined networking (SDN) and network function virtualization (NFV) have been proposed to tackle traffic problems during COVID-19, enabling the system to authenticate and authorize users. Such advanced network technologies are also deployed to deal with

privacy in COVID-19 applications, as confirmed in the Beyond 5G (B5G) framework.[21]

For coming generations, safety is likely to remain a critical concern. Privacy will still be preserved since people are familiar with the right of privacy (both in law and in personal perception). This is summarized as follows.

- Rapid digital transformation enables a variety of virtual teams with new forms of user authentication.
- Contactless authentication for safety (e.g., face recognition and verification with masks) becomes more important.
- New threats related to current situations (e.g. Zoom bombing and COVID-19 phishing) emerge.
- Security and privacy levels are reconsidered based on external factors such as pandemic crisis and law.
- Emerging technologies become more practical and acceptable during the crisis.

Due to the radical change, digital transformation has been unintentionally promoted to maintain business. Thus, the acceptable level of security is more flexible for this generation. Adoption of new technology in the real world is more possible. It is suggested that management, including CEOs, CIOs, IT managers, and stakeholders, reach an understanding of the safety factor and other related factors before effectively conducting change management.

CONCLUSION

Changes related to law, economy, people's perceptions, and the impact of the pandemic on digital transformation create an evolutionary perspective of system authentication. A number of factors of concern have been raised in each generation. To date, the safety concern has been noted, and the level of other existing concerns can also be flexible. Although the acceptable security level, in particular for the authentication process, is sometimes lower, we do not consider that overall security is low. In other words, security is based on people's acceptance, and its aim is to protect information while business continues seamlessly. Traditionally, authentication is viewed as IT infrastructure, but today, it could be indicated as social infrastructure. New technologies that support user authentication, including technologies tested in a laboratory (e.g., blockchain, 5G/B5G, NFV/SDN) will become more practical within a short time to promote digital transformation. Finally, although the pandemic is still happening, it is possible that people are now familiar and comfortable with practices such as physical distancing, e-meetings, online transactions, and even a new model at companies that allow some employees to continue working from home permanently, and it may be hard to dismiss this new normal after the crisis. Conducting data governance with revisions to address all factors and manage the changes are highly recommended.

REFERENCES

1. T. Weil and S. Murugesan, "IT risk and resilience—Cybersecurity response to COVID-19," *IT Professional*, vol. 22, no. 3, pp. 4–10, 2020.
2. K. Schaffer, "Rethinking authentication," *IT Professional*, vol. 21, no. 6, pp. 52–55, 2019.
3. M. Durucu, M. Isik and F. Calisir, "What is more important to internet banking website users: Usability or functionality?" *Int. J. Bus. Inf. Syst.*, vol. 30, no. 2, pp. 232–251, 2019.
4. H. C. Pham, D. D. Pham, L. Brennan and J. Richardson, "Information security and people: A conundrum for compliance," *Australas. J. Inf. Syst.*, vol. 21, pp. 1–16, 2017.
5. V. Agarwal, A. Sahai, A. Gupta and N. Jain, "Human identification and verification based on signature, fingerprint and iris integration," in *Proc. 6th Int. Conf. Rel., Infocom Technol. Optim.*, Noida, India, 2017, pp. 456–461.
6. C. Feng, S. Wu and N. Liu, "A user-centric machine learning framework for cyber security operations center," in *Proc. IEEE Int. Conf. Intell. Security Inform.*, Beijing, China, 2017, pp. 173–175.
7. T. Jaikla, S. Pichetjamroen, C. Vorakulpipat and A. Pichetjamroen, "A secure four-factor attendance system for smartphone device," in *Proc. 22nd Int. Conf. Adv. Commun. Technol.*, Pyeong Chang, South Korea, 2020, pp. 65–68.
8. S. Sadana, A. Lele, S. Tsundus, P. Kumbhare and U. Ganguly, "A highly reliable and unbiased PUF based on differential OTP memory," *IEEE Electron Device Lett.*, vol. 39, no. 8, pp. 1159–1162, Aug. 2018.
9. Y. G. Yang, P. Xu, R. Yang, Y. H. Zhou and W. M. Shi, "Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Sci. Rep.*, vol. 6, pp. 1–14, 2016.

10. D. Dőaz-Sánchez, A. Marőn-Lopez, F. A. Mendoza, P. A. Cabarcos and R. S. Sherratt, "TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 4, pp. 3502–3531, Oct.–Dec. 2019.
11. A. Tsohou *et al.*, "Privacy, security, legal and technology acceptance requirements for a GDPR compliance platform," in *Computer Security*, vol. 11980. Katsikas S., Ed. *et al.*, (Eds), CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019. Lecture Notes in Computer Science, 204–223, 2020.
12. J. A. de Guzman, K. Thilakarathna and A. Seneviratne, "Security and privacy approaches in mixed reality: A literature survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 110:1–110:37, 2020.
13. C. Vorakulpipat, E. Rattanalerdnusorn, S. Sirapaisan, V. Savangsuk and N. Kasisopha, "A mobile-based patient-centric passive system for guiding patients through the hospital workflow: design and development," *JMIR mHealth uHealth*, vol. 7 no. 7, pp. 1–19, 2019.
14. P. Han *et al.*, "CloudDLP: Transparent and scalable data sanitization for browser-based cloud storage," *IEEE Access*, vol. 8, pp. 68449–68459, 2020.
15. P. Sawatdipong, N. Wechsuwanarux, P. Udomsuvannakul and S. Fuengfoosin, "COVID-19 Requirements for E-Meetings for Board of Directors and Shareholders' meetings," Chandler MHM Newsletter, 9 Apr., 2020.
16. Z. Cohen, "Covid-19: Why selfies are in the spotlight for proving ID," *Biometric Technol. Today*, vol. 2020, no. 6, pp. 10–12, 2020.
17. M. L. Ngan, P. J. Grother and K. K. Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre- COVID-19 algorithms," NIST Interagency/Internal Report (NISTIR), 2020.
18. Executive Office of the President, Office of Management and Budget, OMB M- 04- 04, "E-Authentication Guidance for Federal Agencies," 2003.
19. S. K. Udgata and N. K. Suryadevara, "Internet of Things and sensor network for COVID-19," in *Springer Briefs in Applied Sciences and Technology*. Berlin, Germany: Springer, 2021.
20. N. Chalaemwongwan and W. Kurutach, "A practical national digital ID framework on blockchain (NIDBC)," in *Proc. 15th Int. Conf. Elect. Eng./Electron., Comput., Telecommun. Inf. Technol.*, Chiang Rai, Thailand, 2018, pp. 497–500.
21. M. A. Rahman, M. S. Hossain, N. A. Alrajeh and N. Guizani, "B5G and explainable deep learning assisted healthcare vertical at the edge: COVID-I9 Perspective," *IEEE Netw.*, vol. 34, no. 4, pp. 98–105, Jul./Aug. 2020.

CHALEE VORAKULPIPAT is currently the Head of the Information Security Research Team, National Electronics and Computer Technology Center, Thailand. He has been involved in a number of projects addressing Information Security (including ThaiCERT), National e-Science, Mobile Device Management, and e-Health. He has more than 60 refereed publications in these areas. In academia, he serves as a Lecturer for Information Systems courses at universities in Thailand. He has been a keynote speaker at several International Security events. He holds professional certificates including CISSP, CISA, PMP, and IRCA (ISMS Lead Auditor). He is a recipient of the 2019 $(ISC)^2$; Information Security Leadership Award. He received the Ph.D. degree in information systems from the University of Salford, U.K.; the M.S. degree in information technology from Kasetsart University, Thailand; and the B.Eng degree in electronics engineering from KMITL, Thailand. Contact him at chalee.vorakulpipat@nectec.or.th.

EKKACHAN RATTANALERDNUSORN is currently a Senior Research Assistant with the National Electronics and Computer Technology Center (NECTEC), Thailand. For over a decade, he has done extensive research on Information Security, with an emphasis on access control module and network security module. His current research focuses on multifactor authentication. He holds information security professional certificates including CompTIA CASP+, CompTIA Security+ and IRCA (ISMS Lead Auditor). He received the M.S. and B.S. degrees in computer science from Chulalongkorn University. Contact him at ekkachan.rattanalerdnusorn@nectec.or.th.