Common Sense Authentication

In the mid-1970s, 96 kilobytes of computer memory cost more than US$100,000. Today, 8 gigabytes of computer memory can be purchased for less than US$50. That difference demonstrates the huge advancements in information systems in the last 45 years. But not everything related to information systems has advanced at breakneck speed. For instance, in the early days, punch card systems were used to maintain financial and healthcare information. The biggest threat to that type of system was users choosing convenience over security. Today, even with online data capture and real-time systems, little has changed: The biggest threat to system security is still people acting irresponsibly. But there are some common sense solutions to that age-old problem.

> “THE BIGGEST THREAT TO SYSTEM SECURITY IS STILL PEOPLE ACTING IRRESPONSIBLY.”

User Authentication

There are many facets to system security, and they vary by enterprise and application. The one thing all systems have in common is user authentication to allow system access. User authentication provides reasonable assurance that the subscriber accessing the service today is the same as the one who accessed it previously. The US National Institute of Standards and Technology (NIST) issued an update to its Digital Identity Guidelines on 2 March 2020, specifying three levels of security that can be attained and guidance as to which level is appropriate for different applications.[1] Regardless of the authentication method used to obtain access to a system, passwords are almost always a part of it. Thus, ensuring the security of those passwords is a critical function of system security.

Primary functions of user authentication to control employees’ access to a system are segregation of duties (SoD) and providing supervision. In an entity with strong internal controls, user authentication limits the system’s functionality to specific users. For example, the accounts payable clerk can enter payments into the system but cannot approve payments. The accounts payable supervisor can approve payments but cannot enter them into the system. Employees who have neither of these responsibilities can do neither. Although this is a simple example of both SoD and supervision, two key components of a system of internal control, neither is attained if the user authentication method is compromised.

To minimize the potential for compromise of system security, passwords are often restricted in various ways. A common restriction is that a password must include at least one uppercase letter, one lowercase letter, a number and a special character. However, there is little evidence that such practices enhance system security.[2] In a study of the impact of restrictions on user-defined passwords, only 15 percent of passwords were random when restrictions were imposed, compared

Paul C. Schauer, Ph.D.
Is a professor in the department of accounting and information systems at Bowling Green State University (Ohio, USA). Before becoming a professor, he spent 20 years working in public accounting, including eight years as an information systems auditor with Coopers & Lybrand. He has published numerous papers on auditing and information systems.

with 11 percent when they were not. This study also found that 67 percent of passwords contained either a meaningful detail, such as a person, an object or a proper name, or a combination of meaningful details when restrictions were imposed, compared with 59 percent when they were not.[3] Another study found that users who received password guidelines that included persuasive text and sample password creation methods created stronger passwords than those who received guidelines with strict composition rules.[4] These studies clearly question the effectiveness of these widely used restrictions, which may provide a false sense of security. Enterprises that impose stringent password composition policies suffer the same fate as those that do not.[5] What are the alternatives?

The Psychology of Password Selection

To better understand how to ensure that users create effective passwords, it is helpful to examine the psychology involved in selecting a password. The trade-off faced by every user is choosing a complex password that increases system security vs. one that is easy to remember. A study of elementary school students as young as nine years old demonstrated that they had some understanding of the attributes of strong passwords.[6] It is safe to assume that most employees are at least as knowledgeable as nine year olds. This understanding of the importance of strong passwords is often reinforced by training provided by employers. Simple logic leads to the conclusion that employees know they should select strong passwords. The reason they do not is that they prioritize convenience over security. One study found that 36 percent of users were willing to sacrifice security for convenience.[7]

One solution is to make security more convenient, or to make strong passwords easier to remember. For example, rather than using the name of a pet or a spouse's initials as part of their passwords, employees should use phrases that have meaning to no one but themselves. Mnemonics provide one possible solution. For instance, a line from a movie, "I was so busy keeping my job that I forgot to do my job," becomes "iwsbkmjtiftdmj." It appears to be totally random but can be easily remembered by the user.[8] A punch line from a joke or the lyrics to a song can also be used in this way.

Employee Education

People who understand the implications of security breaches are more likely to utilize strong passwords. The factors that motivate people to select security over convenience are vulnerability, severity and fear. Vulnerability and severity are perceptions, and fear is an emotion.[9] If the objective is to encourage employees to choose security over convenience, these three motivational factors must be addressed directly by changing their perceptions and instilling fear.

> “DATA SENSITIVITY MAY BE ONE OF THE MOST MISUNDERSTOOD CONCEPTS IN SYSTEM SECURITY.”

Employees' perceptions of the vulnerability of the information systems to which they have access are based on the information they have. The employer has rules for creating passwords and changing them regularly, procedures for identifying who has access to what data, and an IT department that is dedicated to making sure the system is secure. Based on that information alone, employees believe the enterprise is not vulnerable to data breaches, so there is no good reason to select security over convenience. To change their perceptions, employees can be shown examples of enterprises with similar security controls that have incurred significant data breaches. It is useful to tell employees how many attempts to gain unauthorized access have been detected and prevented. It should be emphasized that past success in stopping unauthorized access does not mean that the next attempt will not succeed. Employees should be reminded that it takes only one. The threat can be personalized by informing employees that their credentials may be the next target of unauthorized access if they choose passwords that are too easily guessed or if they allow others to gain access to their passwords. Employees should be well trained. People trained in password development create stronger passwords than those who have not received training.[10]

Data sensitivity may be one of the most misunderstood concepts in system security. Employees' perceptions of sensitivity are informed by news stories about millions of credit card numbers or Social Security numbers being stolen or a government hacking an enterprise's information system to obtain intellectual property. They may not consider the theft of an enterprise's customer list or its unpatented process for applying finish to kitchen cabinets more detrimental than the theft of money. It is doubtful that employees would identify a large grocery store chain's preferential pricing from a major beverage company or the preferential shelf space the beverage company gets in return as sensitive. However, all these examples give an enterprise a competitive advantage and should, therefore, be considered sensitive. Employees should be educated so that they have the same understanding of the sensitivity of information as management does.

Data are not the only sensitive elements in an information system. The functionality incorporated into that system is sensitive as well. In this technological age, internal controls are integrated with system security. There is a reason why the employee who posts payments to accounts receivable cannot update the customer file. Employees should be educated about why this is so. The more employees understand about the sensitivity of system functionality, the more responsibility they will take to protect it.

Fear is a powerful emotion. Management can use fear in two ways: disciplinary action and peer pressure. Disciplinary action for failure to comply with system security policies is one option. However, research has shown that including these types of policies in an employee manual or other documentation is ineffective. Actions speak louder than words, but for disciplinary action to apply, an infraction must have already occurred. Peer pressure may be a better method. An effective strategy may be a campaign emphasizing that system security is only as strong as its weakest link: Employees do not want to let their coworkers down by being that weak link.

There are other methods to ensure compliance. For instance, managers should lead by example. If management emphasizes system security and makes it part of the corporate culture, employees are more likely to take ownership of system security as well. Reminders of the importance of system security can take many forms including a note in the corporate newsletter, a post on an internal bulletin board, a comment in corporate meetings or a banner that appears on the login screen every few months. When management makes security important, that message spreads throughout the enterprise.

> "IF MANAGEMENT EMPHASIZES SYSTEM SECURITY AND MAKES IT PART OF THE CORPORATE CULTURE, EMPLOYEES ARE MORE LIKELY TO TAKE OWNERSHIP OF SYSTEM SECURITY AS WELL."

Password Policy

Eliminating ineffective requirements such as the use of uppercase and lowercase letters does not mean that all restrictions should be discarded. When instituting policies for the creation of passwords, it is important to remember that security-related restrictions should not adversely affect user convenience. If security is easy, security is more likely.

The length of a password is important. Eight characters is a common minimum, but there is no reason to restrict length. The longer the password, the harder it is to guess. Limiting length also limits the number of possible combinations, which limits the strength of the password.

Restrictions should be imposed on the use of proper names, words in the dictionary and popular phrases such as song titles. Random sequences of letters provide a much stronger password than words because of their randomness.

When changing a password, the new password should differ from the old one by at least three characters. This eliminates the practice of sequencing passwords or merely changing a letter from uppercase to lowercase. For example, if the password Puetkq16 was compromised, it would take little effort for the perpetrator to compromise Puetkr16 or Puetkq17 once it was changed.[11] Uniqueness in passwords is paramount. Security systems often prevent the reuse of previous passwords. A strong policy that discourages the use of passwords that have been used elsewhere should be included in the password change process. Other suggestions for users include the following:

- Complexity is not necessary, but memorability is.
- A beloved cat or dog does not need to be immortalized in a password.
- Bigger is better.
- Users should be willing to jump through a few hoops to keep passwords safe.[12]
- Employees are an integral part of system security.

The alternative to user-defined passwords is assigned passwords. The primary objection to this practice is that users will likely record the passwords somewhere that is easily accessible because they are afraid they will forget their assigned passwords. Easily accessible to the user may also mean easily accessible to others. The solution is to help employees remember their passwords by requiring them to enter the password a second time when they initially receive it. This method results in 42 percent of users remembering the password. Requiring them to enter the password a third time increases that percentage by 17 points, and adding one more required entry increases it to 70 percent.[13] Although it is tedious, requiring this repetition the first few times a user logs on after receiving a new password is likely to eliminate the need to record it.

Customer Access

Customers often have access to an enterprise's system. They may submit electronic purchase orders, or they may be billed electronically. The transfer of electronic documents and data from computer to computer is common. The protocols for initiating such transactions are varied and often quite complex. These methodologies are not addressed here; rather, customer access via the enterprise's website is the focus.

Passwords remain the primary method of authentication for customers accessing an enterprise's website. The restrictions placed on customers' passwords are often the same as those applicable to employees. However, there are differences between the two groups. Customers own some of the data they access, while employees do not. Customers' access is limited to their own data, while employees have access to many customers' data. Customers require privacy. Employees are subject to internal controls. The motivation for security is different for customers and employees, so the restrictions on their authentication procedures should also be different. This is true whether the enterprise is a healthcare provider, an online retailer, an insurance company or a financial institution.

An examination of 76 websites that cover a spectrum of entities identified several interesting characteristics. All of them required a password for authentication. Nine required personal information as a second method of identifying the user during the initial login. Two offered multifactor authentication. More than half used the uppercase letter, lowercase letter, number and special character restrictions on the creation of passwords. All but three required that passwords be at least eight characters long. None required an assigned password that could not be changed to a customer-selected password. One took a unique approach: If the password was only eight characters, the uppercase, lowercase, number and special character approach was used. If the password was at least 12 characters, letters and numbers could be used, but no dictionary words or proper names. If it was more than 20 characters, there were no restrictions.

Enterprises' approaches to authentication procedures for their websites can be characterized by the two-by-two matrix in **figure 1**.

Figure 1—Authentication Matrix

	User selects convenience over security	User selects security over convenience
User does not understand characteristics and benefits of a strong password	Quadrant 1	Quadrant 3
User understands characteristics and benefits of a strong password	Quadrant 2	Quadrant 4

Based on the survey of 76 websites described, many enterprises' authentication policies address those users included in quadrants 1 and 2. The enterprises believe that their users do not understand the characteristics and benefits of a strong password, do not care about security, or both. Quadrant 3 is an empty set. Users cannot select security if they do not understand the characteristics of security. Every enterprise should want its customers to be in quadrant 4, but very few made any effort to get them there. Many required customers to create strong passwords, forcing them to select security. However, almost all of them relied on the customers' perception that strong is better than weak rather than educating them on the benefits of a strong password.

> “CUSTOMERS' MOTIVATIONS FOR SELECTING SECURITY OVER CONVENIENCE ARE THE SAME AS EMPLOYEES': VULNERABILITY, SEVERITY AND FEAR.”

Customers' motivations for selecting security over convenience are the same as employees': vulnerability, severity and fear. An employer can inform employees of the vulnerability of its systems and the severity of the impact of unauthorized access, and it can instill fear of disciplinary action if employees fail to take proper security precautions. If an enterprise informs its customers of the same issues, they may take their business elsewhere, to an organization they believe they can trust. In this case, educating customers about the repercussions of a weak password may be detrimental to the business; merely implying that stronger is better may be the best alternative.

Education is still the key to encouraging customers to use strong passwords. The procedures for password development applicable to employees are just as applicable to customers. A creative approach may lead to more secure passwords.

Conclusion

User authentication methods have become much more sophisticated over time. However, passwords are still widely used for authentication purposes. Implementing procedures for the creation of passwords based on studies of human behavior and common sense can make information systems more secure—an objective that everyone should embrace.

Endnotes

1. Grassi, P.; J. Fenton; “NIST Special Publication 800-63-3 Digital Identity Guidelines,” National Institute of Standards and Technology, USA, June 2017, *https://pages.nist.gov/800-63-3/sp800-63-3.html#mfa-definition*
2. Florêncio, D.; C. Herley; P. Van Oorschot; “Pushing on String: The ‘Don't Care’ Region of Password Strength,” *Communications of the ACM*, vol. 59, iss. 11, 2016, p. 66–74, *https://www.microsoft.com/en-us/research/wp-content/uploads/2016/09/pushingOnString.pdf*
3. Campbell, J.; W. Ma; D. Kleeman; “Impact of Restrictive Composition Policy on User Password Choices,” *Behaviour and Information Technology*, vol. 30, iss. 3, 2011, p. 379–388

4 Yildirim, M.; I. Mackie; "Encouraging Users to Improve Password Security and Memorability," *International Journal of Information Security*, vol. 18, iss. 6, 2019, p. 741–759, *https://link.springer.com/article/10.1007/s10207-019-00429-y*

5 *Op cit* Florêncio *et al.*

6 Coggins, P. E., III; "Implications of What Children Know About Computer Passwords," *Computers in the Schools*, vol. 30, iss. 3, 2013, p. 282–293

7 Tam, L.; M. Glassman; M. Vandenwauver; "The Psychology of Password Management: A Tradeoff Between Security and Convenience," *Behaviour and Information Technology*, vol. 29, iss. 3, 2010, p. 233–244, *https://www.researchgate.net/publication/220208616_The_psychology_of_password_management_A_tradeoff_between_security_and_convenience*

8 Kelly, C. J.; "The Password Is: Useless (Probably)," *Computerworld*, vol. 38, iss. 49, 2004, p. 32, *https://www.computerworld.com/article/2567669/the-password-is--useless--probably-.html*

9 Burns, A. J.; C. Posey; T. L. Roberts; P. B. Lowry; "Examining the Relationship of Organizational Insiders' Psychological Capital With Information Security Threat and Coping Appraisals," *Computers in Human Behavior*, vol. 68, 2017, p. 190–209

10 Weber, J. E.; D. Guster; P. Safonov; M. B. Schmidt; "Weak Password Security: An Empirical Study," *Information Security Journal: A Global Perspective*, vol. 17, iss. 1, 2008, p. 45–54

11 McClure, S.; J. Scambray; "Poorly Chosen Passwords Constitute Most Common Threat to Network Security," *InfoWorld*, vol. 21, iss. 43, 1999, p. 60

12 Renzulli, K. A.; "How to Create a Hack-Proof Password You Can Actually Remember," *Newsweek Global*, vol. 174, iss. 5, 2020, p. 10–14

13 Woods, N.; M. Siponen; "Improving Password Memorability, While Not Inconveniencing the User," *International Journal of Human-Computer Studies*, vol. 128, 2019, p. 61–71