

Jim Routh

ICIT Fellow and Former CSO,
Board Member, and Advisor

The Growing Obsolescence of Passwords

AN ICIT FELLOW PERSPECTIVE
MAY 2021

Introduction

Back at MIT in 1960, Fernando J. Corbató developed passwords while establishing the compatible time-sharing system (CTSS), enabling file permissions to registered users [1]. Sixty years later, user IDs and passwords have served enterprise security remarkably well. In fact, user IDs and password combinations are the predominant credentials used for online authentication on the vast majority of websites, mobile applications, and software-as-a-service (SaaS) applications. Many cyber professionals advocate for increasing the strength of passwords via more character complexity and length, as this will improve the effectiveness of passwords as an authentication mechanism. However, this presupposes that the consumer is the only one who knows their user IDs and password. We are currently facing a reality where passwords are growing in obsolescence, regardless of the length, due to users choosing the same password for multiple websites and mobile applications since they have so many digital assets requiring credentials.

Credentials No Longer Inhibit Cybercrime

Most digital consumers use more than a hundred websites, SaaS, and mobile applications. A user's ability to remember each application's credentials is directly related to how often they use it. Enterprises want frequent interactions to increase their brand awareness. However, digital consumers want convenient, easy access to their data. This is why consumers reuse passwords, as this enables them to reduce the number of passwords they need to remember. Thus, the inherent problem is not necessarily with the credential itself but rather with customers reusing them across digital assets [2].

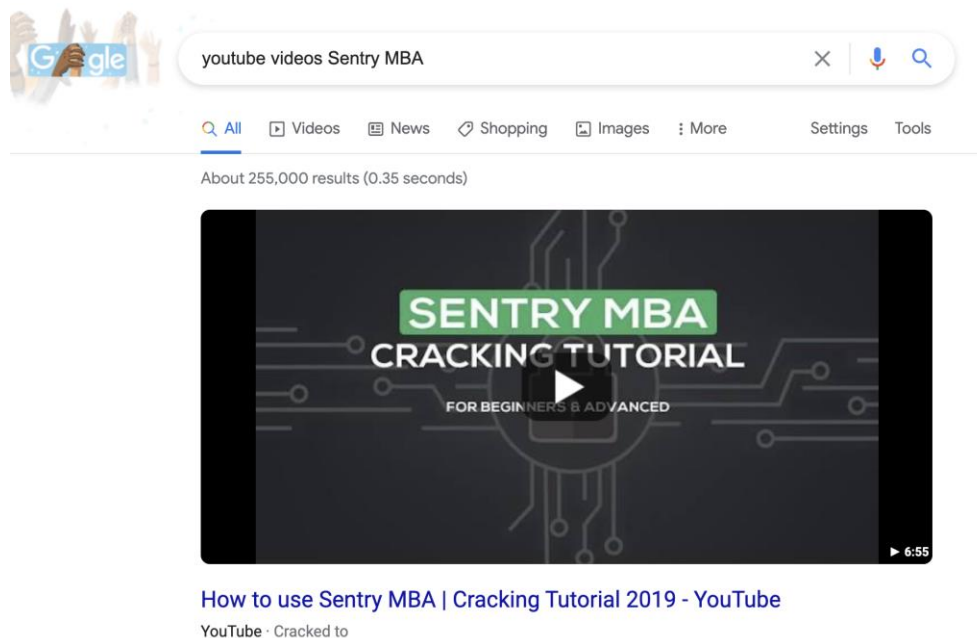
“Technical skill is no longer a prerequisite for cybercriminals who seek to access online accounts using active credentials.”

The most effective way to understand the growing obsolescence of credentials is to look at the situation like a cybercriminal. Over the past five years, cybercriminals figured out that it is easier to use stolen credentials to access systems than find and exploit vulnerabilities in systems. The tools and credentials available to threat actors enable them to use automation to take over online accounts at a scale with very few constraints [3].

Technical skill is no longer a prerequisite for cybercriminals who seek to access online accounts using active credentials. Their first step is to acquire user IDs with their associated passwords in bulk through fraud forums on the Dark Web, where billions of credentials are available. The second step is to use a tool like Sentry MBA, a commercial software that enables individuals to initiate authentication attempts at scale, to try the credentials on active websites. This approach is called *credential stuffing* since it uses credentials in bulk [4]. It typically results in a 2% success rate due to digital consumers increasingly using the same password across multiple sites. In other words, if a criminal buys 10,000 credentials, they can usually gain ownership of 200 online accounts. Once they access the information in those accounts, they can monetize it

through downstream fraud tactics like aggregating the data and offering it for resale, setting up linkages to money-mule accounts, or making fraudulent purchases [5].

Experts estimate that 50-90% of authentication requests on popular consumer digital sites are from cybercriminals [6]. That means the majority of web traffic on web application servers of highly successful enterprises is from criminals attempting to steal customer data. In fact, a large and growing percentage of an enterprise's IT infrastructure cost is subsidizing cybercriminals attempting authentication. This model's economic viability is not sustainable for any enterprise in the long run, and credential theft is at the heart of the problem [7]. There are billions of credentials available and few constraints to stop cybercriminals from using active credentials to commit fraud [8].



If you are curious about the scope of credential stuffing, simply go to your favorite search engine and enter “YouTube Sentry MBA.” You will get approximately 255,000 search results. This is a clear indication of cybercriminals’ desire to perform credential stuffing and their interest in using automation to scale it [9].

It's Time to Think Beyond MultiFactor Authentication

All IT professionals are taught that an online authentication is an event with a beginning and end. The outcome is always binary, meaning accessing the system is either successful or unsuccessful. If access is enabled, then the digital user is trusted with the account information and transaction capabilities provided in the application. If authentication fails, then the user cannot access the contents of the application.

As a result, cybersecurity professionals often recommend adding binary authentication techniques to credentials to improve authentication [10]. If several factors are used, this is commonly called multifactor authentication (MFA). The working premise of MFA is that the system can rely on a second factor to block access if the credentials are compromised. Most commonly, a consumer has to enter their standard user ID and password, then also transmit a one-time password (OTP) sent through text message or email. However, this approach adds friction. To threat actors, the OTP is an effective security and risk management method. Unfortunately, it also adds steps for digital consumers, often making them less happy with the login process. There are alternative MFA options besides OTP, but these options are still designed to fit into the authentication event.

Enterprises that accept the need for consumer friction and implement MFA must recognize that a large percentage of online consumers will not adopt MFA, instead choosing to avoid using online services. While many users will attempt to set up MFA, they will give up during the registration process and opt to simply reset their password whenever they need to access their online information. To them, the friction is not worth the online functionality. In some cases, enterprises see 30-50% of digital consumers avoid MFA options, opting out of or entirely avoiding account registration.

Most cybersecurity professionals believe that consumer friction is part of the cost of protecting sensitive consumer data. It is a constant trade-off between digital friction for the user versus safeguarding sensitive data from threat actors. Highly sensitive data requires more friction, while less sensitive data requires a lower level of friction. Cybersecurity professionals facilitate the balance between consumer friction and protecting sensitive online data. However, it's time to start advocating for management to consider password alternatives that reduce consumer friction while improving risk management at lower costs to the enterprise than traditional MFA approaches [11].

"It's time to start advocating for management to consider password alternatives that reduce consumer friction while improving risk management at lower costs to the enterprise than traditional MFA approaches"

The few enterprises that have dealt with MFA implementation's practical challenges and the resulting consumer friction are attempting to fundamentally transform authentication into a system that no longer relies on credentials. The potential results for these enterprises include:

1. A digital consumer experience with significantly less friction, as there are no passwords to remember.
2. A fundamentally more effective method of online risk management that reduces account takeover.

3. Lower operating costs secondary to eliminating the need for password resets and discouraging credential stuffing.

Better online security with less consumer friction at a lower cost sounds too good to be true; yet, most enterprises do not consider MFA alternatives because they are constrained in their thinking to what they learned about authentication as a binary event. For instance, passwords are no longer a necessary foundation for authentication, and the process of authentication no longer must be a binary event [12].

Considering authentication as a continuous process instead of an event changes the paradigm, opening up new possibilities. For example, an enterprise can capture online behavioral attributes from consumers and develop behavioral patterns for specific attributes. Once these are mathematically represented, any real-time authentication event can be compared to these baseline patterns and scored based on deviation from normal behavior. This can give enterprises a confidence level score, enabling them to program the machines charged with authentication to take various actions depending on different predetermined thresholds. As an example, if the confidence level is high, then full access is provided. However, if the confidence level dips, then access is restricted, or another form of authentication is requested. Multiple applications can use a single confidence score yet be programmed to take different actions based on the protected data's sensitivity. The best thing about a confidence score is that the digital consumer does not experience additional friction, as it is calculated without any input from them [13].

Consumers choose their authentication method when they set up a device. The standard used across device manufacturers is FIDO 2.0. This standard enables iPhone consumers to use Touch ID and Face ID, while Android consumers can use fingerprint or face authentication. While the fingerprint pattern never leaves the device, it is validated using the FIDO 2.0 standard, WebAuthN. However, digital consumers choose to authenticate themselves; this choice can be incorporated into a continuous behavior-based authentication model. In turn, account takeover becomes significantly more difficult since there are no longer credentials to be compromised. Customers and enterprises prefer this since it removes the need for passwords, which means no memorization, reuse, or help desk calls to reset passwords. A continuous behavior-based authentication model will work across channels, offering better risk management and digital consumer experiences while enabling the consumer to choose between channel and authentication options [14].

There are three steps an enterprise needs to take to create a behavior-based authentication algorithm:

1. Make a list of all available attribute information, share it with your privacy team and other stakeholders, and ask them to choose the most benign attributes.
2. Use a data streaming architecture to convert attribution information into a string of numbers and store it as a pattern.

3. Take real-time attribute information, convert it into numbers, and compare it to the pattern created in Step 2 to create a deviation score.

This method will enable businesses to implement behavior-based authentication in a way that threat actors cannot hack. Threat actors will simply take their stolen credentials and automatic login programs and attempt to hack into other enterprises. It is not worth their while to try to break this method. Enterprises don't have to build this capability from scratch. There is an opportunity for enterprises to understand how software vendors may apply the three steps identified above to their product platform.

Conclusion

Today, there are alternatives to using passwords for authentication that are available for enterprises (single sign-on, verification steps, password masking, etc.) [15]. Indeed, many vendors promote their use of "password-less authentication." These solutions represent a positive step toward a better authentication experience and should be considered within the context of improving the digital consumer experience for enterprises [16].

There has never been a better time to do away with obsolete passwords by implementing continuous behavior-based authentication. It will significantly improve user experiences, increasing revenue and profit for enterprises through lower operating costs and higher user adoption. Continuous behavior-based authentication results in better security and customer experience at a lower cost, making it the future for every online enterprise.

About the Author

Jim Routh is currently on the Boards of Supply Wisdom, GrammaTech, Acceptto and ZeroNorth, early-stage cyber security and risk management software companies. He is the former Board Chair for the Health Information Sharing & Analysis Center (H-ISAC) where he served for five years and former Board member for the Financial Services Information Sharing & Analysis Center (FS-ISAC). He has presented to Boards and Board Committees (Technology & Governance, Audit Committees) for many public and private companies as the CISO or CSO, providing cyber security updates and education designed for board members over the past twenty years. Jim brings to the boards a vast business and technology background and is considered a digital and cyber security industry expert and thought leader. He has prepared and delivered several customized education sessions to Board members for the National Association of Corporate Directors (NACD) based on leading cyber security practices. Jim is currently an advisor for Wiz, Devo, Agari, BigID, Gurukul, Data Theorem, Cloudknox, Cleer Security, Picnic, Tala and Virsec. He serves in an advisory capacity and investor for four cyber specific venture funds including: ClearSky, CyberStarts, Security Leadership Capital and Rain Capital.

Jim has a long history in technology and cyber security as a leader and management consultant. He was formerly a cyber security leader for many large companies including:

- **MassMutual**
 - CISO, May 2019 - Dec. 2020
- **CVS Health**
 - CSO, Nov. 2018 - April 2019
- **Aetna**
 - CSO, May 2015 - Nov. 2018
 - CISO, May 2013 - May 2015
- **JP Morgan Chase**
 - Global Leader for Software & Mobile Security, Feb. 2010 - May 2013
- **KPMG**
 - CISO, July 2009 - Dec. 2009
- **Depository Trust & Clearing Corporation (DTCC)**
 - CISO, March 2005 - May 2010
- **American Express**
 - CISO, Jul. 2003 - Sept. 2004.
 - VP Information Risk Management, Aug. 2001 - Sept. 2003.
 - VP IT, July 1998 - Aug. 2001
- **American Management Systems, Inc.**
 - Management Consultant, July 1995 - July 1998
- **DMR Group, Inc.**
 - Management Consultant, July 1988 - June 1995

While at Aetna, Jim developed one of the most mature converged security programs in the private sector. Prior to that he served as an IT leader at American Express and a management

consultant for over a decade for financial service firms.

Jim is a known icon in the cyber security industry. The awards he has received include the Santa Fe Group/Shared Assessments Lifetime Achievement Award, CSO Hall of Fame, ISELuminary Award, SINET Impact Award, Evanta Break Away Leadership Award, InformationSecurity Executive of the Year Award (twice), BITS Leadership Award. He has published numerous white papers [\[17\]](#) [\[18\]](#).

Jim is recognized as an industry leader in digital transformations and innovation in cyber security practices using data science as a foundation for unconventional cyber security controls and enterprise resilience. He offers a board of directors keen insights on the alignment of business strategy with digital transformation in the consumer marketplace.

About ICIT

The Institute for Critical Infrastructure Technology ([ICIT](#)) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

References

- [1] K. Hafner, "Fernando Corbató, a Father of Your Computer (and Your Password), Dies at 93 (Published 2019)", *Nytimes.com*, 2019. [Online]. Available: <https://www.nytimes.com/2019/07/12/science/fernando-corbato-dead.html>. [Accessed: 05-May- 2021].

- [2] J. Overson, "Credential Stuffing – Shape Security Blog", *Shape Security Blog*, 2019. [Online]. Available: <https://blog.shapesecurity.com/category/threat-lab/credential-stuffing-shape-threat-lab/>. [Accessed: 05- May- 2021].

- [3] "Credential Stuffing 101: The risk of bots to your business", *Akamai*, 2021. [Online]. Available: <https://www.akamai.com/us/en/infographics/credential-stuffing-the-risk-of-bots-to-your-business-infographic.jsp>. [Accessed: 05- May- 2021].

- [4] T. Foltýn, "Credential-stuffing attacks behind 30 billion login attempts in 2018 | WeLiveSecurity", *WeLiveSecurity*, 2019. [Online]. Available: <https://www.welivesecurity.com/2019/04/10/credential-stuffing-attacks-login/>. [Accessed: 05-May- 2021].

- [5] P. Muncaster, "Will credential stuffing dominate the threat landscape?", *Barracuda*, 2019. [Online]. Available: <https://blog.barracuda.com/2019/04/02/is-2019-the-year-credential-stuffing-dominates-the-threat-landscape/>. [Accessed: 05- May- 2021].

- [6] N. Mueller, "Credential stuffing Software Attack | OWASP Foundation", *Owasp.org*, 2021. [Online]. Available: https://owasp.org/www-community/attacks/Credential_stuffing. [Accessed: 05- May- 2021].

- [7] E. Chickowski, "Credential Compromises by the Numbers", *Dark Reading*, 2019. [Online]. Available: <https://www.darkreading.com/attacks-breaches/credential-compromises-by-the-numbers/d/d-id/1333733>. [Accessed: 05- May- 2021].

[8] "Bad Bot Report: The Pandemic of the Internet", *Imperva*, 2021. [Online]. Available: <https://www.imperva.com/resources/resource-library/reports/2020-bad-bot-report/>. [Accessed: 05- May- 2021].

[9] S. Gatlan, "28 Billion Credential Stuffing Attempts During Second Half of 2018", *BleepingComputer*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/28-billion-credential-stuffing-attempts-during-second-half-of-2018/>. [Accessed: 05- May- 2021].

[10] J. Killoran, "Password Alternatives: Top 3 Choices for Better Security", *Swoop*, 2020. [Online]. Available: <https://swoopnow.com/password-alternatives/>. [Accessed: 05- May- 2021].

[11] T. Armerding, "Password alternatives: Time to do away with passwords?", *Synopsys*, 2019. [Online]. Available: <https://www.synopsys.com/blogs/software-security/password-alternatives/>. [Accessed: 05- May- 2021].

[12] "Digital Security: 5 Alternatives to Passwords", *OpenMind*, 2016. [Online]. Available: <https://www.bbvaopenmind.com/en/technology/digital-world/digital-security-5-alternatives-to-passwords/>. [Accessed: 05- May- 2021].

[13] R. Rafaeli, "Passwords Are Scarily Insecure. Here Are a Few Safer Alternatives.", *Entrepreneur*, 2018. [Online]. Available: <https://www.entrepreneur.com/article/309054>. [Accessed: 05- May- 2021].

[14] "FIDO Alliance - Open Authentication Standards More Secure than Passwords", *FIDO Alliance*, 2021. [Online]. Available: <https://fidoalliance.org/>. [Accessed: 05- May- 2021].

[15] "What are the alternatives to passwords? | WeLiveSecurity", *WeLiveSecurity*, 2015. [Online]. Available: <https://www.welivesecurity.com/2015/02/05/alternatives-passwords/>. [Accessed: 05- May- 2021].

[16] S. Gerber, "Alternates to passwords: 11 ways to safeguard logins to websites or programs", *TNW / Podium*, 2019. [Online]. Available: <https://thenextweb.com/podium/2019/06/21/alternates-to-passwords-11-ways-to-safeguard-logins-to-websites-or-programs/>. [Accessed: 05- May- 2021].

[17] J. Routh, "Why Data Science is Foundational for an Advanced Cyber Program", *Fsisac.com*, 2020. [Online]. Available: <https://www.fsisac.com/insights/data-science-is-foundational-for-cyber-programs>. [Accessed: 05- May- 2021].

[18] J. Routh, "The Rising Tide of Cloud Computing", *Fsisac.com*, 2020. [Online]. Available: <https://www.fsisac.com/insights/rising-tide-of-cloud-computing>. [Accessed: 05- May- 2021].