BSIMM Paper- Obsolescence of Passwords

Passwords have served enterprises well for more than sixty years and remain the dominant form of authentication for digital assets today despite their growing obsolescence. The resilience of the global software supply chain is at risk due to the continued use of passwords for code repositories and cloud accounts [see articles on Log4j]. Authentication controls for software developer access to code repositories and cloud accounts with access to the build process is now within the scope of accountability for dev ops leaders and software security professionals.

Here is a primer on authentication for devops teams, developers and software security professionals. Password obsolescence is growing not due to a defect in passwords as an authentication method, but a growing defect in our ability to remember complex passwords across all of the digital assets that we come in contact with daily. Digital consumers and employees can't remember passwords for all of the digital assets in use so we compensate by doing one of the following:

1. Use the same password across multiple websites and mobile apps for some of the digital assets
2. Register with a password that we don't remember and simply use the password reset function the next time we visit the website
3. Avoid signing up as a registered use whenever possible

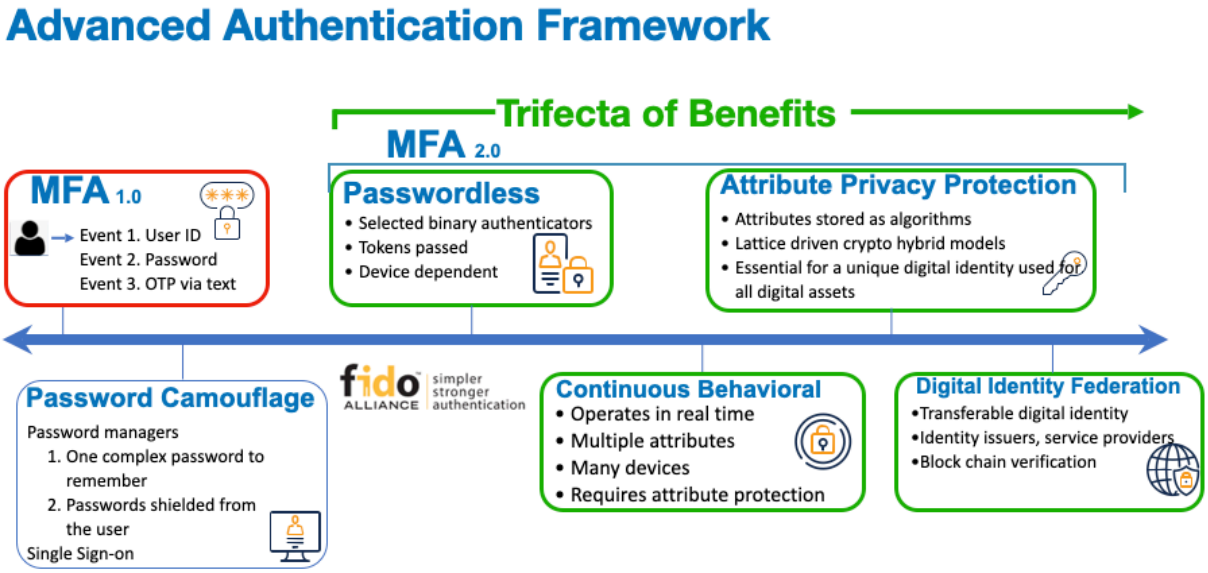
The first password was put into use by Fernando J. Corbató in 1960 for the folders in use for a mainframe based time-sharing application at MIT. Everyone uses passwords every day including systems administrators, help desk professionals, DBAs, developers and access administrators who have privileged entitlements in enterprises. Cyber criminals discovered several years ago that their ability to harvest authentication credentials through phishing and purchase on the dark web creates the opportunity to try out these credentials across websites at scale. Approximately 2% of the time the criminal will have success in taking over the online account as a direct result of our use of the same password across websites. This technique is called credential stuffing and is enabled by the billions of credentials that are readily available on the dark web. It turns out that using credentials to take over a web account is easier for criminals than exploiting known software vulnerabilities since online users with credentials have a higher level of trust in networks and are shielded from activity monitoring using log files.

If you'd like an indicator for how widespread credential stuffing is today follow these steps:

Go to your favorite search engine on your laptop and enter this into the search window: Sentry MBA Youtube. Check the number of results your search query generated. It's likely to be over half a million results. What these means, is that approximately half a million Youtube videos were created to teach you and anyone else how to use a password cracking platform called Sentry MBA for credential stuffing. If you change your search query to Sentry MBA download, you'll discover how many websites distribute Sentry MBA for free. It's generally free since cyber criminal syndicates sell the compromised credentials that enable the password cracking software to work. It is not uncommon for consumer branded websites with popular loyalty programs to receive over 90% of the web traffic to their site originate from cyber criminals using Sentry MBA or another password cracking platform for credential stuffing. High traffic websites for digital consumers spend millions of dollars on botnet protection software to attempt to block log in attempts using software at scale vs. traffic from an individual digital consumer.

The answer to these specific problems appears to be simple yet has proven to be be somewhat elusive for enterprises dealing with digital consumers; get rid of passwords and the need to store credentials and criminals are forced to go back to exploiting software vulnerabilities. Let's identify what choices enterprises have today to reduce account takeover by eliminating credentials (secrets, passwords) and implementing authentication methods that

don't use passwords. This applies to authentication for digital consumers, employees and software developers. I call this advanced authentication and I developed this framework to help me



understand what types of choices enterprises have to eliminate passwords and improve authentication methods. This framework is not intended to be product specific or to be based on an analysis of the market for authentication options. It's a guide to the types of options available to an enterprise to consider going forward. It also applies to software developers, devops teams, site reliability engineers, and software security professionals.

The first category is what I refer to as MFA 1.0 for Multi Factor Authentication. Some refer to this as 2FA or two factor authentication. Federal industry regulators and government agencies at all levels have advocated MFA for more than a decade and what they mean is using additional authentication factors on top of the user ID and password credentials. Unfortunately, this simplistic type of MFA (MFA 1.0) rides on the shaky foundation of the password that is growing in obsolescence and often entails the use of a one-time password generated through SMS received on a cell phone. SMS messages to a mobile device can be spoofed resulting in the two factors being defeated. MFA 2.0 represents multi factor authentication that does not use a password, often referred to as "passwordless" options.

The next category in improving the authentication experience for digital consumers and workers is what I call password camouflage. These are options that insulate the difficulties of remembering complex passwords from the end user through single sign on platforms or password management software. In the first case if I'm a worker in an enterprise and I successful log into the network (using the required authentication method) then I'm verified through a SAML and receive access to selected applications without having to re-enter my credentials. In the second, case I can choose to use a password manager or if I'm an employee my employer may provide me with one. Password managers operate under a principle that the consumer only has to remember a single password to open access to the "vault" or data base of passwords while relying on the password manager to automatically generate random complex and unique passwords for all of the digital assets in use. There is significant improvement in user experience which is positive but the top four consumer password managers have all suffered breaches where the credentials were harvested by criminals.

The next category is passwordless, meaning that there are no passwords generated or used for authentication purposes. This is a relative new category (enterprises have had commercial product options available for the past 4-5 years) and there are differences in both product design and use of standards, specifically a standard called FIDO2 from the FIDO (Fast Identity Online) Alliance. The FIDO Alliance membership is comprised of both enterprises in addition to software providers and mobile device manufacturers. The beauty of FIDO is it enables any digital consumer to choose their mobile device and configure the biometric authenticator they wish to use on their device while then using the same authenticator along with a cryptographic key for mobile software applications or to log into a website. The passing of cryptographic keys happens in the background so the user experience is seamless. There are a growing number of use cases being identified and implemented as the FIDO Alliance continues to evolve industry standards supported by the World Wide Web Consortium (W3C).

Many of the commercial products for a passwordless experience provide options to use FIDO2 in addition to the use of authenticators bound to a device and the unique configuration of the device. This category begins the enterprise process enabling the achievement of three primary benefits to the enterprise called the trifecta of business benefits:

1. Significantly improve the digital consumer experience resulting in more digital users using more functionality of the digital asset
2. Substantial reduction in the costs of dealing with account takeover (ATO) incidents in addition to a corresponding reduction in brand damage
3. Gradual dismantling of password reset infrastructure and a corresponding reduction help desk calls contributing to a lower operating cost model for the enterprise

The trifecta of business benefits applies to all categories beyond password camouflage.

The next category requires a bit of a shift in the way IT professionals have always thought about on line authentication. When we first learned about technology we were taught that authentication was an event, with a beginning and an end that resulted in a binary outcome (successful log in or not). Continuous behavioral authentication requires enterprise technical professionals to consider an adjustment to what we learned by using a continuous process as opposed to a specific event. Specifically, a digital consumer demonstrates behavioral attributes in how they choose to use the technology components and devices of their choice that can be represented mathematically and stored as a pattern. The real time flow of measuring the same attributes allows a comparison to the pattern represented numerically. The comparison can be expressed in a deviation of the pattern and measured with a score that indicates high deviation or low deviation. A threshold can be determine for the deviation score to trigger automated action (additive authentication requirement, challenge questions, etc.) all in close to real time (in milliseconds). This means that enterprises can measure and act on deviation score triggers without human involvement in close to real time. It's a game-changer for cyber security control design and offers additive authentication factors without any friction for the digital consumer since the pattern matching is occurring in near real time while the digital consumer is engaged with the digital asset. Password less options combined with cryptographic based standards significantly improve the digital consumer authentication experience while also eliminating account takeover since there are no credentials that can be harvested by criminals.

The next category is not mature currently and includes methods for reducing the risk of exposure of credentials of any kind to cyber criminals. Many of these methods are relatively easy to adopt for example:

- When designing authentication controls choose attributes that are benign to the digital consumer (eg: use swipe sensitivity or browser configuration instead of using browser history) and aligned with privacy practices

- Only store attribute information in algorithm form and never store raw attribute information for a digital consumer

Some emerging methods involve the use of advanced mathematics to create a private key using fuzzy extraction from a public key. This category offers the potential of technology breakthrough leading to the issuance of a single digital identity that can be used by consumers for multiple digital assets. Your driver's license registration may in the future result in a digital identity to be used by your bank for access to your bank accounts. If any kind of digital consumer attributes can be protected through advanced cryptographic options from exposure to the issuing authority as well as everyone else, then the potential for a single digital identity used everywhere remains feasible.

The possibility of the use of a single digital identify would require the evolution of appropriate interoperability standards between issuers and digital assets that are actually being worked on today. Similar to the substantial effort and positive results of the FIDO Alliance, there are organizations emerging today that are working toward the release of standards and frameworks to promote advanced authentication techniques used widely across an ecosystem. The Global Assured Identity Network (GAIN) is working on a framework through open source methods. (https://openid.net/gainpoc/) and the Accountable Digital Identity Association (ADI) has published a standard for interoperability that is evolving to support the future needs of issuers and users of digital Identities. (https://adiassociation.org/)

The advanced authentication framework encourages enterprises to make decisions on the choices available within each category to improve authentication for the digital consumer experience and the worker experience while understand the likely industry evolution over the next decade. Like all technology choices and decisions there are trade-offs and not necessarily a single answer for all enterprise use cases. The industry has shown a preference to technology platforms that specialize in consumer authentication and others that offer improved authentication for the workers in an enterprise despite commercial products that support both. Enterprises are exercising their commitment to consider alternatives to the password today but at a relatively low rate. Unfortunately, the majority of enterprises appear to be seeking alternatives from commercial providers of cloud computing resources and commercial software providers for authentication options and these providers are sticking with MFA 1.0 options while listening closely to enterprises who are unaware of the advanced authentication framework and the options available to them. In the interim, digital consumers have to deal with the friction of password management while cyber criminals reap the benefits stealing of credentials.

You can apply these lessons learned and authentication options in the framework to the software pipeline management process that requires effective authentication controls to protect the software supply chain. Access to code repositories, cloud accounts, privilege access to the software build process and production environments require advanced authentication capabilities. Software security professionals have to add knowledge of advanced authentication to their skill set to keep up with their accountabilities for resilient software.