vericlouds

Why Common IAM Solutions for Identity-based Attacks Aren't Really Working?

When faced with the problem of data being open to all users on an early, 1960's mainframe computer, Fernando "Corby" Corbato rather nonchalantly assigned passwords to protect user private data, and the concept of the computer password was born.

Fast forward to today, and no one ever would have ever guessed that such an easily implemented mechanism would lead to difficult-to-solve complications in the present computing landscape. From the moment the password was born, the password has been under attack utilizing every conceivable attack vector from password grabbers to key loggers to rainbow tables and every form of brute and mathematical attack.

Since around 2010, the computing world has witnessed a significant increase in the occurrence of breaches. These breaches have given rise to a pernicious threat in the form of billions of compromised credentials, creating a significant attack vector on the computing landscape.

Many organizations have undertaken to mitigate this threat leveraging a number of popular security technologies that, in the end, turn out to be insufficient in mitigating this threat some surprising ways. The authors of this paper aim to investigate and dig deeper into a number of the most popular approaches to help expose some of the insufficiencies behind each approach. Then we will provide our recommendation for the most straight forward and reliable approach to more fully mitigating the problem of compromised credentials.

The Current Landscape: The Internet as Anytown

Before we get into investigation of these approaches, let's consider an analogy to help frame and give reference to our discussion.

The internet can easily be likened to and mapped analogously to physical space like a town. We'll call our analogous internet town "Anytown."

In Anytown today, criminals drive around on the streets with keys that have been stolen from consumers and businesses in previous heists (as with the many real-world breaches since 2010). 60-70% of residents in Anytown simply use the same key for their houses, cars, gym lockers, bicycle locks, bank safety deposit boxes, and when they select keys for doors at work (i.e. points of access). Criminals in Anytown understand that, statistically speaking, these keys taken from previous heists are therefore really quite valuable for potentially opening a lot of locks with essentially no effort and minimal to no detection.

Early on, criminals in Anytown brute-forced their way into homes and businesses or took the time to carry out heists that required some level of sophistication. But as criminals exited these heists, they grabbed as many keys (stored by these businesses) as they could.

They now first attempt to use as well as share and sell these stolen keys when attempting to break in. With most Anytown residents still using the same keys for all of their doors, criminals often don't have to force their way in any longer. They can simply pull out their giant key rings, keep "stuffing locks" with billions of stolen keys, and when the doors open, walk right into homes and businesses often completely undetected.

The real-world internet currently looks and still works a lot like our analogous Anytown.

By: Stan Bounev and Chris Olive

Popular Approaches to Mitigating Compromised Credentials

What's really amazing is that in the real world, as with Anytown, both criminals and organizations have access to a nearly identical *list* of the keys that have been stolen. The simplest, most straightforward solution for Anytown and the real world is to actively and passively make sure no locks match keys that have been stolen. And to stipulate that no new locks can be created that match stolen keys.

Unfortunately, many organizations in both Anytown and the real world have decided to take other approaches that are insufficient in the face of these compromised keys or compromised credentials.

We'll proceed from here to discuss these approaches and dig into some of the layers to understand why these approaches are insufficient in and of themselves in stopping criminals from continuing to leverage compromised credentials to breach organizations. Along the way, we'll occasionally map the real-world solution back to our Anytown analogy to hopefully bring clarity as to why these solutions fall short of adequately mitigating the problems associated with compromised credentials.

Password Policies

When compromised credentials first became recognized as a legitimate threat, many organizations immediately focused on password policies and felt simply strengthening those policies would be sufficient. In many cases, users were forced to reset their passwords more often. Within our Anytown analogy, this would be the same as organizations requiring new keys and locks on doors (points of access) on a more frequent basis.

The problem with this approach is that it simply reinforces the same behaviors and forces end user inclinations to occur on a more frequent basis – more insecure passwords are formed or old passwords recycled, reused or only slightly altered. This has actually accelerated the problem of compromised credentials and further grown the databases of insecure passwords criminals have collected, leading to the next, futuristic phase of compromise in which criminals have begun leveraging analytics over this larger pool of derivative data to include predictiveness in their compromise attempts.

This is one of several reasons the National Institute of Standards and Technology (NIST) has recommended organizations *stop* forcing periodic password resets. Periodic password resets are no longer considered best or leading practice and for a number of good reasons.[1]

Simply changing all the locks on a more frequent basis (or reusing old locks and keys) has not made Anytown nor the real-world internet any safer from compromised credentials. Therefore, simply strengthening password policies has to be considered an insufficient solution to the problem of compromised credentials.

Single Sign-in On (SSO)

Nearly every IAM-related vendor likes to believe and stipulate that their niche in the IAM space contributes in a positive way to better securing organizations. Single Sign-On (SSO) vendors are no different.

SSO vendors suggest that SSO helps solve the problem of compromised credentials for a number of reasons. One reason given is that elimination of many passwords for end users to create and remember provides the opportunity for each end user to concentrate on creation of a single, strong, secure and unique password. A second stipulation is SSO lessens the exposure of compromised credentials since fewer less secure passwords are available for compromise.

While these SSO stipulations have some theoretical merit, in reality, they don't always translate into the reality for which we'd all hope. Certainly, when considering the concept of SSO, we find ourselves faced with the irony that end users have in essence "created an SSO experience for themselves" by continuing to leverage the same password across multiple accounts and applications.[2]

For SSO applied within our Anytown analogy, doors to homes and organizations would be opened not by keys but by tokens generated from a trusted source. The use of a token is considered trusted and access is granted based on the token being presented in a trusted way, through what is called an "assertion." These tokens and assertions are often still generated by a password given to an often centralized trusted "token maker" (an identity provider or IdP in real world terms). So "SSO" in Anytown would mean many or even most doors would open with trusted tokens as well as traditional passwords. Let's hold on to that analogous reference and concept as we dig a little deeper into the assumptions around SSO as a strong deterrent to compromised credentials.

SSO Isn't Seen by Users as An Opportunity For Strong Passwords

At the actual point in time of password creation or reset, users unfortunately don't see SSO as an opportunity to focus on creation of a secure, unique password. SSO is simply a welcomed convenience on the road to a better user experience (UX). Better and more rigorous password policies can help in these situations. But when forced to create even one complex, secure, and unique password, users will typically resort to writing that password down or generating the most memorable password that fits into what may be a stronger policy.[3]

1 https://www.riskcontrolstrategies.com/2018/01/08/new-nist-guidelines-wrong/

2 The rising popularity of SSO in conjunction with cloud services simply hasn't removed or changed the fact that 60-70% of users still leverage the same password across all accounts or simply use a weak, insecure or compromised password for SSO.

3 Also consider, when it comes to compromised credentials, a compromised password in hand is an exact match password – length, strength, so-called "uniqueness," and complexity of the password are therefore essentially meaningless.

SSO Leverages Already Established Identity Sources

SSO implementations, in an effort to better integrate to organizations typically rely on an already established identity source for creation of the SSO experience. So “an” existing Active Directory (AD), LDAP, or other directory service is often selected as “the” identity source upon which the SSO experience and implementation sits. Unless all users are forced to reset their passwords in alignment with a better and more stringent password policy designed to help mitigate weak or reused passwords, SSO implementations simply lay over the top of identity sources that exist in the same state of compromise as previous to SSO.

If an SSO Password Is Compromised… Ouch!

If an SSO user has or chooses a compromised password, then not only does SSO not mitigate compromised credentials scenarios, but rather better and more quickly enables access to more applications through a compromised credential used in an SSO or identity provider (IdP) store.

SSO Can Introduce New Attack Vectors

SSO is reliant on behind-the-scenes technologies such as Security Assertion Markup Language (SAML), HTTP Federation (HFED)[4], trusted headers, tokens, IdPs and more. SSO simply changes the usage and scope of compromised credentials and can even introduce new threat vectors; it doesn’t mitigate compromised credentials by dealing with them head on.[5]

Not Every Application Can Be SSO’d

Not every application in organizations can be brought under SSO. Legacy applications that contain sensitive information and cannot come under SSO still abound in significant numbers within organizations. And without SSO, these applications still require separate, non-SSO’d credentials for access, their own lifecycle management of these credentials, and therefore remain susceptible to access through compromised credentials.

SSO Often Doesn’t Eliminate Non-SSO Access

SSO in most circumstances for almost all applications often does not eliminate non-SSO access to those applications. SSO is primarily a convenience technology that elevates the user experience, helps eliminate user and administrative fatigue and reliance on help desk, and helps lower organizational help desk costs and spend. SSO does not eliminate the fact critical applications can often be accessed both with localized credentials as well as through federated credentials and tokens used in assertions.[6]

Allowing locks in Anytown to be opened with both tokens as well as passwords, and where the password needed to generate a token may itself be compromised, has not made Anytown nor the real-world internet any safer from compromised credentials. SSO has many benefits and may in theory provide better opportunity for users to generate stronger passwords and for fewer sources of compromise. But the reality in most organizations is that for its many upfront promises, SSO is woefully insufficient in and of itself for mitigating compromised credentials.

Identity Assurance (IA) & Multifactor Authentication (MFA)

As the problem of compromised credentials has persisted, a new perspective has been advanced by both IAM vendors and organizations – especially vendors of multifactor authentication (MFA). This is the assertion that due to the large volume of stolen credentials, everyone should simply consider all primary credentials as "compromised" and instead look to better assure identities as users request access.

In most cases, stipulation is made that identity assurance (IA)[7] can be gained by forcing access requests through a configurable gauntlet of authentication factors. This is what is meant by “multifactor” and is most often realized in the tactical solutions of MFA and Adaptive MFA[8]. Some vendors and organizations claim that the use of MFA has mitigated the problem of compromised credentials by up to 99%. That level of mitigation seems almost “open and shut,” and has caused MFA to be heralded and viewed as “silver bullet” in mitigation of compromised credentials.

In our Anytown analogy, real world MFA would amount to placing more doors with differing types of locking mechanisms in front of existing doors and making users prove they have all the differing types of keys to all the doors, often within a restricted timeframe (after which, some of the locks actually change). If users do prove to have the right keys to all these doors within a timeframe, we can assure ourselves the users are who they say they are. It stands to reason statistically that most criminals aren’t going to be able to harvest all of the necessary keys to all the doors within a short timeframe. This is why MFA looks on the outside to be “open and shut” – a near complete mitigation to compromised credentials.

But as with password policies and SSO, MFA has kinks in its armor as well. And criminals are well aware of these kinks and use these to successfully circumvent MFA in some cases. Let’s dig a layer deeper into MFA to see how it really works and why even MFA is insufficient in reliably mitigating compromised credentials.

---

4 HTTP Federation or HFED, is “SSO slight of hand” that simply relies on stuffing saved credentials into web application login forms. SSO HFED therefore can’t even deliver on the promise of a true single password or a lessened password footprint since an HFED application is simply accepting its own localized credentials that have often been stored by the SSO provider and may differ from a user’s primary SSO credentials entirely.

5 Tokens and API keys used in SSO federation and for API access can then become another threat vector. Reference the recent Facebook API breach as just one example: https://arstechnica.com/information-technology/2018/09/50-million-facebook-accounts-breached-by-an-access-token-harvesting-attack/

6 See footnote 4.

7 “Identity Assurance” (IA) can mean a number of things, depending on how it’s viewed. In some cases, IA is meant to point more to identity proofing or the assurance that a human or machine identity is what it says it is at point of initial establishment. In other cases, it’s meant to describe assurance of an identity at point of access in time or its continuance as an established identity. In this paper, our meaning is based on the latter meaning: the assurance of an identity at point of access or its continuance.

8 Adaptive Multi-Factor Authentication (MFA) is essentially MFA in combination with analytics to create and leverage risk analytics for authentication.

MFA Only Helps If It Is in Place

The first clear and obvious weakness of MFA in mitigation of compromised credentials is that it first of all must be deployed and then adopted and used. Adoption rates for MFA still hover around 30% even when MFA is made available. Obviously, if MFA isn't deployed, it can't be adopted or used. Many organizations still haven't deployed MFA nor made its usage mandatory.

So as effective as MFA is for point in time protection during *interactive* access attempts, it's pointless if it's not deployed as well as adopted.

Attacking the MFA Lifecycle using Compromised Primary Credentials

If MFA is in fact in place and has been adopted, criminals simply return to the reality that what they hold in the form of potentially valid compromised credentials still represents a *primary* factor (and not simply a first or single factor). And that primary credentials are still often very relevant and effective in attacking and circumventing MFA additional factors by attacking the MFA lifecycle.

The bottom line is that primary credentials are still relied upon heavily for remote identity proofing, initial registration to MFA, emergency or temporary MFA access, password reset, and almost all other factors associated with lifecycle around MFA. Criminals understand the mechanics around the MFA lifecycle and simply step back and attack these key areas using compromised primary credentials in an effort to skirt or intercept MFA for high value targets – and often accomplish this with surprising effectiveness.[9] MFA may well be deployed, but all it takes is one link in the MFA chain to rely on single-factor, primary authentication, and compromise can still occur, effectively unlinking an entire related MFA chain.

MFA Can't Cover All Points of Access into Organizations

The biggest kink in the MFA armor is this: Not all access into organizations can be covered by MFA. In our Anytown analogy, buildings in Anytown consist of not only doors where intended walk-in (real-world interactive) access takes place, but loading docks with big garage doors, windows, backdoors, fire escapes, and the like also exist. Not all of these points can accept "multiple doors" (real-world additional factors) being added.

In the real world, access into organizations works much the same way. Not all access is created equal. Access takes many different forms within enterprises, including network services, machine and non-human or non-user access. For criminals looking to attack organizations, non-user IDs are an excellent choice for compromise for a number of reasons. One, organizations typically have their hands full simply addressing human access across the Identity Access Management (IAM) spectrum and have little to no governance focus on non-user IDs. Two, these non-user IDs can often outnumber human IDs by a 2:1, 3:1 or even greater ratio.[10]

Non-user IDs and access where MFA cannot be set in place therefore represents high risk and often unmitigated threat to organizations. These vectors represent a very desirable and sought-after attack on organizations, both due to lack of governance and optics, as well as an intentional circumvention of MFA when organizations have adopted and deployed it.[11]

Threat Intelligence (SIEM, UEBA & SOAR)

Artificial Intelligence (AI), Machine Learning (ML), and Predictive Analytics are all the rage on the present business and compute landscape. Broadly speaking, these technologies, applied to the problems within cybersecurity through Security Information and Event Management (SIEM), User Event Based Analytics (UEBA), and Security Orchestration, Automation and Response (SOAR) as Threat Intelligence solutions, all certainly have their place and value.

Collecting these together under the moniker of Threat Intelligence and stipulating them as effective mitigations to the problem of compromised credentials is very difficult to accept as true mitigations to infiltration by compromise. Where password policies, SSO, IA and MFA at least make the attempt or promise to halt infiltration into organizations by bad actors to start with, Threat Intelligence merely takes the stance that instead of prevention, focus needs to be on early detection and response to infiltration. Proponents of Threat Intelligence are in effect throwing up their hands and stating compromise is going to happen, so organizations should just accept this as a reality and get better at responding.

In our Anytown example, this would be like real-world businesses stating insuring access to buildings by authorized individuals isn't important any longer. Everyone should simply get better at detecting the authenticity of occupants in the building. We stop worrying about if the door is locked and we prepare to properly identify and fight the intruder already inside the building.

9 Quick examples: A criminal being the first to an MFA single-factor (due to "chicken and egg" scenarios) self-registration page; single-factor personal email addresses as a verification or password reset mechanism (still an unbelievably popular option, even within large enterprises) or for On-Demand tokens (ODA); phone SIM swapping for initial ODA; use of OSINT, single-factor email break-ins and social engineering to answer "personal questions" intended for identity proofing and reset of MFA or emergency access at help desk. These are only several of many ways to leverage compromised primary credentials to skirt MFA.

10 One author of this paper was privileged to participate in the cleanup and remediation of one of the largest and most popular breaches in history inside an organization of approximately 360,000 employees. For non-user IDs outside of normal employees, approximately 26MM forms of access were identified across only part of the enterprise estate (cloud and other parts of the enterprise technology stack were excluded for the sake of expediency), with approximately 2MM distinct non-user IDs identified. Assuming only 10% of the non-user identity estate and merely 0.2% of compromise, this would still represent approximately 400 non-user IDs in a state of compromise. https://www.linkedin.com/pulse/problem-non-user-ids-organizations-today-chris-olive/

11 IMAP attacks are another great example of access where MFA cannot be put in place as a mitigation strategy and represents susceptibly to compromised credentials and credentials stuffing. And email, once compromised, represents high value in determining and creating additional vectors of attack and even interception, circumvention and/or redirection of MFA. https://www.helpnetsecurity.com/2019/03/20/imap-based-password-spraying/

Creates Compliance Concerns

A lot of the data available from HIBP is raw (even though returned in SHA-1 format) and represents real data from organizations that is thereby ingested into other organizations that leverage this service. This raises and creates a number of compliance concerns that have to be analyzed and carefully understood closely in the face of the European Union General Data Protection Regulation (EU GDPR) and other strict compliance standards for which many organizations operating in various industry silos and verticals must concern themselves (e.g. HIPAA, PCI, FERPA, etc.).

Free Isn't Commercial

Finally, as with any free service run by a single individual, when issues arise through the use of data provided by HIBP, there is no service level agreement (SLA) and no support. Free services typically run "as is" and do not provide enterprise-grade services.

As mentioned, Troy is an independent security researcher and attends to and runs HIBP as he has time. This means time available for continuous aggregation and assimilation of on-going breaches, meaning aggregated, up-to-date breach intelligence data isn't guaranteed. The data at HIBP is only as valuable as it is current and kept up to date.

Troy has done a wonderful job through this service in raising awareness over the problem of compromised credentials and providing great data as a free service for security researchers. But a free solution is only intended to go so far and only provides limited actual value to organizations that need to formulate accurate actions based on highly manicured, managed and up to date data with the highest number of compromised credentials and the lowest possible percentage of false positives.

Commercial Compromised Credentials Detection

The benefits of leveraging a true commercial compromised credentials solution simply cannot be overstated. Returning to our Anytown analogy, we are reminded again that in that scenario, *both criminals as well as organizations have access to a nearly complete list of all the keys that have been stolen through break-ins over the years in Anytown*. **All organizations in Anytown need to undertake as the most direct approach is to make sure no keys on the known list will open any of the locks in Anytown. Locks that match are re-keyed (changed) and no locks can be created that match keys on the list.**

Organizations leveraging a commercial compromised credentials solution realize the best, most direct benefit and assurance against compromise in the following ways:

Commercial Grade Quality

As with any commercial, paid solution, there are inherent benefits attached to commercial solutions. Support, quality of service and quality of data are all attributes of commercial offerings. Quality of service means SLAs with fewest false positives and quality of the data available containing the highest number of credentials. Attempting to mitigate compromised credentials without having full access to the highest possible number of credentials means some credentials in a compromised state will not be found and flagged. Knowing that the results are accurate allows organizations to rest confident in whatever actions they deem appropriate in leveraging this kind of intelligence for mitigation.

Better Security

Obviously when dealing with passwords in general, organizations are dealing with as well as potentially exposing this highly sensitive aspect of their technology estate to a commercial compromised solutions provider. A commercial provider should be taking great care to:

1. Not store any sensitive information provided by an organization.
2. Make use of a Zero Trust method for detection or at least do not request access to passwords.
3. Perform credentialed comparisons in a safe place, preferably on the client side and not in the cloud.
4. Shield itself from knowing the outcome of credentialed comparisons through obfuscation and/or encryption.
5. Acknowledge and operate in line with privacy and compliance guidelines.

In short, a good, secure, reliable commercial compromised credentials solution provider should not only be providing the largest and best intelligence store around compromised credentials and the highest accuracy wrapped by an SLA. It should also be providing all of those things to its customers taking a secure, zero-trust approach.

Easy Integration into Any Platform

APIs are extremely popular and are expected as a normative approach to consuming intelligence services intended for augmentation and integration with existing solutions. A commercial compromised solutions provider will:

1. Assist with and provide support for API integration.
2. Provide reference implementations as reference points for integration with the most common Identity Management solutions.
3. Continuously update and feature manage their APIs to bring on-going and future value to the investment in their services.

A good, reliable commercial compromised credentials solution provider will be invested in seeing their solution quickly and easily integrated and providing quantitative value to their customers.

Conclusion

While most of the industry is aware of the problems associated with compromised credentials, the perspectives around the problem have tended to vary, leading to varying strategies that cannot confront the problem nor the threat in a direct manner and deliver the highest, most assured level of mitigation. The varying approaches we have mentioned and inspected in some depth, while immensely valuable to organizations in other ways in terms of layered defense in depth, still leave organizations open to the threat posed by compromised credentials.

The most direct approach to solving the problem of compromised credentials is to deal with the credentials themselves, continuously checking for compromise and mitigating while disallowing new credentials to be created that match any existing compromised credentials.[15]

A commercial compromised credentials solution provider provides enormous value to organizations as reliable intelligence tightly coupled to existing Identity Management technologies in a way that provides simple, reliable, direct and on-going mitigation of this growing and pernicious threat to organizations.

Bios

Stan Bounev – Stan brings close to 20 years of product management and business development experience in the financial services and technology industries, and a passion for cybersecurity and identity management.

Prior to co-founding VeriClouds, Stan spent 8 years at Microsoft driving the product planning and product management of key capabilities and security features of Outlook.com and Windows Client.

As the VeriClouds CEO, Stan is currently managing all operational aspects of the company as well as working with customers and prospects to protect their infrastructure from attacks with compromised credentials.

Chris Olive – Chris has over 20 years of extensive experience in cybersecurity as a strategist, consultant, evangelist, speaker, writer, and hands-on technologist for the US Government, the Fortune 500, and large international companies all over the world.

Chris brings passion, unique insights, and a nuanced and intuitive blend of communicative, collaborative, marketing, and hands-on technology skills to the table wherever he is engaged and is adept at presenting to, architecting and advising businesses on securing and mitigating risk in their organizations in a way that provides business value.

Chris has a BS in Computer Science from Harding University and is currently a Senior Identity Engineer for RSA Security, a recognized leader in securing organizations world-wide.

15 NIST Special Publication 800-63B, Section 5.1.1.2: "When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to... breach corpuses." The framers of NIST understand, rightly stipulate and insist that the most effective, reliable, direct approach to compromised credentials mitigation is comparison against known compromised credentials and breach corpuses. https://pages.nist.gov/800-63-3/sp800-63b.html