Transition to Multi-factor Authentication

A common tactic

While network attacks have become more complex, the compromise of passwords continues to be one of the main tactics used to successfully attack networks and data. One of many examples occurred in September 2017 when Deloitte, one of the world's largest accounting firms, reported a breach that resulted in the compromise of client emails and data including those of government agencies and other large enterprises. After further analysis it was concluded that the attackers gained access to the email server through an administrator account that was protected only by password [1]. Public estimates indicate such data breaches can cost an organization millions of dollars [2]. While smart timeout and lockout mechanisms can almost prevent brute force attacks on remote services, passwords are often easily compromised through methods such as dictionary attacks on password hashes, keylogging, sniffing of passwords sent in the clear, malicious TLS inspection, social engineering, and lack of user awareness.

Although selecting strong passwords and setting timeout and lockout policies play an important role in securing an enterprise, relying on password strength alone is not sufficient in many cases. There are plenty of social engineering, password-guessing, password-cracking, and password-sniffing tools and techniques available for attackers to gain initial access or maintain persistence within networks. This is why the concept of Multi-factor Authentication (MFA) has evolved as one of the most effective controls to protect an enterprise. Password-based authentication involves use of a single credential to authenticate to a system. MFA requires two or more factors for successful authentication, preferably including at least one that is resistant to replay attacks. When properly implemented, MFA presents a significant obstacle to attackers trying to gain or maintain access to an organization's network: attackers would have to expend resources to coordinate a compromise of all factors in the MFA system before the user discovers the compromise and resets or revokes the associated credentials.

What is Multi-factor Authentication?

Authentication is the process of verifying the identity of a user to a system that provides access. MFA is an authentication method that combines two or more authentication factors to validate a user's identity. There are three types of factors of authentication: something you know (e.g. a password), something you have (e.g. a token), and something you are (e.g. biometrics). Examples of MFA implementations include:

- Inserting a chip-based ATM card (something you have) and entering a PIN (something you know)
- Swiping a badge (something you have), scanning your fingerprint (something you are), and entering a PIN (something you know)
- Entering a password (something you know) and receiving a one-time-use code via SMS on a registered mobile device (something you have).

An important consideration for the effectiveness of an MFA implementation is how the factors are protected and combined. In the first example, a stolen card is likely to be reported and replaced before the PIN can be guessed. In the second example however, the badge swipe value might be able to be recovered remotely. If the verification provides user feedback on each of the factors (e.g. invalid badge, misread fingerprint, and wrong PIN are all valid responses for failed authentication), an adversary can verify that they have the correct input for the badge and biometric input, and independently attempt to guess the PIN. Similarly, for the third example, an adversary can discover the password before attempting to discover the SMS-based input, and then try to intercept the one-time-use code. Basic MFA mechanisms like the third example are nearly as easy to exploit as passwords [3], whereas those that effectively combine and protect the factors require a more coordinated attack against two or more factors.

What are the threats?

There are methods that target each of the authentication factor categories. The strength of MFA decreases when all the factors can be compromised independently without alerting the legitimate user. To counter this, monitor the use of MFA credentials and alert on unusual access behavior that might indicate a compromise has gone undetected by the legitimate user. One can also implement time and/or location based attributes to limit access based on the legitimate user's behaviors.

Factors you know are always at risk for disclosure or guessing by an adversary. Social engineering, open source research, key logging, and capturing successful authentication traffic are all tactics that adversaries regularly use to reveal passwords, PINs, or answers to security questions. Kerberos tickets and password hashes based on user passwords can also be stolen from compromised devices and replayed (aka Pass-the-Ticket and Pass-the-Hash). At the time of this writing it is increasingly common for one-time-password mechanisms that send passwords over partially unsecured communications (e.g. PINs over SMS) to be compromised by rerouting those messages [4]. Use MFA that include both what the user knows (with timeout and lockout) and what the user has. For U.S, government employees, a Personal Identity Verification (PIV) token provides such a combination that optionally allows fingerprint activation to be used as a second factor, with a PIN, to provide a third factor. Commercially available tokens, such as the YubiKey (FIPS or Universal-2-Factor modes) or SecurID time-based one-time password tokens for example, also effectively combine what you have with one or more of what you know or what you are.

Physical tokens and devices can always be lost, stolen, or duplicated. In some cases an adversary with physical access to the token could tamper with the token to change its behavior or use it to infect the host it interfaces with, though for many modern tokens this requires significant skill, investment, and risk [5]. Consider using devices that include physical security mechanisms, such as tamper evidence or response. The NSA recommends using devices validated by the NIST Cryptographic Module Validation Program to the FIPS 140-2 standard. FIPS 140-2 level 1 validation is sufficient for most devices that will remain in a user's possession and can be easily revoked and replaced if lost; devices validated to levels 3 or 4 provide tamper evidence or tamper responses (respectively) that can provide additional protection if the device is temporarily left unattended in high risk environments. Some MFA token systems depend on central authentication servers, certification authorities, and/or token issuance systems, and these servers should be very carefully protected and isolated.[1]

Advanced threat actors can replicate biometric factors. For example, when Samsung first released the fingerprint authentication feature on the Galaxy S5, groups of researchers and hackers claimed to have successfully unlocked phones—including one belonging to a German official—by using photos of users' fingerprints and inexpensive fingerprint recreations made with household materials [6]. Liveness testing has improved some biometrics, but they are often still based on information accessible from used drinking glasses and high-resolution photography. Since biometric spoofing is a concern, consider using biometric factors as an addition to two others if strong authentication is needed.

Some systems may not support MFA, and can only work with traditional password authentication. Attackers that detect the use of these systems on enterprise networks may focus their efforts on compromising the passwords for and gaining access to those systems, rather than expending their resources trying to break into MFA-protected systems. Employ privilege access management[2] devices to enforce MFA to devices that only support password-based authentication. Such PAM solutions can proxy the request to the target devices using randomly generated, well protected, one-time-use passwords and can implement dynamic access control rules to limit the damage an adversary can cause if they succeed in hijacking an authentication mechanism or bypassing the PAM.

Rather than try to compromise each MFA factor individually, attackers may try to find and gain persistence on a host where the factors come together. Manage host security configurations[3] to reduce the risk of an adversary gaining access

[1] Network isolation is a core concept further explored in *Segment Networks and Deploy Application-Aware Defenses*, part of NSA's Cybersecurity Top 10 Mitigations packet.

[2] Privileged access management is further explored in *Defend Privileges and Accounts*, part of NSA's Cybersecurity Top 10 Mitigations packet.

[3] For more details, see *Actively Manage Systems and Configurations*, part of NSA's Cybersecurity Top 10 Mitigations packet.

to the host (where they can recover and/or abuse all the factors). Consider including device authentication and health checks as part of a dynamic access control system.

Train users and administrators regularly on the specifics of the MFA systems they use and the associated threats. All users and administrators of the system should be able to identify a compromise of one or more of the factors when it happens and know the appropriate responses and reporting requirements. Timely and non-punitive reporting, revocation, and replacement processes will minimize the burden on users and minimize the time an adversary can abuse a compromised MFA.

Adaptive access control

In addition to authentication, access decisions should include other identity attributes and integrate behavior analytics using these attributes to recognize and respond to high risk requests. Examples of identity attributes that are beginning to be used include where you request access from (e.g. geolocation) and when you request access, as well as traditional attributes like organizations and roles. Modern, adaptive, attribute-based access control systems are recommended for access to high-value resources such as domain and enterprise administrative functions and especially sensitive or mission critical data. Such systems can recognize a request from an unusual place, at an unusual time, or for resources inconsistent with the user's role, and can detect and respond to other anomalous requests. Adaptive access control responses can range from alerting administrators on suspicious access attempts to denying access.

Make things easy for the user

Some MFA credentials make authentication easier and faster than ever before. For example, fingerprint readers and facial recognition offer seamless and near-instantaneous authentication (appropriate only for low-risk environments since biometrics alone often do not provide strong assurance). When properly implemented on devices with lockout features, random PINs are far shorter than full passwords and can often be more easily remembered. While MFA can provide security and usability benefits over traditional password-based authentication, failure to carefully plan the transition from passwords to MFA credentials can create unnecessary burden. MFA systems require users to enroll in the system, and a lengthy, confusing enrollment process could disrupt users. Users will need to become accustomed to keeping track of their tokens, and accommodations for forgotten tokens must be made. Account lockout resulting from too many consecutive false password or PIN authentication attempts will frustrate users, and users may dread the thought of an MFA system that now includes two or more potential points of authentication failures. Lockout recovery mechanisms that require the user to follow complicated procedures and find an issuance/re-issuance infrastructure that is hard to access can become frustrating and reduce productivity. These usability drawbacks can lead to users' rejection of an MFA system; and, even if MFA is mandated, upset users might avoid putting effort into protecting their credentials, leaving MFA factors more susceptible to compromise.

Enterprises must consider the impact to users that MFA systems present and carefully coordinate the transition to gain users' acceptance. Train administrators, help desk personnel, and users on the MFA system as well as the enrollment plan. Describe key usability improvements that MFA provides over password-only authentication. For example, the need to memorize and manage multiple complex passwords for multiple systems has always placed a burden on users; an MFA token with PIN authentication can help significantly reduce this burden. Anticipate potential issues with user access requirements and successful and failed authentication behavior. Provide a reliable and readily available issuance/re-issuance and compromise reporting infrastructure to minimize the pain associated with reporting and replacing lost or stolen tokens. Finally, train users and administrators on the benefits of and procedures for authentication factor revocation.

Make things tough for the adversary

Multi-factor Authentication is a beneficial tool designed to defend against an array of authentication attacks, which rely on stealing user credentials. Traditional password-based authentication is susceptible to password-guessing, password-cracking, and password-sniffing tools and techniques, and users can be tricked into divulging their credentials through social engineering campaigns. A compromise of single-factor authentication costs attackers minimal resources as they attempt to get inside enterprise networks and therefore allows them to spend their remaining time and effort conducting more advanced attacks from the inside. And, as seen in the Deloitte attack, the compromise of one set of credentials can

result in the exposure of even more credentials. MFA's uniting of two or more additional or alternative factors protects against threats targeting the inherent flaws with password-only authentication. Proper MFA implementation will cost the adversary more resources, increase the chances of detection, and significantly hinder their ability to exploit the authentication system.

Works Cited

[1] Hopkins, N. "Deloitte hit by cyber attack revealing clients' secret emails." The Guardian. 25 September, 2017. [Online], Available: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

[2] Ponemon, L. "Calculating the Cost of a Data Breach in 2018, the age of AI and the IoT", (2018, July 11). Retrieved March 28, 2019. From https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[3] Cox, S. "When Two-Factor Authentication Fails: Rethinking The Approach To Identity Security." Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/02/21/when-two-factor-authentication-fails-rethinking-the-approach-to-identity-security/#7aed40bb6fea

[4] Barret, B. "How to Protect Yourself Against a SIM Swap Attack" (2018, August 19). Retrieved March 28, 2019. From https://www.wired.com/story/sim-swap-attack-defend-phone/

[5] Boudriga, N. "Smart Card Security: The SIM/USIM Case". Information Systems Security, Auerbach – excerpt from Security of Mobile Communications, New York: Auerbach Publications (2009). Retrieved March 28, 2019. From http://www.infosectoday.com/Articles/Smart-Card-Security.htm

[6] Can Your Face Be Hacked On An iPhone? (2018, May 01). Retrieved January 29, 2019. From https://www.tracesecurity.com/blog/articles/can-your-face-be-hacked-on-an-iphone

Related NSA Cybersecurity Guidance

- Privileged Access Management, 25 Apr 2017 https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/privileged-access-management.cfm
- Least Privilege, 10 Apr 2017 https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/least-privilege.cfm
- Hardening Authentication, 03 Nov 2016 https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/hardening-authentication-update.cfm
- Hardening Authentication (NSA Video), 21 Jul 2016 https://www.youtube.com/watch?v=fXpKl3Jam-w

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov