AUTHENTICATION ASSURANCE FOR TODAY'S FEDERAL MISSION AND WORKFORCE

Kayvan Alikhani
Senior Director of Technology, RSA

Stephen Ellis
Global Public Sector Marketing Lead, RSA

ABSTRACT

Vulnerabilities to IT systems that are reliant on a gate-keeper that is limited to the single factor UserID/password authentication method are well known. Securing the Federal government requires a strong authentication paradigm. This white paper explores options and alternatives – particularly in the light of the Federal government's mission and workforce.

OUR ADVERSARIES ARE ACCESSING FEDERAL NETWORKS

Recent breaches to the Federal government IT systems have shown that our adversaries were able to access networks and remain on them for substantial periods of time. This has caused great cost to address and incalculable damage to our national security and the mission of the Federal government. These incidents have shed a stark light on the weakness of single factor authentication (UserID/password). As with Government systems, commercial infrastructure is similarly under attack. Recently, a foreign criminal syndicate was able to hack its way to 1.2 billion username and password combinations.[1]

Indeed, we've seen an explosion of authentication-related dire headlines. This should not be surprising to professionals following the security landscape. In point-of-fact, RSA's 2015 Cybersecurity Poverty Index™ (based on the NIST Cybersecurity Framework) showed that nearly 75% of survey respondents reported that their organizations lacked the level of maturity necessary to address today's cybersecurity risks. [2]

REQUIREMENTS FOR THE AUTHENTICATION LANDSCAPE

When we hear the news about yet another site or service being hacked, where large amounts of sensitive user information has been compromised – we have to specify: what was compromised? Often, the answer is: user credentials. A hacker uses someone's stolen user-name/password to hack into a site to accomplish the malicious mission of copying/altering/deleting/inserting data into a system.

There is plenty of analysis out there on the risky nature of passwords – yet we still rely on them every day. What are our options and alternatives? How do we reduce the 'importance' of unintended access to username/passwords combinations as we know it?

There really is no simple answer. In the halls of Government today, many are looking at the widely adopted CAC/PIV card technology to provide authentication to privileged users. The CAC/PIV card approach can be helpful, in certain scenarios, to harden access to some applications used on desktop and laptop computers. This technology, however, doesn't address many of the use-cases of how today's Federal workforce serves its mission.

CAC/PIV CANNOT MEET TODAY'S FEDERAL WORKFORCE NEEDS

Today's Federal workforce depends on an ever-expanding technology ecosystem in their day-to-day work. They access on-premise and cloud infrastructure; use mobile devices (both government-issued and BYOD; access IT infrastructure such as routers and switches; communicate with IP-enabled devices that have their own "identity" considerations; engage with citizens and other constituents on social media and other third-party managed platforms; and use an impossibly large and ever-changing number of applications. Federal workers are located around the globe, including conflict areas and enemy territory. Contributing to the mission of the Federal government are millions of non-employee users (contractors, state & local government agents, researchers, foreign government personnel, etc.). Unfortunately, these scenarios aren't addressable by CAC/PIV cards.

To secure today's mission and today's workforce, we need to consider new approaches that are cost-effective, easy-to-deploy, and support how the today's Federal workforce works on its disparate and vital missions.

ONE TIME PASSWORDS

One time password technologies (including tokens such as RSA SecurID) are proven and have been around for years. Though not new, this technology is seeing an explosion of renewed interest given its low-cost and support of a wide range of use-cases (devices, infrastructure, mobile, applications, etc.)

Token codes, either through a separate device or accessed via an app are a proven, user-friendly way to provide regular 2-Factor authentication. Token-based OTP solutions, such as RSA SecurID, provide a unique key-code that is refreshed at frequent and regular intervals. The one-time password – something you have – is coupled with a secret personal identification number (PIN) – something you know – to create a combination that is nearly impossible for a hacker to guess or defeat with a brute-force approach. This authentication technology provides anytime, anywhere, secure access to VPNs, wireless access points, web applications and network operating systems and more.

BIOMETRIC AUTHENTICATION

We are seeing even more innovations in the mobile space that take advantage of the built in capabilities of smartphones and tablets including high resolution cameras for facial recognition, high fidelity microphones for voice recognition, location & motion sensors, touch screen and fingerprint sensors, etc. Device makers are moving fast to make sure they include support for native biometric authentication methods in their products.

Soon, we will be hard-pressed to buy a modern smartphone/tablet/phablet/laptop that is not equipped with a native and user-friendly biometric authenticator (such as fingerprint, face, voice, iris, or other behavioral verification technologies). Apple's Touch ID, for example, has introduced us all to a friendly alternative to using plastic credit cards when completing purchases at point of sale terminals. Many organizations have started allowing for Touch ID to be used even in remote transaction scenarios (purchase from home), either as an alternative to the UserID/Password based authentication, or as a complement to it.

There is momentum behind biometrics. Gartner predicts that, by 2016, 30 percent of organizations will use biometric authentication on mobile devices, up from five percent today.[3] Goode Intelligence predicts that by the end of 2015 there will be 619 million people using biometrics on their mobile devices.[4]

This sounds great, but there are some cautions. Security researchers have noted concern around the implementation of the biometric scanning on the devices. The "where" and "how" a biometric record is generated on the device, where is it stored, and what applications or machine level functions can get access to it and under what circumstances are all potential points of vulnerability. If a hacker can have "root" access or if a device is "jailbroken" security threats rise substantially. After all, a digital version of a fingerprint can be manipulated in the same way as a stolen password credential. The caution here is not to assume that biometric capabilities equal more security without further understanding of how the user, device, and applications interact.

A LAYERED APPROACH PROVIDES A HIGHER LEVEL OF TRUST

Though not a panacea, biometric authentication should be investigated as part of your layered approach to an increasingly flexible and usable world of multi-factor authentication. Addressing the advancing threat landscape with an additional factor, "something that you are" can add a higher level assurance option for strengthening secure access to information when combined with "something you have" or "something you know".

There are a wide range of user authentication technologies that have potential on mobile devices, based on biological "biometrics" such as fingerprint, face or voice print, iris structures, ear shape, heartbeat analysis as well as "behaviometrics" like keystroke analysis and handwriting.

Biometrics can be joined with OTP/token-based authentication methods to provide stepped-up multi-factor authentication and pleasant mobile user experience. The added security comes from a combination of biometrics with OTP authentication as a part of a "defense in depth" authentication strategy (such as geo location + biometric voice or facial recognition + pin). Voice and face biometrics methods are broadly possible on popular mobile devices being used today and yield high user acceptance levels, so we anticipate starting there. In addition, to avoid rejecting the "right" user due to environmental constraints (voice verification may not work if used on a busy street, face verification may fail in a dark restaurant, fingerprint verification may fail when used with greasy hands), combining biometric methods with other methods (graphical pins, one time tokens, out of band messaging, use of wearable/carry-able devices, etc.), enables us to replace complex password policies with more secure solutions, that improve accuracy and usability.

DEVICE-BASED AUTHENTICATION: IN THE DEVICE WE TRUST

Looking forward, we are witnessing a massive shift towards "trusting" device-based user authentication.

As we look to apply better cyber-hygiene to Authentication we should consider adopting practices to:

- Stop hosting all such user credentials in easy to smash-and-grab places.
- Reduce the importance/significance of the credentials on the server, if compromised.
- Make it more difficult for hackers to 'impersonate' real users (or steal their login credentials).

Establishing a stronger "trust" relation with devices, from which all users actually access sites and services, resonates with all of these approaches. Once we've trusted the device, then we can trust the user using the device, and to get there, we move (at least part) of the user credentials away from the servers, and onto the trusted devices; a distribution that changes the threat model dramatically.

The end-state of this strategy is for less data on the server – which in turn reduces the importance of user credentials on the server. Here, for a hacker to get their hands on the same tens of millions of credentials, and to make use of user credentials, they would have to physically steal that many actual devices (phones and tablets), AND successfully hack into each and every one of them.

One unintended consequence of this strategy is a shifted focus to targeting the devices of specific users.

With a shift-to-device approach, the device becomes a more interesting place to harvest credentials for a targeted, single person. In other words, an organizations IT footprint has decreased its own exposure by making it the user's problem to make sure that his credentials are safe on his personal device. To address this threat we need to have a simultaneous strategy to lock-down the device.

Unauthorized/unintended access to data can never be 100% prevented, especially for the data at rest (even if such data is encrypted). To address this weakness many devices are now equipped with a protected environment, that runs in parallel to the standard operating system. This protects sensitive data and secures sensitive operations on such data by creating a Hardware Root of Trust, or a Hardware Anchor. We're seeing a common design philosophy, shared by Apple, Microsoft, Samsung, Google and other key device makers: They are all moving towards one-form-or-the-other-of Mobile (or portable) Hardware Security Module (HSM).

HSM is a facility that has been historically used by software running on servers to store/execute sensitive data/operations.

Analogously, the Trusted Platform Module (TPM) initiative has sought to address this issue for laptops, desktops, and servers. TPM has seen support and adoption already in the Federal government, particularly within the Department of Defense.

CONCLUSION

Across the Federal government, there is an urgency to strengthen security by moving beyond a password-only authentication regime. We know this is a work in progress and will take time. We also know that solutions have to address the way the Federal workforce operates. One example: are strategies being developed to manage employee's personal passwords as well as work resources – given that their devices are used for both?

Federal IT organizations must deploy authentication capabilities that verify users with a high level of assurance and across a large range of devices. Looking forward, Agencies should be planning for multi-factor authentication solutions that use a layered approach of the methods discussed here, as well as other situational and behavioral risk factors – all in addition to passwords.

ABOUT RSA

Every day, and for over 30 years, RSA's singular mission has been to help our more than 30,000 customers around the world protect their most valuable digital assets. RSA is driven by its uncompromising belief that organizations should not have to accept getting breached or hacked as an unavoidable consequence of operating in a digital world. In fact, RSA believes that organizations must become aggressive defenders of their right to operate securely and that no other company is in a better position to help them.

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud, cyber-espionage, and cybercrime.

RSA Federal Solutions is the premier provider of intelligence-driven security solutions to the Federal government, serving every cabinet level agency, each military service, and the intelligence community. For more information, please visit federal.rsa.com.

APPENDIX

1. http://www.bbc.com/news/technology-28654613
2. https://www.emc.com/collateral/ebook/rsa-cybersecurity-poverty-index-ebook.pdf
3. http://www.gartner.com/newsroom/id/2661115
4. http://www.goodeintelligence.com/media-centre/view/mobile-leading-the-way-in-the-consumerisation-of-biometrics

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

www.RSA.com