The Problem With Passwords

Enhancing your mainframe security: password insecurity, data breaches, and multi-factor authentication

Table of Contents

Introduction: Stronger by Design?

Mainframe systems are built to be both reliable and scalable, more so than most other systems and endpoints. The problem is their security is often taken for granted. This should be of serious concern, given that around 80 percent of the world's system-of-record data resides on mainframe systems, and more commercial transactions are processed on mainframes than on any other platform. Too often, however, mainframe security has failed to be a priority, with the standard security posture that everyone has read access to everything. Just because a mainframe is deep within a network, behind three firewalls, and at the back of your data center, doesn't mean it is secure. To the bad actors, the mainframe is simply "another server" to be attacked.

Arguably, the greatest threats are insider threats: the bad actors won't be looking to target a system or application but are more likely to target individuals and attempt to steal system logins and credentials. If you are still authenticating users with passwords alone, then moving to multi-factor authentication (MFA) is long overdue.

Securing the mainframe: protecting your critical assets

- Mainframes hold 80 percent of the world's business data
- Mainframes host critical core IT for 92 of the world's top 100 banks, 18 of the world's 25 top retailers, 23 of the 25 top airlines, all of the world's top 10 insurers – and 71 percent of Fortune 500 companies
- Mainframes host more transactions daily than Google (1.3m/second CICS versus 68,542/second Google) - including 55 percent of all enterprise transactions
- Mainframes handle 90 percent of all credit card transactions

Scary Stuff: Password Insecurity

Standard mainframe security approaches are not enough and can be undone by password insecurity. In effect, passwords represent a single-point-of-failure. In the mainframe world, the maximum password length is eight characters. Up to 100-character passphrases are also available but few sites actually use them, citing reasons that usually involve updating legacy applications. There have been efforts to tighten up password security: IBM and CA Technologies added mixed case and additional characters, and the ability to challenge and force users to create more complex, and therefore, stronger passwords.

The problem is, if passwords become too complex and so difficult to remember, we end up driving behaviors in our user communities where, for example, passwords are "stored" on sticky notes or written to text files using tools like Notepad. I've even seen them written on whiteboards in offices. Some people use password vaults such as LastPass, but not everyone. Passwords, in general, are easily shared, easily stolen, and easily guessed: people are terrible at entropy. We all know the popular password choices: pet, children, and partner names.

How many times do we type those passwords in locations where we can be easily observed? One of the biggest threats is password reuse; combine this with the problems outlined above and you end up with convenient attack points.

This is a major problem. Incidentally, it's easy to check if you have an account that's been compromised in a data breach: simply go to www.haveibeenpwned.com and enter your e-mail address. A major data point from a recent Verizon Data Breach Investigations Report (DBIR)[1] implies this problem is growing: the percentage of hacking-related breaches involving the misuse of stolen or weak credentials reached 81 percent, effectively putting it front and center in terms of the tactics being leveraged by attackers. (Incidentally, the 2018 report described 53,000 incidents and 2,216 confirmed data breaches.)

The reality is that the mainframe often has the weakest password policies and algorithms in the entire enterprise. Are we making it difficult enough for potential hackers to get in? If we could be doing more, then shouldn't we?

[1]Source: Verizon Data Breach Investigations Report (DBIR) 2017 – via https://enterprise.verizon.com/resources/reports/dbir/

Risky Business: The Implications of Stolen Credentials

Assuming you already have a "perfect" implementation of mainframe security, the impacts can depend on whose credentials have been stolen. If they belong to a business user, a bad actor may be able to access your applications and data. If they're from an IT technician working in development, people may be able to access source code, your IP, and possibly your development and production environments. If it's a systems programmer or systems administrator whose credentials are lifted, they may be able to change system configuration and security controls as well as having access to source code, IP, development, and production data. How about DBAs, security administrators, and other roles? Even worse, if you don't have a "perfect" implementation of mainframe security, it may be possible to elevate the credentials of a DBA to that of a systems programmer. How about the credentials of a business user being used to logon to TSO, and one of the many possible privilege escalation attacks being launched?

Multiple risks are associated with any breach, no matter how it is perpetrated: for example, fines imposed by regulatory bodies relating to GDPR or PCI. If there is a data breach, along with fines, the organization will most likely face compensation payments and the costs for identity theft insurance for all affected users for 12-24 months—quite apart from the media coverage and serious reputational damage. Other impacts can, potentially, be even more damaging: from a denial of service attack that simply disables all mainframe systems, to a ransomware attack where all of your data is encrypted and a ransom demanded.

Potential attack scenario

One of your users is running a vulnerable version of MS Word...

Opens a malicious Word doc from a trusted sender whose e-mail account has been compromised

Malware (keylogger) is launched on the user's system, capturing mainframe credentials (userid/password)

Malware also gives bad actor remote access to the user's Windows machine for complete command and control

Bad actor is only limited by their imagination as they now have a valid logon to your mainframe...

Solution: The Right Tools and Your Security Journey

While your mainframe may not be secure right now, the mainframe is the most securable commercial computing platform available, and all the tools you might require are available. These include:

- Security products such as RACF, ACF2 or Top Secret
- Network segmentation
- Privileged user management e.g., BMC Mainframe Services by RSM Partners Breakglasss
- Real-time threat detection
- Multi-factor authentication (MFA)
- Remove application passwords and use encrypted PassTickets
- Client/server certificates
- Incident response

Deploying these should also form part of a planned sequence of actions. First, understand your security posture, carry out a security assessment, conduct penetration testing and remediate any issues.

The next step is to implement role-based access control, working to a least-privilege model, as well as implementing real-time alerts and a "break glass" solution to manage privileged users and their access. You then deploy MFA. The last but extremely important step in this initial rollout is to educate all of your users on the measures now in place, on the actions and behaviors expected, and to bring home the fact that security is the responsibility of everyone.

Enhanced Mainframe Security: MFA

Given that some 81 percent of breaches are attributable to credential reuse, multi-factor authentication (MFA) is a key weapon in your identity and access management armory. A highly-useful mechanism to validate the identity of somebody who wants to access your systems, MFA creates a high degree of friction for bad actors while presenting minimal delays and disruption to legitimate users. Indeed, investing in MFA can be an extremely smart decision, as mainframes become more open and connected to the wider world, regulations like GDPR demand stricter compliance (and include bigger fines) for data protection, and with PCI DSS actually requiring MFA to be implemented in line with Requirement 8.3 and its sub-requirements.

MFA works by inspecting multiple identifying elements associated with a particular user account, raising the authentication assurance level that a system requires from a specific user. Various products are available. For example, IBM Multi-Factor Authentication for z/OS is integrated with RACF; RACF has an MFA API set available for other vendors to use. Additional options include an OTP (one-time password) generator to create a password that is only valid for a short period, perhaps 60 seconds.

Mainframe MFA via RSA

RSA SecureID and RSA Authentication Manager are popular products in this space, using the "something you have" (hardware or software token) and "something you know" (PIN) approach, including cards and fobs that display an OTP, PIN pads, and soft tokens. The user creates and updates a PIN by logging into the RSA Authentication Manager application on z/OS, normally via a website. If they use a fob when logging into their mainframe application, they enter the PIN followed by the random token displayed by the fob. If the user has access to an RSA software application on their mobile or RSA PIN pad device, they enter their PIN to generate a random token, which they enter when logging into their mainframe application.

Mainframe MFA via Apple device

This approach is based on the IBM TouchToken for z/OS and IBM TouchToken App on an iOS device: "something you have" (iOS device and App) and "something you are" (your fingerprint). The user registers their iOS device with the IBM TouchToken application on z/OS via a website and using their RACF user ID and password/passphrase. They install a certificate on the iPhone that matches the certificate used by MFA, then use IBM TouchToken software on their phone by using their fingerprint to generate a random token, generated using the secret key and current time. They enter this token when logging into their mainframe application.

The two previous solutions are known as "in-band." However, another approach is known as MFA "out-of-band." This is where IBM Multi-Factor Authentication for z/OS is used with a web page to logon and enter RACF credentials—with an MFA web page for multiple authentication and reflecting the user's MFA policy (which may include RSA SecureID, IBM TouchToken for z/OS and others)—so enabling different policies for different individuals with different combinations. This approach, while still single token, is closer to true MFA than "in-band."

True MFA for the mainframe

True MFA arrived with IBM Multi-Factor Authentication for z/OS in late 2017, expanding the options available "for creating a layered defense." This integrated solution requires selected Z users to authenticate using multiple factors: "something they know"—password or security question; "something they have"—ID badge or cryptographic token device; and "something they are"—a fingerprint or other biometric. This solution is specifically designed to support many different token types:

- RSA SecurID hard and soft tokens
- IBM TouchToken app for time-based one-time password (TOTP)
- PassTicket support and application-level granularity
- Smart card certificate-based authentication - one of the supported types is a personal identity verification/common access cards (PIV/CAC)
- RADIUS (Remote Authentication Dial-in User Service) support – generic, SafeNet, RSA SecurID
- Generic time-based one-time password (TOTP) support (like Google Authenticator, Android, and Windows support)
- Compound authentication for "in-band" via Passphrase field

The RADIUS server checks information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified along with, optionally, other information related to the request such as the user's network address or phone number, account status and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat file database. Modern RADIUS servers can do this or can refer to external sources – commonly SQL, Kerberos, LDAP or Active Directory – to verify the user's credentials.

In my view, the best way to unlock the benefits of MFA and deliver a great user experience is to combine the approaches described here with a powerful Session Manager; we use Tubes for z/OS from Macro 4. Indeed, a secure mainframe is best achieved in general by using a range of best of breed technology, expertise, and professional services.

Next Steps

Implementing MFA as part of your mainframe security journey means you gain a valuable way to mitigate risks, avoid costs, and meet the requirements of regulatory and audit bodies. Questions to ask include, “Which options are best for our business?” and, “how much help should I give the end user?” to make it clear what people need to do while ensuring that you always stay on the right side of compliance. In this situation, the best approach is to use a modern session manager, easing the pain for end-users who are signing in to multiple applications. This means you are providing a single logon and control, simplifying the process (use PassTicket), and perhaps customizing logon screens and adding instructions. If PassTickets are a concern, another option is to set the telnet server default to your session manager, so forcing users to logon to your session manager using MFA; they can then logon to other applications using standard security, such as user ID and password.

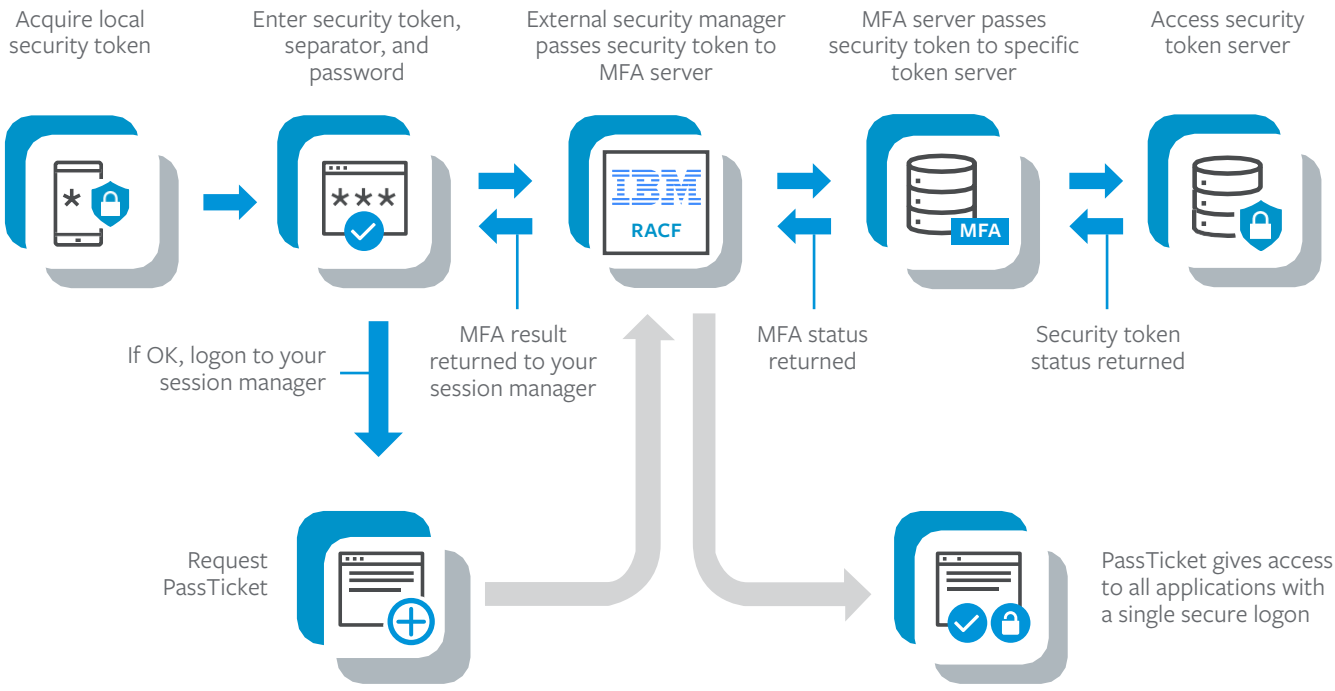

Figure 1: Example in-band and compound using RACF* and IBM TouchToken*
*Other ESMs and MFA solutions are available

Why BMC Mainframe Services by RSM Partners?

BMC Mainframe Services by RSM Partners is a globally-recognized expert in IBM Z mainframe security, providing both consultancy services and niche software tools, and working with some of the world's largest organizations. No other partner offers the same depth of knowledge and experience in ensuring mainframe security.

From mainframe penetration testing and vulnerability assessments to software tools greatly enhancing security management of the platform, clients know they can rely on BMC Mainframe Services by RSM Partners for quality, flexibility, and value.

Further reading

1. IBM Redbook – IBM MFA V1R1 / TouchToken, PassTicket, and Application Bypass Support
   REDP-5386-00
2. IBM Multi-Factor Authentication for z/OS User's Guide
   SC27-8448-03
3. IBM Multi-Factor Authentication for z/OS Installation and Customization
   SC27-8447-03

For more information

Please visit bmc.com

About BMC

BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent **www.bmc.com**

522051