Mainframe Threats
Today’s top security threats—and how to mitigate them
Today’s Threat Landscape

This paper highlights five of the major mainframe threats that our teams commonly encounter. It also suggests some of measures you can take to counter these threats and mitigate the risks. All of the threats discussed here are relatively easy for mainframe security experts to detect and then provide fixes and remediation work. The expertise, processes and technology required to deliver a more robust mainframe security posture are already available, and should ideally be applied as part of a Zero Trust approach to mainframe security.
The mainframe remains the processing and transactional heart of many organizations: the system of record and transactional beast of burden, which quickly adapted and coped with the huge increase in volumes seen during the coronavirus pandemic. Today's mainframe is increasingly seen as an important platform for growth and for long-term applications. Recognized as a hub for innovation, it is playing a central role in helping organizations to achieve their digital transformations. But the platform is at risk for four main reasons.
Risky Business

Penetration tests and security assessments by BMC Mainframe Services have uncovered the most common risks posed to mainframe security.

**First**, the people who truly understand mainframes have traditionally been a small group. The complexity (apparent obscurity) of the platform has led some people to conclude that it is virtually secure by default. This is not the case.

**Second**, that complexity/obscurity is compounded by scarcity: the average person is unable to simply buy a mainframe, install the software and start testing it. The technology is still too costly and tightly controlled to be reverse engineered. But as more people are interested and more information is shared online, knowledge about the platform and how it can be hacked will become widespread. (In fact, to the smarter hackers today, the mainframe is already “just another server”.)

**Third**, these beliefs have fostered an environment in which organizations are giving their employees READ access to everything, the attitude being “It doesn’t matter, they can only read it.” In the mainframe world, however, if you can read something – especially data – you can copy it. If you can copy it, you can download it. And if you can download it, you can potentially exfiltrate the data.

**Fourth**, there is a persistent lack of understanding around the detail and nuances of mainframe security by people tasked with keeping it secure. This is what leads to many of the vulnerabilities discussed in this paper. Individuals may not properly understand the risks involved in, say, giving someone a Superuser privilege.

The threat is real and growing. In every location where we conduct a security audit or penetration test, we always expose significant security concerns, including the exposure of highly sensitive data. From files containing credit card and personal details of customers to Superuser IDs with default passwords, there is always something that can be exploited. Despite increasingly tough regulatory regimes, huge financial penalties and the risk of reputational damage, many sites continue to fall far short of the standards required. But it doesn’t have to be that way.

Can you be sure that your own mainframe shop does not have a high number of vulnerabilities, hidden from view, that are placing this critical asset at risk from internal and external threats?
Too Many Users with Escalated Privileges

How does it happen? The Superuser privilege is inappropriately used, granting ALL users excessive access to system services and OMVS/USS (Unix System Services) resources and data.

What’s the risk? Sensitive data can be easily copied, deleted or held to ransom: the ramifications are huge.

Organizations often grant Superuser privileges to people without properly understanding the risks and potential impacts of such an action. In doing so, you open up your systems and environment in ways that anybody who is particularly talented in this field could use to exploit those privileges.

In reality, organizations should be applying a Zero Trust mindset. With READ access so often the norm, default access should be NONE. We should not automatically trust anyone and anything, either inside and outside our perimeters: it makes more sense to verify everyone and everything. Users need to provide a clear business reason why they require access to something, and then we can grant the appropriate levels of access for that use. This is about applying the principle of least privilege (PoLP): authenticating everybody, applying least privilege rights for all data access, systems and applications. Such an approach need not impact on working practices and efficiency, either, if implemented correctly.
Privilege Escalation Vulnerabilities

**How does it happen?** Many enterprises grant excessive access to libraries and authorized datasets that leave administrator and system level access unprotected.

**What’s the risk?** Bad actors can leverage this to elevate their privileges, to read and write all data and memory.

This threat arises from provisioning access to system resources inappropriately. The default may be set so that everybody has READ access or the default might be UPDATE. Alternatively, too wide a group of people may have been granted elevated access to the system libraries. Such elevated levels of access bring the risk of someone accessing your files to elevate their own permissions on the system.

For the mainframe, that could mean taking yourself from Problem State, where Normal user/applications run, to Supervisor State: a supposedly ‘protected’ and authorized elevated state in which a user has free rein to do all the clever stuff - or can make mischief. In the non-mainframe world, this would be called getting route level privileges. If you can get to that state, you gain the ability to read and write all data including memory. If a bad actor was skilled enough, they could go to somebody’s online banking application and change data, increasing (or deleting) balances. It is hoped but it cannot be guaranteed that checks and balances exist to stop such activity.
Default Passwords and Weak Password Management

**How does it happen?** Static passwords with no regular change intervals and default passwords that are used for months at a time.

**What’s the risk?** Unless manually changed, phishing or keylogger attacks could go undetected.

Password insecurity is rife. The number one password used in 2020 was ‘123456’. The number two was ‘123456789’. The word ‘password’ normally appears in the top five. It has been estimated that it would take a hacker less than a second to crack eight of the ten most commonly used passwords.

On the mainframe, the maximum password length is eight characters. One of the biggest threats is password reuse, further fueling potential attack points. Up to 100-character passphrases are available but few use them. There have been efforts to tighten up password security, adding mixed case and additional characters, and the ability to challenge and force users to create more complex and so stronger passwords. However, if passwords become too complex and difficult to remember, it can drive behaviors that lead to passwords being written on Post-it notes and even whiteboards. Password vaults are not commonly used. While data being stored today is stronger cryptographically than previously, it can still be hacked. Organizations should therefore not solely rely on passwords and ensure strong password controls. Users need to avoid static passwords, and ensure they are changed regularly. For mainframe privileged users, multi-factor authentication (MFA) is an absolute must.
When data is encrypted, its original form is effectively ‘destroyed’ – or at least scrambled. The only way to get the data back into a usable format is if you have the cryptographic keys. If you consider a ransomware attack, the bad actor needs to gain access, find the data, encrypt it, and now holds the key. If the organization wants its data back, it has to pay a ransom for the keys. If the organization has already encrypted its data, it may have done half of the bad actor’s work already. Now, the attacker shifts their focus from locating the data and encrypting it to locating the keys. If they can be stolen, and themselves encrypted, the hacker now has a key to your keys.

Additional processes, procedures and rigor are urgently required around protecting cryptographic data and keys. A bad actor may be able to not only download your data and decrypt it, but also to potentially re-encrypt it and write it back.
“Faceless” Accounts

How does it happen? Tasks that are system processes have poor or rarely changed passwords but system level privileges.

What’s the risk? A bad actor could have lengthy dwell times in addition to pervasive access to system resources to expand their attack.

Faceless accounts are where the organization needs an account that is associated with a system task: there is no real person or actual user associated with it. In technical terms, these are known as system tasks or system processes. These tend to be long-running tasks on, for example, z/OS, Db2 and related sub-systems, and often come with system-level privileges. They typically have a password that is very rarely changed and, if they do have a password, it is almost certainly easy to guess. They are another possible attack vector for hackers, who could gain widespread and prolonged system access.

The question to ask is, have you protected all of your “faceless” accounts properly and are they appropriately defined? 99% of these system tasks do not require a password: they should instead have a special Protected state on the system, which means they cannot be used to log on. Of the few that do require userid and password, passwords should be strong, changed regularly and subject to strong controls (unfortunately, MFA cannot be used in these cases).
Case Study: Pen Test Reveals Vulnerabilities at Bank

+ 96 vulnerabilities detected.

+ Risks identified: High (42), Medium (47) and Low (7) risks.

+ Fixes and recommendations provided to remediate vulnerabilities and process deficiencies.

This large European bank lacked the tools needed to maintain a strong security posture and was not using existing software to its full capabilities. Default access rights of READ (or higher) were used excessively. There were no detective controls to monitor platforms for potential threats such as malicious behavior, fraud and misconfigurations, and no continuous security improvement plan to ensure controls remained fit for purpose.

The bank, which had not performed a formal security assessment or pen test for some time, contacted BMC Mainframe Services to help remediate various internal audit issues. Provided with the necessary access and authorizations for pen tests and a more detailed security assessment, the BMC team rapidly uncovered 96 different vulnerabilities classed as High (42), Medium (47) and Low (7) risk:

+ Access to critical system utilities, tools, and functions.
+ READ access by default to system and business files.
+ Access to issue critical commands.
+ Recommended security profiles missing.
+ Recommended security configuration not in place.

The bank was found to be CMM Level 1: base practices were being performed informally and processes were undocumented, with clear risks present and wide scope for improvement.

Recommendations included: new software recommendations; implementing role-based access control (RBAC); security assessment of mainframe networking configuration and Unix System Services (USS); vulnerability scanning to test the security of products running on the mainframe; reviewing the environment and acquiring new tools to improve and maintain a stronger security stance e.g. automated auditing, monitoring and alerts.

“...The pen test and security assessment revealed a catalogue of vulnerabilities, with clear risks present and wide scope for improvement...”

Senior Security Architect, Large European Bank
Securing Your Mainframe

In most cases, weak controls and inadequate security result from:

- Insufficient headcount, inadequate resourcing or a lack of in-house skills and expertise.
- Poor system configuration.
- Mainframe and security processes that are either no longer fit-for-purpose or simply do not exist.
- Outdated (or an absence of) appropriate tools and technologies to secure the mainframe.

It is important to identify the extent of the problem first, which can mean using external specialists for penetration testing, ideally followed by a full security assessment. The main objective of pen tests is to identify security weaknesses that can be remediated. Pen tests are used to test an organization’s security policies, its adherence to compliance requirements, security awareness of employees, and its ability to identify and respond to security incidents.

The objective is to work towards a Zero Trust environment. In addition to the principle of least privilege (PoLP), organizations require improved threat detection and response capabilities on the basis that endpoint detection and response (EDR) and managed detection and response (MDR) are no longer enough; Extended Detection and Response (XDR) is coming to the fore. Security should never sleep, but the reality is that there simply are not enough skilled mainframe security experts to constantly monitor all of our systems all of the time. This is why we should look to automation, AI and machine learning to deliver new levels of threat intelligence via XDR. Every system, every user, every drift “from the normal” in terms of behavior counts – and we need to be on top of it.
About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

BMC, the BMC logo, and BMC’s other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners. © Copyright 2021 BMC Software, Inc.