What Does the IBM z14 Encryption Solution Protect?

LOU LOSEE

FEBRUARY 20, 2018

www.krisecurity.com
Mainframe Security is comprised of Confidentiality, Integrity, and Availability

Security. This is what everyone wants and it is what z/OS and IBM mainframes are known for. But what does the security architecture look like on the mainframe, how does the IBM z14 encryption solution address our security needs, what else do we need to do to make sure we are addressing all of the possible threats?

Mainframe Security is comprised of Confidentiality, Integrity and Availability and all three of these components interact with one another.

- **Confidentiality** – Protecting information from disclosure to unauthorized parties.
- **Integrity** – Protecting information from being modified by unauthorized parties.
- **Availability** – Authorized parties can access the information when needed.

Confidentiality is provided by a combination of the ESM (External Security Manager) only allowing designated users access to data and by cryptography which prevents unauthorized users from viewing the clear data.

Integrity is maintained by the hardware using separation of supervisor state from problem state programs. Privileged instructions are only executed in “supervisor state”. Problem state programs can only access and modify their own data by requesting a function from the operating system which executes in supervisor state. As with confidentiality, cryptography has a role in integrity when applied to data as it prevents the modification of data or allows the detection that data has been modified. The interfaces for these requests are well defined and written in a manner to prevent exploitation by a rogue problem state program.

Availability deals with prevention of ‘attacks’, whether accidental or malicious that prevent users from getting to the data they require. This could be acts of nature such as floods or other natural disasters as well as denial of service attacks, system failures or an accidental incorrect setting of a critical system parameter by system personnel (configuration vulnerability).
There Can Be No Security on Your z/OS System Without Operating System Integrity

When considering how to protect this triad of security components, one should consider the attack surface. The attack surface is the boundary where attacks should be prevented. However, if any weakness is discovered in that boundary, the system becomes vulnerable. The IBM z14 provides transparent pervasive encryption of data at rest and data in flight.

Applications access the data without requiring any change and the data is also encrypted while in transit to other systems. This capability is a great leap forward for security. Data can be encrypted by policy which then requires no more attention from administrators or developers. Administrators and developers no longer must continually determine what data should be encrypted. This capability of the z14 addresses some of the attack surface, especially when it comes to Confidentiality and Integrity, however it does not address all of it. With respect to Integrity, the attack surface between problem state programs and supervisor state programs falls into three categories; these interfaces being:

- Program Calls (PCs)
- Supervisor Calls (SVCs)
- Authorized Programs (APF)

“Now is the time for organizations to do away with the misconceptions and begin taking mainframe code vulnerabilities seriously.”

RAY OVERBY
PRESIDENT, KEY RESOURCES, INC.
The Three Interfaces used for Requesting Services from Authorized Programs

These three interfaces are the methods used for requesting supervisor state system programs to provide services to a problem state program. If a problem state program can bypass the controls in any of these methods of obtaining supervisor state it has broken through the attack surface and is able to circumvent the integrity of the system. This is because a supervisor state program can modify any area of memory as well as potentially assuming credentials of other users including administrators or system personnel. The rogue problem state program could also deny availability by overwriting critical system areas causing the system to crash. So how does a problem state program break through the attack surface and gain supervisor state? Typically, this occurs when one of the PCs, SVCs, or APF programs is either designed incorrectly or contains coding errors. The pervasive encryption provided by the IBM z14 does nothing to prevent this type of attack. Neither do the other controls on the system such as the ESM which are not designed to prevent supervisor state programs access to data.

So, what can be done to address this type of vulnerability?

It requires advanced threat detection. Vulnerability scanning of the programs (PCs, SVCs and APF programs) that comprise the attack surface for vulnerabilities before they are exploited and also getting the vendor of any code containing exploitable errors to correct them. The z/Assure® Vulnerability Analysis Program (VAP) performs this type of rapid detection and response.

The IBM mainframe has an unrivaled and well-deserved reputation for integrity. No other system provides hardware redundancy and built in security like mainframe. However, you are relying on hundreds of programs which comprise the attack surface all having been designed and coded correctly. To ensure the mainframe maintains its place as a premier system it is necessary to verify that the attack surface is immune to attack by ensuring the programs comprising it have been scanned for design and/or coding errors.
Key Resources Inc. has decades of expertise providing software, services and consulting to enterprises running critical apps on IBM® z/OS. We help CIOs, CISOs and programmers take control of mainframe security so they can protect their data, avoid costly breaches and maintain regulatory compliance.

Contact Key Resources
Call 1-800-574-1339 ext 701
Visit www.krisecurity.com/contact

www.krisecurity.com