Building on prime security with Linux on IBM Z and LinuxONE

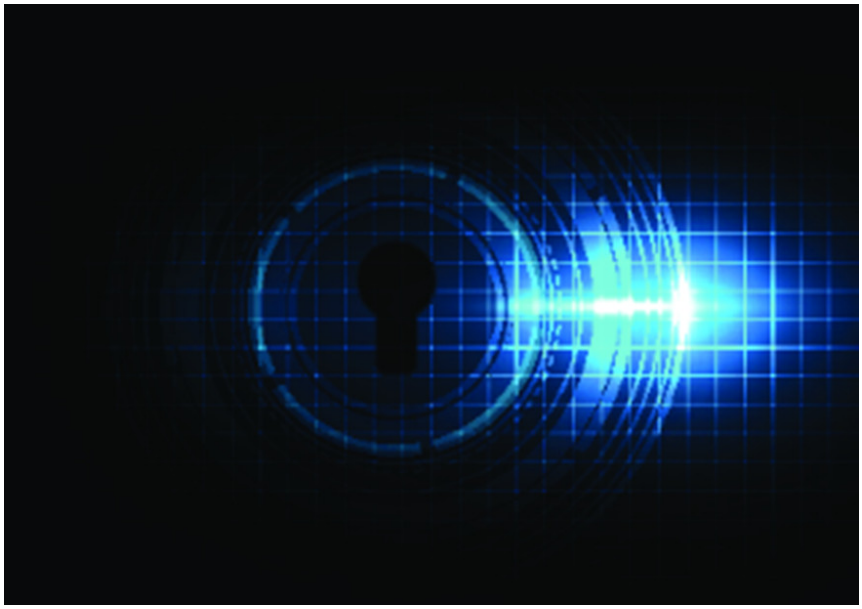
Dr. Reinhard Bündgen

Note

Before using this document, be sure to read the information in “Notices” on page 7.

Prime security with Linux on IBM Z and LinuxONE

The IBM Z® and LinuxONE systems are known as being highly securable platforms. But how does this affect running Linux® on IBM Z or LinuxONE?



After all, *Linux is Linux*. This is a true statement: Linux on IBM® Z and LinuxONE uses the same privilege, authorization, and access control concepts as any other Linux. The same methods for setting up firewalls, enforcing auditing, secure network protocols, disk and file system encryption and so forth are part of any Linux distribution, independent of the platform they are running on. The hardware features of IBM Z and LinuxONE make all the difference.

Learn about:

- How you can protect any data leaving the operating system, be it data in-flight or data at-rest.
- How confidential computing implements secure KVM guests on IBM Z and LinuxONE and supports fully encrypted boot images that are controlled by the image owner.
- And last but not least why IBM servers protect against tomorrow's quantum computing threats today.

Firmware

All modern computer systems are defined by a combination of true hardware and special software that closely interacts with the hardware. This special software is called firmware.

The firmware is shipped with the hardware and typically considered part of the hardware. Because of its software nature, firmware is replaceable. Sometimes system management requires a replacement, for example, to enable new devices. Loading compromised firmware into your system might undo all security of that system. It has the potential to eliminate the anchor of trust on which all security assumptions are built. IBM implements strict procedures for loading firmware into an IBM Z or LinuxONE system: all firmware loaded must be signed by IBM manufacturing and an IBM Z or LinuxONE system only starts if the loaded firmware is signed by IBM. That way the IBM Z and LinuxONE sysztems are reliable roots of trust for customer workloads.

Virtualization

The forerunner models of IBM Z were the pioneers of virtualization. Today, virtualization technology can be found on any modern computer system.

From a security perspective, virtualization technology is valued according to its capability to isolate virtual machines from each other, ensuring that no virtual machine can observe or influence the computation or data of another virtual machine. The Start Interpretive Execution (SIE) technology of IBM Z and LinuxONE is the only virtualization technology based upon which a virtualization solution was implemented and certified according to Common Criteria at the EAL 5 level. It is the same SIE virtualization technology that is used by the z/VM® and KVM hypervisors to provide strong isolation between z/VM or KVM guests. This makes IBM Z and LinuxONE ideal systems to host competing tenants on the same machine.

Confidential computing

Deploying sensitive workloads in a cloud requires complete trust in the cloud provider because the owner or administrator of a machine or hypervisor that hosts a workload has full control over that workload.

Not only can a hypervisor define the configuration and decide when to start and stop a virtual machine, but it also has full access to all memory of the virtual machine.

Therefore, it can observe and even manipulate its computation and data. To address this problem, some hardware vendors have implemented trusted execution environments (TEEs). TEEs support confidential computing, where virtual machines run as black boxes with states that can neither be inspected nor accessed by hypervisors or hardware management consoles.

IBM Secure Execution for Linux is the confidential computing solution that runs secure KVM guests on IBM Z and LinuxONE [1,2]. In contrast to other confidential computing solutions, it supports boot images that are fully encrypted and measured by the image owner. Because of the encryption, the owners can include secrets, such as dm-crypt or SSH keys, in the boot image. Thus, the attack surface of a secure guest is minimized. In addition, a secure execution image can be started without any interaction with the image owner.

Hardware security modules (HSMs)

IBM Crypto Express adapters are tamper-responding HSMs that support cryptographic operations using secure keys.

These secure keys can only be used on a specifically configured HSM. That is, the plaintext value of a secure key is never observable inside an operating system. IBM Crypto Express adapters [3] have earned the highest level of certification, FIPS 140-2 level 4, and can be configured in different modes:

- HSMs configured as Common Cryptographic Architecture (CCA) adapters are intended for the financial industry and are certified as payment card industry (PCI) compliant.
- HSMs configured as Enterprise PKCS #11 (EP11) adapters are intended for workloads using the PKCS #11 standard.

You can plug up to 60 Crypto Express adapters into an IBM Z or LinuxONE system. Each adapter can be logically partitioned into up to 85 domains, each acting as an independent virtual HSM. With this partitioning, thousands of virtual machines can access a dedicated virtual HSM. Linux on IBM Z and LinuxONE can access these adapters through the `zcrypt` device driver [4]. This device driver supports configurations for redundant HSMs to handle HSM failover and load balancing of cryptographic requests transparently to applications.

Pervasive encryption and protected key cryptography

Each processor of an IBM Z or LinuxONE system has a special component called Central Processor Assist for Cryptographic Functions (CPACF) [5]. CPACF accelerates the most common cryptographic operations

that are standardized by the US National Institute of Standards and Technology (NIST), for example AES, SHA2, SHA3, ECDH, and ECDSA [6].

Crypto modules like the Linux in-kernel cryptographic operations, OpenSSL, openCryptoki [7], gnuTLS, and gnuPG, can take advantage of CPACF acceleration, eliminating excuses to not protect data leaving the operating system, be it data in-flight or at-rest.

CPACF also supports a unique feature called protected key cryptography. A protected key is a clear key that is encrypted by a key-encrypting key (KEK) hidden in the firmware that is specific to a virtual machine. A protected key can be used for cryptographic operations that use CPACF. The CCA and EP11 HSMs can covertly convert CCA and EP11 secure keys into protected keys. As with secure keys, plaintext values of protected keys are never observable by an operating system. This makes protected keys ideal for bulk encryption, providing a high level of security as well as high-speed cryptography.

Linux end-to-end disk encryption is based on dm-crypt and LUKS, and can use protected keys. Substituting the AES cipher with the PAES cipher causes dm-crypt to encrypt volumes with protected keys which are derived from secure keys [8]. This solves two problems:

- The plaintext value of the key used to encrypt or decrypt the volume is never available in the operating system and therefore cannot be stolen.
- The secure key used to open a volume can safely be stored on unprotected storage, thus resolving the catch-22 situation of where to put the ultimate secret that protects a volume. Using secure keys eliminates the need to interactively query passphrases for each volume. Hence dm-crypt volumes can be programmatically opened.

Other exploiters of protected keys can be programs that call the CCA library or openCryptoki. Such programs can be configured to use protected keys instead of secure keys. Software vendors can use the libzpc library [9] to call protected-key cryptographic operations in their applications.

Random numbers

High-quality random numbers are essential to the security of many algorithms and protocols.

Computers are deterministic by nature and so cannot easily generate randomness. The lack of sufficient randomness has caused cryptographic leaks in the past. This is of particular concern for virtual machines which often lack direct connections to devices that could provide events with random timing. With IBM z16, IBM z15™, and LinuxONE III, each processor has a true-random-number unit, which can be accessed by Linux, and which is used to feed the kernel entropy pool and to seed pseudo-random-number generators [4].

Robust memory

IBM Z and LinuxONE main memory is designed to be highly resilient.

The RAIM technology [10] introduces redundancy, including error correction technology, at every level of the memory hierarchy. While being primarily designed as a RAS feature to protect against random bit flips in huge memory configurations, RAIM also provides protection against the row hammer memory attack that forcefully tries to trigger bit flips.

Quantum safe cryptography

Quantum computers of a sufficient size will threaten the very basis of cryptography, rendering digital signatures and cryptographic protocols like TLS (HTTPS) insecure.

While nobody knows whether or when a sufficiently large quantum computer will exist, their impact would be immense, and the threat of harvesting encrypted data today for later decryption is very real. To be prepared today, IBM already provides quantum safe technology with the IBM Z and LinuxONE systems. The IBM z16 system uses quantum safe methods inside its hardware and firmware to protect customer hardware investments against potential quantum threats. Starting with Crypto Express 7S, adapters in CCA or EP11 mode provide first versions of quantum-safe cryptographic algorithms accessible to Linux software.

Conclusion

Linux is Linux is a true statement which implies that Linux on IBM Z and LinuxONE inherits all security concepts supported by any Linux.

Yet, hardware designed for security does make a difference. IBM Z and LinuxONE systems provide a reliable root of trust. It protects workloads deployed in virtual machines, protects data in-flight, at-rest, and in-use. With directly attached HSMs you can run workloads that need to comply with the strictest regulations. Running protected key cryptography for dm-crypt allows end-to-end encryption of data at-rest in an automatically managed server environment.

IBM cares about your data. That is why IBM Z, especially IBM z16, and LinuxONE systems are designed for security, and why IBM leads you on a journey to a quantum safe future.

References

View a list of documents referenced in this white paper.

[1]

Bornträger et al, *Secure your cloud workloads with IBM Secure Execution for Linux on IBM z15 and LinuxONE III*, in IBM Journal of R&D, vol. 64, 2020

https://ieeexplore.ieee.org/document/9138728

[2]

Introducing IBM Secure Execution for Linux,

https://www.ibm.com/docs/en/linux-on-systems?topic=security-introducing-secure-execution-linux

[3]

CEX7S / 4769 overview,

https://www.ibm.com/security/cryptocards/pciecc4/overview

[4]

Linux on IBM Z and LinuxONE Device Drivers, Features and Commands,

https://www.ibm.com/docs/en/linux-on-systems?topic=overview-device-drivers-features-commands

[5]

z/Architecture Principles of Operations, SA22-7812-xx,

https://www.ibm.com/support/pages/zarchitecture-principles-operation

[6]

IBM z15 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX7S)

https://www.ibm.com/downloads/cas/6K2653EJ

[7]

openCryptoki - An open source implementation of PKCS #11,

https://www.ibm.com/docs/en/linux-on-systems?topic=support-opencryptoki-open-source-pkcs-11

[8]

Pervasive Encryption,

https://www.ibm.com/docs/en/linux-on-systems?topic=security-pervasive-encryption

[9]
libzpc - A Protected-Key Cryptographic Library,

```
https://www.ibm.com/docs/en/linux-on-systems?topic=support-libzpc-protected-key-cryptographic-library
```

[10]
Maeany et al, *IBM zEnterprise redundant array of independent memory subsystem*, in IBM Journal of R &D, vol. 56, 2012

```
https://ieeexplore.ieee.org/document/6136239
```

Accessibility

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Documentation accessibility

The Linux on IBM Z and LinuxONE publications are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF file and want to request a Web-based format for this publication send an email to eservdoc@de.ibm.com or write to:

IBM Deutschland Research & Development GmbH
Information Development
Department 3282
Schoenaicher Strasse 220
71032 Boeblingen
Germany

In the request, be sure to include the publication number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility at

```
www.ibm.com/able
```

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive

Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.