Technical Insight

Gen-Z: Securing the Future of Data

By Mitch Lewis

December 2019

Evaluator Group

Enabling you to make the best technology decisions

Executive Summary

Today's data landscape is constantly expanding. With unprecedented volumes of data being generated every day and rapidly growing data topologies – from IoT and edge devices, to public, hybrid, and multi-clouds – data is spread over vast geographic locations and an increasing number of physical devices. Along with growing data landscapes, the number of cyber-attacks is rising at an alarming rate, increasing the need to ensure rigid data security at every component within a system. Despite this need, many IT organizations often have reservations about implementing proper security practices due to cost, complexity, or inconvenience. The reality, however, is that the cost of implementing proper security practices is often far less than the cost incurred by suffering a data security incident.

The Gen-Z interconnect was created to provide memory-semantic data access across direct attached, switched, and fabric environments. Gen-Z was developed with a focus on accommodating continuous performance increases through the increased adoption of next generation devices such as persistent memory, as well as leveraging DRAM through composable memory. Gen-Z's memory semantic technology enables a variety of flexible data solutions to overcome many of the challenges faced in the modern data center. Gen-Z facilitates expanded use of memory resources including disaggregation and pooling of shared memory to create flexible solutions and expanded memory access. Using this technology relieves performance and configuration issues caused by inflexible or limited resource allocation.

These developments have clear benefits to many organizations, however they also introduce the potential for new security threats. Disaggregation of memory resources provides flexibility in configurations and access, but it can also provide flexibility for attackers to maliciously access or insert data if the environment is not properly secured. Persistent memory presents its own security risks by providing the potential for malware to exist persistently within executable memory. In increasingly complex and interconnected data environments, every component is a vector for attack, and a single compromised component can be disastrous for the entire system. While Gen-Z was developed with a focus on performance and flexibility, it was also developed with the proper functionality to achieve those goals securely at every level including the fabric, the data, and all attached devices.

Standard technologies that are widely used today such as Ethernet, InfiniBand, and Fibre Channel, have not placed their focus on security. Gen-Z*,* on the other hand*, is* focused on securing data environments at every component to prevent a malicious attack on a single target, as well as the overarching system. The Gen-Z interconnect was created with a number of security features that are either not addressed by current technologies, or were inefficiently added as an afterthought. This report will discuss these aspects of the Gen-Z technology and how they can secure data environments at every component.

Access Control

As a first line of defense, data transferred over a Gen-Z fabric can be configured with access control keys to ensure that the data has the right to access the target endpoint. Access control keys are an effective way to isolate data and prevent unauthorized read and write attempts by restricting data access to only

those with a verifiable key. One or more access keys can be associated with each component and linked in the fabric. Data packets transferring from one component to another can hold this access key in their header, allowing them access to links and components associated with the same access key.

Enforcement of access keys is done at the Gen-Z switch. When the switch receives a packet, it compares the access key in the header of the packet to the access key associated with the targeted link and component endpoint. If the access keys match, then the packet is transferred along and is received by the target component. If, however, the access key in the data packet does not match that of the target component, then the offending data packet will be discarded. When the packet is discarded, a data access event is recorded in an audit log and a security event is alerted to the fabric manager.

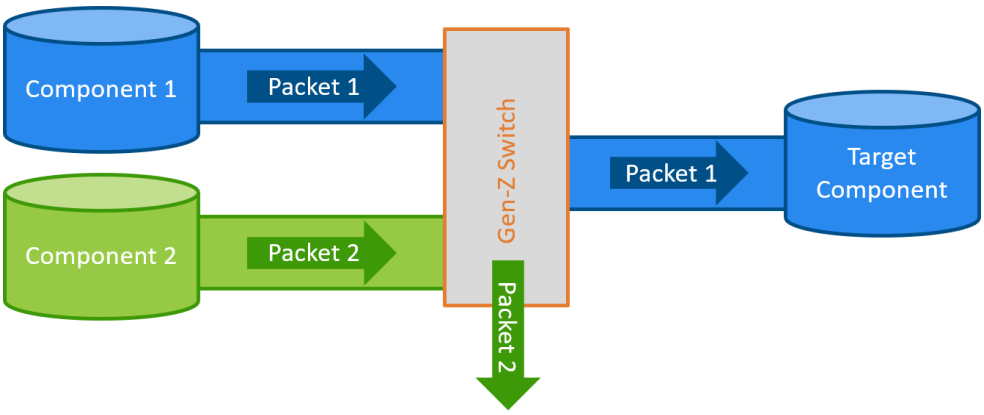

Figure 1: Access Control

Utilization of data access keys ensures that only data packets configured with the correct key will be able to reach their target by creating logical partitioning of links and devices. In addition to stopping errant data packets from reaching their destination, by raising a security event the access control mechanism is able to help quickly identify a source of error, including malicious activity or misconfiguration.

Memory Region Keys

Similar to access control keys, Gen-Z also incorporates memory region keys. These keys are used to provide partitioning and protection for components that share memory regions. As with access keys, the memory region key of a component is stored in the header of outgoing data packets. These keys will then be validated against the memory region key of the target component before the packet is accepted. Unlike access keys, in which the validation is done at the switch, memory region keys are validated by the receiving component.

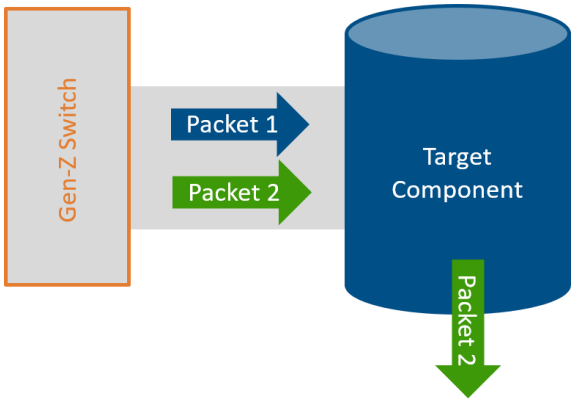

Figure 2: Memory Region Key

If the memory region key stored in the header of the data packet matches the key assigned to the target component, it is authorized and the data packet is received. A data packet with an invalid memory region key will be dropped, audit logged, and trigger a security event, just as in the case of an invalid access key.

Authentication and Encryption

The transfer of packets between components across an interconnect without proper security precautions can lead a to an abundance of issues. Unsecured data being transferred is at risk to be captured and accessed by malicious entities, therefore it is crucial for data to be encrypted, making it useless to anyone without the proper means of decryption. Another potential attack that is vital to protect against is packet injection, which involves inserting unauthorized, and potentially malicious, packets into the data stream. This means that data received must be authenticated upon receipt to ensure it is valid. Gen-Z uses a technique known as Authenticated Encryption with Associated Data (AEAD) in order to achieve both encryption and authentication efficiently within a single process.

Gen-Z uses the FIPS approved 256-bit AES-GCM cipher to enable AEAD. AEAD secures data in a packet by encrypting it and additionally allowing the receiving component to verify the authenticity of the packet it is receiving. To do this, the packet is first encrypted, with the exception of certain header data, including a unique Message Authentication Code (MAC) that is calculated for the packet. As the data is transferred, it is secured through the encryption. Once a data packet is received, the receiving component will begin to decrypt the data and calculate a MAC. The MAC value calculated by the target will then be compared to the MAC value that was received to ensure that the packet is authentic. Any packet for which the MAC value cannot be validated, or the data cannot be decrypted, will be dropped and a security event will be triggered. AEAD is an efficient way to effectively protect data in transit from being accessed as well as protecting the target component from any inauthentic data that may have been injected.

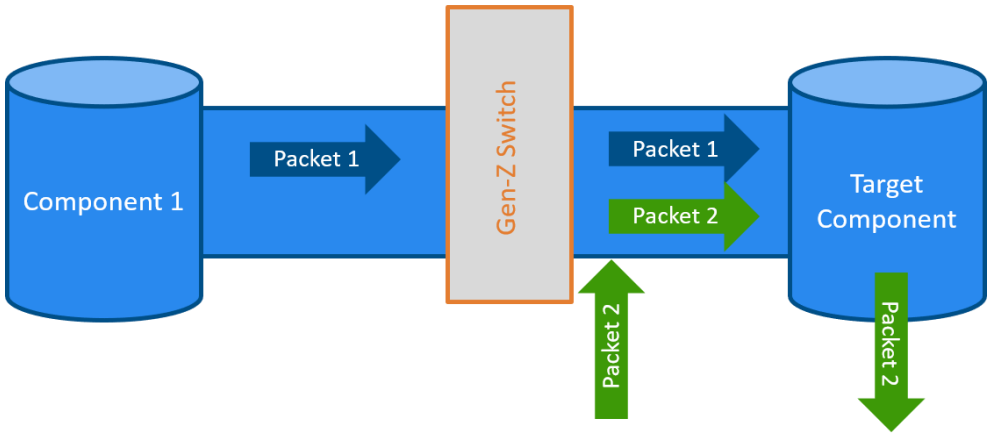

Figure 3: Packet Injection with Packet Authentication

Anti-Replay Attack

In addition to protecting against attacks that inject new foreign data packets, it is also crucial to protect against the injection of packets that have already been received. These attacks, known as replay attacks, resend previously received data, creating the potential to overwrite any changes that were recorded since the original data packet was first received. Since this replayed data packet is legitimate data that was originally verified upon its first receipt, it is crucial to detect data that is not unique.

Gen-Z protects against replay attacks using its AEAD process. When enabled, authentication and encryption must be applied for every new and retransmitted data packet. The associated MAC value is calculated using the packet data and a unique nonce value, which creates a unique identifier. Upon receiving a data packet, the target component validates that the MAC is a unique value to ensure that the data packet has not been received before. If the receiving component recognizes the MAC as non-unique value, then the data packet will be dropped and, as with other Gen-Z data protection protocols, a log and security event is created.

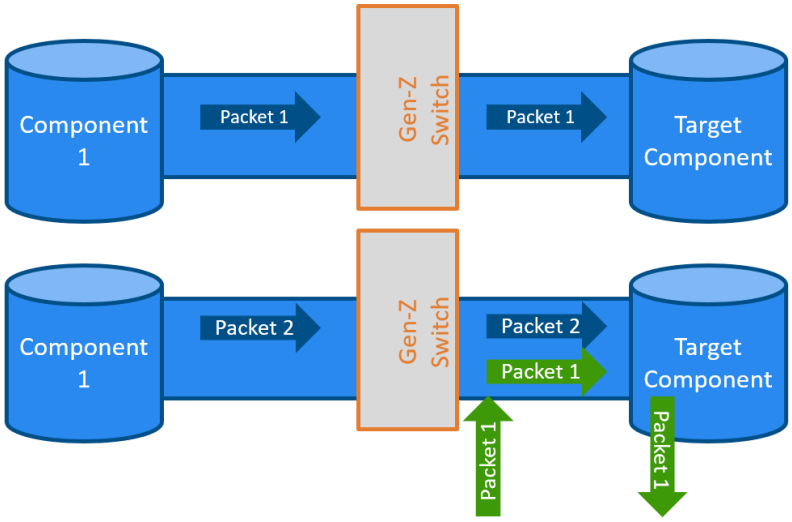

Figure 4: Anti-Replay Attack

In Situ Insertion Mitigation

The Gen-Z protocol has additional security functionality to protect against the physical insertion or replacement of devices that might otherwise go undetected. It is possible in certain low power situations for a component to be replaced transparently. Without proper protection, this could cause harm to the entire environment. Gen-Z prevents this by using a method of nonce validation between components. Components are configured with nonce values that are communicated between components to ensure their validity. In the case that a component substitution occurred, the substituted component can be detected by peer components via the detection of an incorrect or missing nonce value.

Another threat that may be faced is the insertion of bump-in-the-wire components. These are components that are inserted within the system and can be detected by an additional latency. Prior to packet transmissions between components, Gen-Z measures the path length and calculates the estimated transmission time. The transmission time of data packets is then monitored, allowing an inserted bump-in-the-wire component to be detected due to an increased latency.

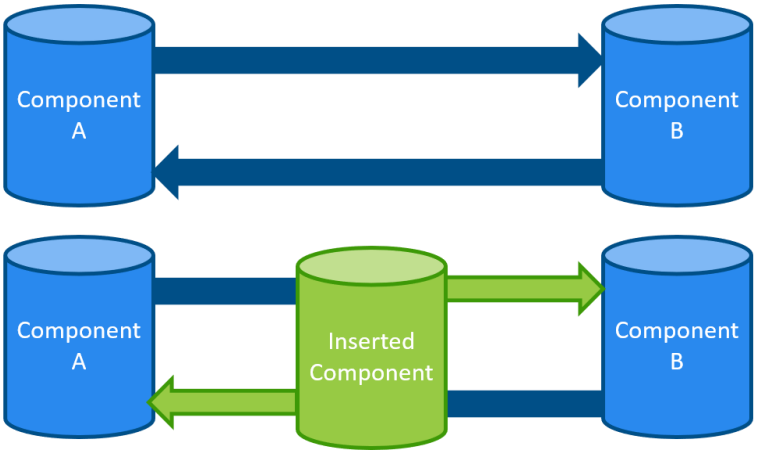

Figure 5: Bump-in-the-Wire Insertion

Component Authentication

In addition to Gen-Z's multiple security features, the Gen-Z consortium has been adamant about the development and use of component authentication. The Gen-Z consortium defined standard data objects that can be used to authenticate hardware, hardware configurations, and firmware. These data objects can be exchanged between components over the Management Component Transport Protocol (MCTP) allowing for a challenge and response process in which an initiator device can request and verify certificates and firmware measurements that are sent from a component.

Component authentication is an important layer of enhancement to the Gen-Z security. By verifying a component's certificate, it is protected from communicating with other components that may be incorrect, corrupted, or altered. This prevents the use of unauthorized hardware inserted into a system as well as hardware being removed from an environment to extract data from an unknown source. It also provides protection against a component communicating with another component that may have been corrupted by malware.

The Gen-Z consortium has shared their standardized data objects for use by other interconnects. Along with MCTP over Gen-Z, MCTP can be used over I2C, I3C, PCIe, and multiple other interconnects. This sharing and standardization of hardware authentication creates a cohesive approach to securing infrastructure environments.

Final Thoughts

Data security is a vital piece of the modern data landscape and one that is often left unaddressed until it is too late. Many interconnect technologies were not originally built with security in mind, leaving unaddressed concerns or inadequate attempts to add security features. The creation of the Gen-Z

interconnect introduces new efficiencies and interoperability while being built from the ground up with security in mind.

Gen-Z enforces security with the idea that every component is a possible point of attack and any compromised component can be detrimental to the entire system. Gen-Z uses a mixture of multiple highly-effective security protocols to protect the interconnect from various attacks, including hardware isolation through access keys and memory region keys, authenticated encryption, and in situ insertion mitigation. In addition, Gen-Z can use the Management Component Transport Protocol to initiate component authentication and verify every component.

The number of malicious cyber-attacks being launched each year is growing and the need for a highly-secure interconnect will only continue to increase with further developments such as edge computing and automation. With the combination of memory semantic data access and multiple layers of built-in security features, Gen-Z is well positioned as an effective interconnect to handle the emergence of persistent memory and disaggregation, and will address the ever-growing data security concerns that existing technologies are not prepared for.

About Evaluator Group

Evaluator Group Inc. is a technology research and advisory company covering Information Management, Storage and Systems. Executives and IT Managers use us daily to make informed decisions to architect and purchase systems supporting their digital data. We get beyond the technology landscape by defining requirements and knowing the products in-depth along with the intricacies that dictate long-term successful strategies. ***www.evaluatorgroup.com*** *@evaluator_group*