This presentation covers Gen-Z’s Security capabilities.
Disclaimer

This document is provided ‘as is’ with no warranties whatsoever, including any warranty of merchantability, noninfringement, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. Gen-Z Consortium disclaims all liability for infringement of proprietary rights, relating to use of information in this document. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Gen-Z is a trademark or registered trademark of the Gen-Z Consortium.
All other product names are trademarks, registered trademarks, or servicemarks of their respective owners.

All material is subject to change at any time at the discretion of the Gen-Z Consortium

http://genzconsortium.org/
Gen-Z architecture assumes every component is an attack vector. This is critical to appreciate, as time and again cyber attacks have exploited hardware and software that take no steps to authenticate access and establish trust.

This slide illustrates how attacks are carried out today at all levels irrespective of the interconnect used.
**Break-down of Malicious Component Threats**

- Attacks on packets traversing the subnet from other components
  - Packet eavesdropping
  - Packet destruction
  - Packet modification
- Denial of service attacks:
  - Destruction of in-flight packets by an intermediate component
  - Extreme packet injection rates to cause resource exhaustion and congestion collapse
  - Data destruction—Request acknowledgment without successful execution or acknowledgment of deliberately modified data
  - Resource exhaustion by failure to send expected packets. This can occur if two components are interlocked via a specific packet exchange sequence and one prevents the sequence from progressing causing resources to be consumed for long time periods.
- Unauthorized packet injection including, but not limited to, unauthorized attempts to read or write the Data Space or Control Space of other components.
  - A variant of this is the replay attack. A replay attack is when the malicious component captures a legitimate packet, and at a later time injects it back into the subnet. Without mitigation, the receiving component has no way to distinguish the injected packet from a correct packet and may perform an unauthorized action such as writing to an address space overwriting any changes that have been made between receipt of the legitimate packet and the unauthorized replay.
- Precision Time manipulation to force time forwards or backwards.

This slide provides a high-level breakdown on malicious component threats. Again, these threats are interconnect independent, and cyber attacks make use of these on a regular basis.
This slide describes a set of high-level actions that can be used to mitigate the threats posed by malicious components. All of these actions are supported by Gen-Z, and can be applied to any Gen-Z-based solution.

• The payload within a Gen-Z packet can be encrypted to ensure privacy.
• Gen-Z supports packet deadlines to enable more aggressive end-to-end request packet retransmission timers.
• Gen-Z supports Hash-based Message Authentication (HMAC) that can be included in any explicit OpClass packet.
• Gen-Z Explicit OpClass packets contain Access Keys and select request packets contain R-Keys to provide hardware-enforced access control. Further, Gen-Z supports additional access control and packet filtering to ensure components can communicate only with configured peers.
• Gen-Z explicit OpClass packets can include an anti-replay field (sequence number or precision time-based) to ensure request packets are not intercepted and replayed multiple times.
• Precision time request and responses are exchanged using explicit OpClass packets, and can be cryptographically secured.
Gen-Z architecture specifies mechanisms that cover all of the listed mitigations.
Fundamental Threat Mitigations

- Thorough and complete packet validation
- Hardware-enforced access controls
- Robust congestion management and packet injection controls to support heavy loads with predictable jitter
- End-to-end packet encryption and authentication (256b AES-GCM)
- Data replication
- Component Authentication
In Situ insertion is the physical interposition of hardware, e.g., crocodile clips or a Y-cable to physically collect and / or modify packets.

Switches can provide a limited level of packet filtering. For example, during leaf component configuration, a switch can filter any non-Control OpClass packets to prevent the component or any other component from communicating with the component under configuration. Once configured or through a Link CTL exchange, the switch can filter the SCID / SSID in all packets to ensure that a leaf component only transmits packets corresponding to its component identifier.

Though outside of the specification’s scope, management can use a challenge-response protocol to authenticate the public / private keys. Such a protocol can be transported in Gen-Z Read / Write or Write MSG or Vendor-defined packets.
Example Nonce Configuration Sequence illustrates one possible sequence to configure the Core Structure Component Nonce and the Interface Structure Peer Nonce fields:

- Management sets Component 0 Core Structure Component Nonce = X and, sets Component 1 Core Structure Component Nonce = Y.
- Management sets Component 0 Interface Structure Peer Nonce = Y, and sets Interface I-CAP 1 Control Peer Nonce Validation Enable = 1b.
  - Once enabled, the Component 0 interface initiates a Nonce Notification Link CTL packet exchange.
  - Since Component 1 Interface I-CAP 1 Control Peer Nonce Validation Enable = 0b, the Link ACK indicates that management has not configured the Component 1 Interface Structure Peer Nonce field.
  - Upon receipt of the Link ACK, the Component 0 interface sets Interface I-Status Peer Nonce Detected = 0b, and silently discards all non-In-band Management end-to-end packets.
- Management sets Component 1 Interface Structure Peer Nonce = X, and sets Interface I-CAP 1 Control Peer Nonce Validation Enable = 1b.
  - Once enabled, the Component 1 interface initiates a Nonce Notification Link CTL packet exchange.
• Since Component 0 Interface I-CAP 1 Control Peer Nonce Validation Enable = 1b, the Link ACK returns Component 0 Nonce X. Further, Component 1 interface silently discards all non-In-band Management end-to-end packets.

• Upon receipt of the Nonce Notification Link CTL, Component 0 interface validates Component 0 Interface Structure Peer Nonce equals Nonce Notification nonce Y, and stops discarding all non-In-band Management end-to-end packets.

• Upon receipt of the Link ACK, if Component 0 Interface Structure Peer Nonce equals the returned nonce, then sets Component 1 interface’s Interface I-Status Peer Nonce Detected = 1b, and stops discarding all non-In-band Management end-to-end packets.
Gen-Z supports multiple mechanisms to enforce access control and access permission validation in hardware with minimum resources and performance impact (most validation can occur in parallel with other aspects of packet validation, thus eliminating any latency impacts).

Access control is used to determine whether a component is authorized to communicate with another component and, if supported, if the component is permitted to access a given resource. Authorization is determined entirely in software (application / middleware / management), and is enforced in hardware (simple, high-performance). Access control is not a substitution for a robust security solution. Access control is sufficient to mitigate potential damage caused by erroneous or failing components or to quickly isolate malicious actors, but Access Control does not prevent packet spoofing or anti-replay attacks (see Gen-Z Security for details on how these attacks are handled).

Gen-Z supports multiple techniques to enable components to incorporate access control as required by specific solution stacks.
After considerable research and development developing Gen-Z component authentication, members determined that the proposed Redfish-based data objects used to perform component authentication could be applied across the industry to multiple technologies thus benefiting all. As a result, Gen-Z members donated these Redfish-based data objects to the DMTF (http://www.dmtf.org). The DMTF built upon these data objects which will now be used by multiple industry bodies to perform component authentication. To learn more about the security threats and why component authentication is the foundation for a secured infrastructure, please see: https://genzconsortium.org/wp-content/uploads/2019/03/Gen-Z-Component-Authentication-Secured-Infrastructure.pdf. These data objects will be extended to add key management support which will provide numerous industry-wide benefits.
Gen-Z Packet Authentication and Encryption

Gen-Z data privacy + packet authentication = maximum security protection

Gen-Z uses authenticating encryption to provide:
• AES 256 encryption
• Packet tamper and anti-replay attack protection
• Packet authenticating encryption may be selectively enabled
• Unique session per communicating peer
• Data plane, control plane, or both
Gen-Z encryption sessions will use DMTF SPDM session establishment (WIP)
• DMTF SPDM will be supported by multiple interconnects thus enhancing solution and infrastructure security
• See: https://www.dmtf.org/content/dmtf-releases-security-protocol-and-data-model-spdm-architecture-work-progress
Violations reported to management
Secured Gen-Z Buffer Operations

Gen-Z specifies 16 Buffer operations that simplify data movement, buffer allocation, security, etc.

- No work queues, completion queues, etc. to manage—single buffer request / response
- One, Two, and Three party data movement

Buffer operations can improve performance in multiple ways
- Three-party data movement eliminates need for all data to flow through a SoC
- Signaled buffer operations eliminate multi-thread / multi node coordination overhead and complexity
- T10 DIF / PI acceleration and Secured Hash / Encryption acceleration
- Simplifies software / management, reduces control packet overheads, multipath aggregation, etc.
Gen-Z Emergency/Planned Primary Media Backup

- Enables primary media to be automatically copied to a secondary media.
  - Works in a single enclosure or composable
  - Primary and secondary media can be dedicated or shared by multiple compute / systems
  - Primary and secondary media can be mechanically co-located or discrete
    - Shared amortizes backup media costs across multiple primary media modules
- Emergency backup can be initiated by a processor once it has flushed its caches or if the primary media controller detects h/w failure
- Planned backup can be initiated by software to create dynamic data checkpoints
Direct attached and shared / composable memory emergency and planned backup services
- Strong data integrity, cryptographically-secured hash, or encryption as moved to / from primary / secondary media
- Only primary media comprehends data protection applied—does not extend trust to secondary backup media
Summary

Gen-Z architecture designed from the start to support a fully-secured infrastructure

- Multiple hardware-enforced isolation mechanisms
- Component authentication and session management built on top of DMTF SPDM to simplify security infrastructure and management
- Strong privacy and packet tampering and anti-replay protection
This concludes this presentation. Thank you.