Network Security Considerations for ATM Services

Paul Groppel

Sean Boden

L3Harris Technologies

TABLE OF CONTENTS

LIST OF FIGURES

risks in migrating ATM data to these infrastructures.

Cyber Security Mitigation Strategies

The Internet is riddled with cyber security threats that continuously attack every layer of the Open System Interconnection (OSI) model. Organizations are constantly investing in hardware and software to aid their efforts in protecting vital systems and services from cyber threats. While these products offer many capabilities, they are often built with a common default enterprise configuration that are not tailored to specific needs of ATM system owners. For some businesses and organizations, this basic configuration is fine. However, for system owners who have unique challenges that need to be addressed, the level of service required to effectively build and integrate security products and solutions into their environment takes an increased level of support by these product vendors. While cost may increase for this level of dedicated service, the result is a tailored solution that provides a more effective protection capability against cyber threats. These same principles can be applied to how a network infrastructure is serviced and protected against the growing cyber threats ATM systems and services face as they adopt a network architecture for their application needs. While commercial carriers can offer flexible network offerings and decreased costs by leveraging their shared network infrastructure offered to their consumers, the level of service provided is bound by Service Level Agreements (SLAs) that are highly structured and difficult to modify to address unique ATM challenges. In contrast, using an integrator who understands customer needs can offer highly flexible service offerings to address unique challenges faced in protecting critical ATM systems and services.

Commercial Carrier Services

Commercial telecommunication carriers have built large network infrastructures to service customers across the country. From large organizations (Government, financial, retail, etc.) to residential consumers, these carriers offer varying service models to address each client segment needs. However, this also presents a challenge with the types of services they can provide to clients with unique needs and data requirements. While there are several benefits for leveraging commercial carrier infrastructures, there are also several weaknesses that can have a major impact on ATM critical systems and services.

Opportunities

Cost Savings – Commercial carriers have large network infrastructures that offer various data path options. They are able to offer cost savings by sharing paths between all customers (a one size fits all approach). This shared infrastructure model keeps

Lack of Dedicated Support – Commercial carriers have thousands of customers and all have unique needs and services. Often times, when a support call is received it is balanced against competing priorities amongst all of the carrier's customers. Call center technicians may not have dedicated or intimate knowledge of systems or services being impacted and treat calls as any other call they receive.

Dedicated Managed Services

Unlike commercial carriers, a dedicated managed service provides an all-inclusive service model the ensures critical ATM systems and services are given the appropriate level of support needed to maintain operations and ensure protection of critical data. While transport offerings may not be as cheap as a commercial carrier, the dedicated support and services are far superior. An integrator with intimate knowledge of customer's needs and unique mission requirements can offer tailored offerings.

Opportunities

Dedicated Protection – A dedicated managed security service is designed around the mission and provides the appropriate support required for ATM systems and service to be protected against adversarial threats. Network and data protection solutions and configurations can be designed to protect vital air traffic services without having to worry about impacts to, or from, other external customers. Additionally, a managed service can offer a holistic view into the network and aid in the protection of critical system components.

Enhanced Services –

Non-

Web Portal - The Web Portal is used to access the SD-WAN Orchestrator for management and reporting. It can also communicate with OSS/BSS systems for service activation (as required by SD-WAN deployment options).

Understanding these components allows for better understanding of benefits gained in using SD-WAN and SD

send packets, ensuring application performance requirements defined in the application overlay are met. Several features include but are not limited to:

Dynamic Path Switching	Unidirectional measurement and steering
Per-flow load balancing	Forward Error Control (FEC)
Per-packet load balancing	Packet Duplication (Use multiple links to send the same packet)

These aid in optimizing application performance and security by ensuring services remain active while network anomalies are investigated, thus preventing application service downtime and increasing overall availability.

Conclusion

With over 140,000 flight operations per day, the security and functionality of critical ATM systems and services must be a top priority for air transportation industry leaders. For decades, separate networks for voice services and IP were the most secure method for organizations to protect sensitive data and services. However, to reduce management costs of maintaining separate network architectures, organizations are beginning to consolidate these traditionally separate data types into a single infrastructure. When using a shared network infrastructure, commercial carriers typically place multiple customers and services on the same network core. Often, an issue for one or more customers may require a carrier to take actions that may impact critical services of other customers that share the same network infrastructure. As significant pressure exists to be an early adopter of emerging technologies, a strong focus should be on the success of the past with an ability to responsibly adapt to the ever-changing threat landscape.