UNISYS | Securing Your Tomorrow®

HOW MICROSEGMENTATION CLOSES SECURITY GAPS FOR HETEROGENEOUS AIRPORT ECOSYSTEMS

ABOUT THE AUTHORS

Ashwin Pal: *Ashwin has had over 20 years' experience in the IT security industry in Asia Pacific. In Unisys Ashwin has responsibility for leading sales engagements to C level executives within the region, providing project-based quality assurance, providing input into new product development, client, P&L and staff management. Ashwin is passionate about cybersecurity and is a sought-after cybersecurity expert.*

Venkatasubramanian Viswanathan: *Venkat is a senior airport applications SME with Unisys, Singapore. Venkat has been developing and delivering solutions for multiple airport/airline industry customers across APAC. In his current role, Venkat leverages his experience in building the Unisys Airports strategy.*

The Airport IT Landscape is Changing

With the IATA predicting that air traffic will double by 2037, airports are gearing up to provide an excellent passenger experience to the growing number of travelers by improving efficiency across their operations. Tech-savvy travelers also demand self-service options to reduce wait times at airport counters. Airports today are adopting increasing numbers of complex, heterogeneous information technology (IT) and operational technology (OT) systems to streamline business processes and deliver a great experience to travelers.

The airport IT landscape is now a mix of legacy and modern technology. Interconnected systems do everything from directing passengers to boarding gates to moving checked baggage safely and accurately. These solutions incorporate multiple devices and IT systems from many vendors—PCs, X-ray scanning systems, e-gates, surveillance systems and more. While most of these solutions currently remain on-premise, airports are gradually incorporating cloud-based systems as well. On the backend, information sharing is not limited to the airport, it extends to the entire aviation ecosystem to improve coordination and operational efficiencies. All this occurs under the watchful eyes of regulatory bodies that are promulgating increasingly stringent security measures to counter threats like terrorism, theft, sabotage and other crimes in civil aviation.

Within this increasingly challenging environment, airports strive to achieve their customer satisfaction, operational and revenue goals, without compromising security. What's the best way to do this?

Is Cybersecurity at Risk?

As airports increasingly rely more on bytes than bricks to balance the needs and expectations of various stakeholders, cybersecurity breaches to these systems are a significant and growing threat. As they pursue technological advantages, airports use burgeoning numbers of ad-hoc and bespoke solutions to address specific situations. Systems and data security often take a back seat. Even when security is considered, it is often addressed in a piecemeal fashion, almost as an afterthought, without alignment to the existing airport technology infrastructure.

The result has been a proliferation of technological solutions across the airport, comprised of a mix of equipment, devices and networks. State-of-art, contemporary and outdated systems are interconnected. Sensitive/restricted, operational and casual use devices are now part of a single ecosystem. The traditional walls that once separated these are disappearing rapidly and newer systems and devices do not have the requisite layers of secure separation. Systems are being integrated across boundaries to meet the information needs of different stakeholders such as airport operations, retailers and service providers, national and international governments, border control organizations as well as the travelers themselves.

In this complex and ever-evolving landscape, IT/OT systems are often the weak link waiting to be exploited. Once an attacker has breached a vulnerability, they can drive all forms of direct and indirect attacks—bombs, hijack, sabotage, or illegal trafficking and smuggling. For instance, a hacked baggage handling system can redirect a bag to another flight.

Heterogeneous airport networks are notoriously difficult to secure. Airports often rely on a vast array of point solutions and services to secure their IT and OT systems. Use of discrete solutions leaves gaps that malicious insiders or outside attackers can exploit. The interconnectedness of today's airport infrastructures means that once an attacker breaches a vulnerability, they can easily move across the network to potentially disrupt resources, leading to everything from nuisances to smuggling to irreparable damage.

A breached airplane de-icing system can alter the composition of de-icing chemicals to cause ice to form on the body of a plane, reducing maneuverability. Compromised X-ray equipment can prevent detection of prohibited items that can be used to serve someone's malicious intent. The possibilities are endless and frightening.

Are Airports Really Secure?

Heterogeneous airport networks are notoriously difficult to secure. Airports often rely on a vast array of point solutions and services to secure their IT and OT systems. Use of discrete solutions leaves gaps that malicious insiders or outside attackers can exploit. The interconnectedness of today's airport infrastructures means that once an attacker breaches a vulnerability, they can easily move across the network to potentially disrupt resources, leading to everything from nuisances to smuggling to irreparable damage. In recognizing the importance of cybersecurity, the International Civil Aviation Organization (ICAO), an international agency regulating aviation security, has passed Annex 17 and other regulations mandating that member states employ a security governance framework to implement appropriate measures to protect aviation safety and ensure security.

Airports need a way to secure their vast networks. At the same time, they must meet their operational needs by providing access to the multitude of users who rely on them, including airport staff, airlines, ground handlers, retail owners and caterers as well as passengers using kiosks to get their boarding passes and check-in their baggage. Airports must ensure that each of these users can access only the resources they need to do their jobs.

Trust No One

Increasingly, the answer from across the cybersecurity landscape is to take a Zero Trust approach. First introduced by analyst firm Forrester Research as an alternative architecture for IT security, the Zero Trust approach to airport network security protects against flaws by making security ubiquitous. Because Zero Trust considers all network traffic untrusted, this approach requires all resources to be secured, access to be limited, and access control policies to be strictly enforced.

Microsegmentation is an approach for implementing a Zero Trust network. Microsegmentation creates identity-based microsegments of the airport infrastructure called communities of interest (COI). The system assigns access rights based on the identity of the user or device employing the system, not IP address. This ties access rights to the user so they're not dependent on network topology. Each COI gives each user or device "least privilege" access to only the systems they need to do their jobs. One COI might give baggage handling personnel access to only the systems that track gates and flight departure times while another COI might provide only the staff in charge of managing the boarding process as well as security guards with the ability to control the e-gate. Only users or other servers that belong to a server's COI can access designated resources; these resources are undetectable to all unauthorized users and will not respond to pings or probes from non-COI members.

Microsegmentation further reduces risk by encrypting all communications between users/devices and protected assets whether the systems are on internal or external networks.

Multiple secure communities can share the same physical network without other groups being able to access, or even see their workstations and servers. Because COIs enable logical segregation and isolation of network data and users, airports don't need to implement multiple physical networks or additional networking equipment such as firewalls, switches or routers.

By ensuring that no traffic is trusted, authenticating users and devices, and allowing them to access resources only in their COI, microsegmentation significantly reduces the attack surface and limits lateral movement of attacks. Dynamic isolation makes it easier for airports to stop any attacks that do get through in their tracks. And a software-only solution simplifies implementation despite the complexity and heterogeneity of most airport's current and future IT/OT infrastructure.

Microsegmentation dramatically reduces the IT and OT attack surface since resources are only accessible to authorized users. Because users can only access resources within their COI, it prevents lateral movement of unauthorized users. And it protects airport systems from any type of unauthorized user, whether they're an internal or an external attacker.

In the Face of an Attack

Despite the many protections COIs afford, no solution is foolproof. Therefore, any microsegmentation approach also needs safeguards in place to rapidly isolate systems should an attack occur, to prevent that attack from spreading across the network.

The solution, in conjunction with a Security Information and Event Management (SIEM), should thus continuously monitor endpoints, networks and user behaviors to gain a cohesive, end-to-end visibility into threats. If a threat materializes or anomalous behavior occurs, the solution via the SIEM should detect that and alert the airport's security operations center (SOC) to the activity. Policies defined by the SOC via microsegmentation should then restrict or block network communications. Rapid isolation of compromised systems allows airports to identify the source of a breach and contain its impact.

Support for Current and Evolving Infrastructure

With the complexity and diversity of airport IT/OT infrastructures that have built up over the years, airports need a solution that simplifies the process of implementing a Zero Trust microsegmentation approach. More importantly, the solution should work with all of the heterogeneous solutions the airport already has in place and support their expansion plans as needed.

A software-only approach that requires no changes to the existing infrastructure or applications and works in any environment, regardless of vendor, as well as both on-premise and in the cloud, will reduce the complexity and expense of implementing security controls in an ever-changing environment. Such a solution will meet airports existing security requirements and give them the flexibility to choose vendors that address new business and IT needs. Such a system can also scale up with no disruption as airports expand in capacity and add more systems and devices to serve the growing number of travelers.

Conclusion

Airport IT/OT infrastructures are characterized by extreme complexity and heterogeneity. Current disjointed point security solutions can leave significant gaps and vulnerabilities that intruders can potentially exploit to steal data or gain unauthorized access to and potentially disrupt airport systems. By ensuring that no traffic is trusted, authenticating users and devices, and allowing them to access resources only in their COI, microsegmentation significantly reduces the attack surface and limits lateral movement of attacks. Dynamic isolation makes it easier for airports to stop any attacks that do get through in their tracks. And a software-only solution simplifies implementation despite the complexity and heterogeneity of most airport's current and future IT/OT infrastructure. In essence, microsegmentation can meet the current and evolving cybersecurity needs of airports.

Ready for the next step? Fill this questionnaire to avail a free Dark Market Scan to assess if your sensitive data is already at risk. (for APAC respondents only)

For more information visit www.unisys.com

Printed in the United States of America 10/19 19-0582