10.18686/aitr.v2i3.4415

Research on Security Model of Airport Luggage Remote Office System Based on Zero Trust

Hua Sun, Huixin Luo*, Jiazhou Geng

Industrial Information Security (Sichuan) Innovation Center Co., Ltd, Chengdu, Sichuan, 610000

Abstract: With the continuous development of modern information society, remote office equipment itself has many benefits and is widely respected by the public, but at the same time, it also brings many network security issues. In order to help the airport luggage remote office system achieve stability and solve security issues encountered during luggage inspection, an analysis of existing system security risks based on the zero trust concept is conducted, including factors such as data leakage, insufficient monitoring, and incomplete identity authentication. Combined with the characteristics of the luggage system and remote office technology, the security model is ensured to be sufficiently reliable, providing some reference for airlines preparing to implement zero trust airport luggage remote office.

Keywords: Zero trust; Airport luggage; Remote office system; Security model

With the rapid development of the aviation industry, the flow of personnel across regions is becoming increasingly frequent, and more and more passengers are choosing to travel by plane. The increase in tourist numbers has brought serious challenges to the luggage safety management of airports, and enterprises urgently need a safe management system to ensure the safety of passengers' luggage. Therefore, the airport luggage management system in today's era plays an important role in ensuring the safety of passenger luggage. An excellent and safe airport luggage management system will greatly improve the operational efficiency of enterprises and increase passenger satisfaction.

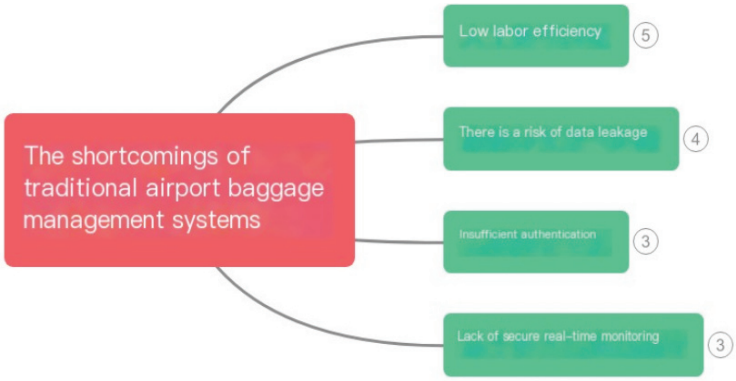
1. Introduction to the concept of zero trust

The zero trust concept is an emerging network security concept, which has a significant improvement compared to traditional network security models. The traditional concept of network security usually relies on boundary defense, which means increasing defense against boundary network environments (firewalls). If the system's boundaries are breached or internal areas are invaded, it is easy to obtain encrypted information because this method has almost 100% trust in the internal network environment. However, the zero trust model assumes that the security level of the internal and external network environments is the same, and will not trust anyone, any device, or even internal managers. The core of the zero trust concept is to "distrust and always verify" all devices. In this mode, all users, devices, and data streams must undergo strict identity verification (whether internal or external users). For users, this means that even if they enter the intranet through basic authentication, they still need to perform authentication when accessing encrypted resources. This type of pattern can greatly reduce malicious access and damage to the network environment. This mode also emphasizes continuous monitoring and detection, similar to the airport baggage management system. By monitoring luggage in real time, abnormal behavior can be detected in a timely manner and corresponding measures can be taken. By utilizing various security technologies and tools, establish a comprehensive security architecture to safeguard the legitimate interests of passengers. The zero trust concept emphasizes the concept of proactive defense, assists security managers in monitoring attacks, minimizes risks, and provides a new direction of thinking for security practitioners in enterprises.

2. The shortcomings of traditional airport baggage management systems

2.1 Low labor efficiency

In previous airport baggage management, manual methods were often used, with real-time monitoring by staff and regular troubleshooting of various areas. However, this type of method cannot obtain real-time information on the working status and operation of the baggage management system, resulting in the inability to detect and solve equipment problems in a timely manner. Another reason is that due to the wide variety of equipment, manpower alone cannot handle so many difficulties, resulting in staff only being able to perform maintenance after equipment problems occur, greatly reducing the efficiency of airport luggage management. However, human experience is far less abundant than computers, and when problems arise, they often rely on past experience to arrive at the scene to confirm the problem before taking solutions, which affects the efficiency of the entire luggage system operation. At the same time, the lack of a comprehensive and holistic obser-



vation approach hinders timely acquisition of equipment failure information, hinders comprehensive and in-depth understanding of system failures, and thus affects decision-making efficiency.

2.2 There is a risk of data leakage

In traditional airport baggage management systems, centralized data storage is usually used, which facilitates the centralized storage of all luggage information in the database for unified management. However, this storage method is very susceptible to attackers, and once the system is attacked, it will face the risk of a large amount of luggage information leakage. Due to the shortcomings of previous technologies, there is still a lack of sufficient encryption protection in data transmission, which makes it possible for data to be intercepted by attackers during transmission, thereby obtaining the privacy information of passengers.

Another point is that due to the negligence of internal employees, access permissions to the internal network may be leaked, providing opportunities for those who are willing to take advantage. If the access permissions of the system are not strictly controlled, attackers are given the opportunity to access unauthorized information through vulnerabilities, resulting in data tampering and, in some cases, data theft and trafficking.

2.3 Insufficient authentication

From a security perspective, authentication is widely present in various systems. Due to vulnerabilities in identity authentication, these systems are susceptible to fraud by attackers, leading to the occurrence of illegal access operations. Traditional forms of digital cryptography, due to their low complexity and insufficient strength, are prone to brute force attacks and increase the operational burden of the system. Meanwhile, when the system adopts single factor authentication, the lack of multiple verification factors can also provide convenience for attackers to steal user identities, posing a threat to the overall security of the system. Taking such confidentiality measures for important and critical data seriously weakens the system's protective capabilities, fails to ensure information security, and poses new challenges to the stable operation of the business.

2.4 Lack of secure real-time monitoring

Real time monitoring is essential in baggage management systems and is also a major challenge facing the current security field. Lack of monitoring means that it is difficult to detect existing security threats in a timely manner, further leading to the risk of management system attacks. The lack of real-time detection technology and alarm systems greatly reduces the system's ability to perceive potential threats, slows down its response speed, and increases the unstable operating factors of the system.

3. A solution strategy based on zero trust security concept

3.1 Utilizing end-to-end encryption technology

With the concept of zero trust, no one or device is trusted in the network environment, and end-to-end encryption technology is adopted to ensure the integrity of data during transmission and enhance data confidentiality. In practical applications, we can combine the security concepts of the new era to build a complete zero trust security system. This system not only includes end-to-end encryption technology, but also multiple security measures such as access control, identity authentication, and data isolation. Through these measures, we can ensure that the system remains robust and reliable in the face of various network security threats.

The solution strategy based on the zero trust security concept can effectively ensure the integrity and confidentiality of data during transmission by adopting end-to-end encryption technology. By combining multi-level and multi-dimensional security measures, we are confident in addressing the challenges of network security in the new era and ensuring stable and far-reaching system security. In this process, end-to-end encryption technology plays a crucial role in safeguarding the development of network security in China.

3.2 Adopting multi-level access control mechanisms

By adopting a multi-level access control strategy, users accessing the system are authenticated from multiple perspectives, including their identity information, device information, and other aspects, to prevent unauthorized visitors and ensure the legitimacy of their identities. In addition to the traditional username and password access mechanism, a dual factor authentication form and biometric authentication method can also be set up to ensure that only authorized users can access, and to ensure that users can only access authorized parts. For unauthorized parts, there is no viewing permission, thereby controlling the user's access range. Establish anomaly detection and early warning system, which can promptly alert and take corresponding measures when unauthorized data flows enter, improving the system's ability to identify and prevent unauthorized access.

4. Conclusion

In today's digital age, opportunities and risks coexist, which is related to the sensitive information field of passengers. To solve the problem of remote work in airport luggage management, the concept of zero trust can be effectively borrowed. The reasonable application of this concept can effectively help airports resist complex attacks encountered in luggage management. To fully implement the zero trust security concept, continuous efforts need to be made at the technical and other levels. In the future, by combining cloud computing, big data, and artificial intelligence technologies, the concept of remote work can be further integrated into daily management operations to improve the security of management systems. Only by constantly innovating and improving existing problems can we better ensure the security of passenger luggage information.

References

[1] Gong Jianfeng, Deng Hongqi, Wen Xinggen, Wang Qinkun. Research on Security Model of Mobile Office System Based on Zero Trust [J]. Information Record Materials, 2022, 23 (02): 38-40.

[2] Zhuo Wei. Research on Civil Aviation Airport Network Security Protection Scheme Based on Zero Trust Security Architecture [J]. Network Security Technology and Application, 2021, (11): 131-132.

[3] Wei Xiaoqiang. Research and Implementation of a Security Model for Remote Office Systems Based on Zero Trust [J]. Information Security Research, 2020, 6 (04): 289-295.

[4] Zhong Xiang, Guo Wei, Ma Yong, Wang Ming. Airport Network Security Protection Scheme Based on Zero Trust Security Architecture [J]. Journal of Civil Aviation, 2019, 3 (03): 114-116+107.

[5] Zhang Guanghua. Research on Security Model Based on Trust Management [D]. Xi'an University of Electronic Science and Technology, 2014.

[6] Bradatsch, L; Miroshkin, O; Kargl, F A Service Function Chaining Enable Zero Trust Architecture [C] 2023 IEEE 47th Conference on Local Computer Networks (LCN) Volume 11 Page 125307-125327 DOI 10.1109.

About the author:

Hua Sun(1979.5-), male, Han ethnicity, from Qujing City, Yunnan Province, doctoral degree, employer: Industrial Information Security (Sichuan) Innovation Center Co., Ltd, associate professor, research direction: artificial intelligence, big data processing.

Huixin Luo(2002.03-), female, from Luoyang, Henan province, research direction: artificial intelligence, big data processing.

Jiazhou Geng(2003.8-), male, Han ethnicity, from Liangshan, Sichuan Province, bachelor degree, an engineer, research direction: artificial intelligence, big data processing.

Project number: Key R&D projects in Sichuan Province+Research on Airport Luggage High Speed Sorting Security Control System Based on Zero Trust Security+2022YFSY0005.