SCIENCE AND INNOVATION
INTERNATIONAL SCIENTIFIC JOURNAL VOLUME 1 ISSUE 8
UIF-2022: 8.2 | ISSN: 2181-3337

MODELS FOR PROTECTING AIRPORT INFORMATION SYSTEMS FROM CYBER INCIDENTS

Allaberganov B.A.
Chief specialist of the Digital Development Department of the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan
Abdullayev D.Sh.
Master's degree, Faculty of Cyber-Security,Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

https://doi.org/10.5281/zenodo.7445057

Abstract. *In today's information age, government organizations and business enterprises are heavily relying on interconnected computer systems to manage a variety of public services including energy, transportation, water, etc. While this increased connectivity has many operational advantages benefitting the public, they have also become vulnerable to cyber attacks such as Corporate Security Breaches, Spear Phishing, and Social Media Fraud. The aviation sector is one the critical infrastructure systems that is not only vulnerable to physical threats, but also cyber threats, especially with the increased use of Bring Your Own Device (BYOD) at airports. It has been recognized that there is currently no cyber security standards established for airports in the United States as the existing standards have mainly focused on aircraft Control System (CS). This paper summarizes the need, background, ongoing developments and research efforts with respect to the establishment of cyber-security standards and best practices at U.S. airports with special emphasis on cyber security education and literacy.*

Keywords: *Airport, critical infrastructure, security, cyber, communications, networks, digital, penetration, vulnerability.*

МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ АЭРОПОРТОВ ОТ КИБЕРИНЦИДЕНТОВ

Аннотация. *В сегодняшнюю информационную эпоху правительственные организации и коммерческие предприятия в значительной степени полагаются на взаимосвязанные компьютерные системы для управления различными общественными услугами, включая энергетику, транспорт, водоснабжение и т. д. Хотя это расширение возможностей подключения дает много эксплуатационных преимуществ, приносящих пользу населению, они также становятся уязвимыми. к кибератакам, таким как нарушения корпоративной безопасности, целевой фишинг и мошенничество в социальных сетях. Авиационный сектор является одной из важнейших инфраструктурных систем, которая уязвима не только для физических угроз, но и для киберугроз, особенно в связи с более широким использованием в аэропортах принципа «принеси свое собственное устройство» (BYOD). Было признано, что в настоящее время для аэропортов в Соединенных Штатах не установлены стандарты кибербезопасности, поскольку существующие стандарты в основном сосредоточены на системе управления воздушным судном (CS). В этом документе обобщаются потребности, предыстория, текущие разработки и исследовательские усилия в отношении установления стандартов кибербезопасности и передовой практики в аэропортах США с особым акцентом на образование и грамотность в области кибербезопасности.*

Ключевые слова*: аэропорт, критическая инфраструктура, безопасность, кибер, связь, сети, цифра, проникновение, уязвимость.*

Introduction. Aviation is a subsector of the Transportation Systems Sector, one of 18 critical infrastructure and key resources sectors identified by the U.S. Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP). Among all the transportation modes, the avionics industry is one of the most advanced in its use of cyber-security standards. The US Federal Aviation Administration's (FAA's) National Airspace System (NAS) includes the US airspace, air navigation facilities, equipment, services, airports, aeronautical charts, information/ services, rules, regulations, procedures, technical information, manpower, and material. The FA A, in conjunction with the Joint Planning and Development Office (JPDO), is in the process of planning and implementing the Next Generation Air Transportation System (NextGen), which represents an evolution from a ground-based system of air traffic control to a satellitebased system of air traffic management with greater communication connections and services. The NAS cyber security architecture is changing drastically to support NextGen implementation by enforcing all network traffic to use one of the following traffic classifications: External Boundary Protection (EBP), Certified Software Management (CSM), Intrusion Detection and Response (IDR), and Internal Policy Enforcement (IPE).

Materials. The latest version of the Roadmap to Secure Control Systems in the Transportation Sector prepared by the transportation community and facilitated by US Department of Homeland Security's (DHS's) National Cyber-security Division (NCSD), Control Systems Security Program (CSSP), acknowledges that the NAS already has a mature cyber security program. Consequently, the Roadmap primarily focuses on control systems associated with airline information services and passenger information and entertainment services, broadly referred to as the aircraft control systems (TSWG, 2020).

Methods. The Roadmap (TSWG, 2020) recognizes that, with the introduction of new generation e-enabled aircraft (such as Boeing 787, Airbus A380, etc.) and the unprecedented amount of new technologies they support (e.x., IP-enabled networks, Commercial OffThe-Shelf [COTS], wireless connectivity, GPSs), aircraft cyber security vulnerabilities have increased exponentially. Similarly, the two-way transfer of critical information between the aircraft systems and the airport systems, via GateLink, Wireless LANs (WLANs), Avionics Full Duplex Switched Ethernet (AFDX) Networking, engine Health and Usage Monitoring Systems (HUMSs), and Electronic Flight Bags (EFBs), can significantly impact the cyber security of both the aircraft and the airports (TSWG, 2021). Airlines have also recognized the need for continuous improvement of information security strategies to guard against cyber threats. For instance, Boeing is working with the aviation industry and the information security industry to develop a unified cyber strategy. It is also actively developing a Cyber Technical Center that will be used for conducting cyber threat and vulnerability assessments, design cyber protection for Boeing airplanes and thereby support the cyber security needs of their airline customers (Rencher et al., 2020).

Results. There are approximately 450 commercial airports and 19,000 additional airports around the United States. Commercial airports have designated areas that have varying levels of security, known as secured areas, security Identification Display Areas (SIDA), Air Operations Area (AOA), and sterile areas (where passengers wait to board departing aircraft after screening). The SIDA and AOA typically include baggage loading areas, areas near terminal buildings, and other areas close to parked aircraft and airport facilities. Note that some airport operators may designate all AOAs as SIDAs (GAO, 2019). Just by virtue of the system itself, airports are particularly vulnerable to internal and external cyber threats and attacks from criminals, terrorists, or foreign actors (McAllister, 2021). Apart from the traditional IT infrastructure such as the email and the Internet, several potential targets for cyber attacks exist within the realm of internal airport operations (McAllister, 2021):

- Access control and perimeter intrusion systems,
- eEnabled aircraft systems,
- Credentialing and Document management systems (CAD, blueprints),
- Radar systems,
- Ground radar,
- Network-enabled baggage systems,
- Wireless and wired network systems,
- HVAC, • Facility management,
- Utilities,
- Supervisory Control and Data Acquisition (SCADA)-type ICSs.

Airport networks are vulnerable to cyber threats via number of ways (Cheong, 2011; Fortinet, 2012):

- USB drives,
- Laptops and netbooks,
- Wireless access points,
- Miscellaneous USB devices (digital cameras, MP3 players, etc.),
- Employees borrowing others' machines or devices,
- The Trojan Human (attackers who visit sites disguised as employee personnel or contractors),
- Optical media (CDs, DVDs, etc.),
- Lack of employee alertness,
- Smartphones,
- E-mail,
- Social networks,
- Targeted botnet attacks,
- Click jacking and cross-site scripting web attacks,
- Distributed Denial-of-Service (DDoS) attacks,
- Cloud computing concerns,
- Data exfiltration and insider threats,
- Online fraud.

In recent years, iPhones, iPads, Androids, and Tablets are a common sight in workplaces, referred to as Bring Your Own Device (BYOD). This trend is also catching up at airports where not only the airport users, but even the airport personnel wish to bring their own devices into the workplace. However, if these devices interact with enterprise systems (such as e-mail and VPN access) they can potentially be used secretly gather confidential information or introduce viruses. Airport employees need only their enterprise login credentials to be able to connect their unapproved personal devices to even a WPA2/802.1x secured network, requiring no permission from the administrator and exposing the network to security threats. A recent survey of IT professionals conducted by AitTight Networks revealed significant security concerns associated with unmanaged personal devices, i.e., BYOD (AirTight, 2020). Wireless Intrusion Prevention System (WIPS), Network Access Control (NAC), and Mobile Device Management (MDM) were identified as some technologies to deal with the increasingly common threat of unmanaged devices connecting to corporate networks. Similarly, the growing usage of mobile Wi-Fi hotspots can pose serious cyber threats since hardware options for mobile hotspots, such as Mi-Fi devices and USB Wi-Fi routers can be easily brought into airport premises and tools for soft hotspot creation are readily available on employee smartphones. It has been estimated that almost 20% of corporations have Rogue Access Points (APs) in their networks at some time which opens up the networks to a number of targeted cyber-attacks. Employees can unknowingly introduce viruses and allow nefarious users access to enterprise systems by visiting reputable websites (such as their local newspaper), clicking on a link in an email, visiting social media sites, or by inserting an infected USB drive in their computer or device.

Conclusion. The future intelligent airports will have advanced communications infrastructure that will support e-enabled aircrafts in the NextGen air transportation system and provide an open platform for end-toend services and supports applications for all, with increased risks associated with cyber threats. Although the increasing risks associated with cyber threats cannot be eliminated, implementing industry standards, good cyber security measures, best practices, and an educational program for all airport employees (and users) can help mitigate them. A defense-in-depth or beltand-suspenders approach is recommended in securing airports from cyber vulnerabilities where one does not rely on any one security mechanism to prevent all potential threats. Further, a user-focused cyber security education for all airport employees to make them aware of potential threats by a dedicated cyber security staff is crucial in mitigating vulnerabilities. National security agencies do recognize that combating cyber threats is a shared responsibility in which the public, private, and non-profit sectors, and every level of government have an important role to play. Thus, in identifying and responding to anomalous activity, airports can leverage their existing relationships with local, state, and federal law enforcement agencies to assist them to ensure an appropriate response and resolution.

In summary, despite all of the advances in technology, there does not exist a silver bullet to protect airport IT systems from all potential cyber threats. A defense-indepth or belt-and-suspenders approach is recommended where one does not rely on any one security mechanism to prevent all potential threats. Of course, in securing airport networks, the needs and the operational functionality have to be balanced to not allow security requirements hinder operations, but at the same time secure critical operations and protect against vulnerabilities being exploited. According to Nessi (2020), a layered security approach, investing in Unified Threat Management devices (UTMs), securing all endpoints of an airport network, keeping software applications as well as firmware upgrades in routers and switches, going compliant with Payment Card Industry Data Security Standard (PCI-DSS), securing enterprise databases that store personal information, including that of airport employees and airport community badge data, are all critical measures to be implemented by an airport manager with the help of the IT team to secure airports from virtual vulnerabilities.

REFERENCES

1. ACI-NA . 2021. ACI-NA Business Information Technology Committee Participation Plan. Airports Council International of North America. Available from Internet: .
2. AirTight Networks. 2020. Impacts of Bring Your Own Device (BYOD) on Enterprise Security. A Survey by AirTight Networks, Inc. Available from Internet: .
3. Cook, C. 2020. Heathrow Terminal 5: An IT Infrastructure success story. Airports International Magazine, Key Publishing Ltd.
4. Cheong, B. 2021. Cyber security at airports. Airports Council International of North America. Available from Internet: .
5. Duggan, D.P. 2020. SAND2005-2846P: Penetration Testing of Industrial Control Systems. Technical report, Sandia National Laboratories.
6. Fortinet. 2019. Top 10 Network Security Threats. Fortinet, Inc. Available from Internet: .
7. GAO. 2019. Aviation Security: A National Strategy and Other Actions Would Strengthen TSA’s Efforts to Secure Commercial Airport Perimeters and Access Controls.
8. GAO-09-399. Report to Congressional Requesters, US Government Accountability Office (GAO), Washington, D.C. Available from Internet: .
9. Hahn, A.; Kregel, B.; Govindarasu, M.; Fitzpatrick, J.; Adnan, R.; Sridhar, S.; Higdon, M. 2020. Development of the PowerCyber SCADA security testbed.