Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.7, March 2016 – www.caeaccess.org

An Analysis of Airports Cyber-Security

Khalid A. Fakeeh, PhD
FCIT,
King Abdul-Aziz University,
Jeddah, Saudi Arabia

ABSTRACT

Airports form part of the most important transport infrastructure of every nation state in the globe. The absolute number of inhabitants and data passing through airports each day and the apparent prospects to embezzle data, shake down money or set off anarchy makes them an unavoidable target for cyber attack. Cyber-security events are considerably growing year-on-year across the full spectrum of worldwide trade. Due to their visibility, interruption of the indispensable operations of airlines and airports could plausibly be the subject of a cyber-attack by cyber terrorists. Unluckily, not all airports have put into practice cyber-security systems that would defend and manage those operations and all connected aspects. It cleanly means that even though various may have security measures in place, cyber criminals, 'hacktivists', or cyber terrorists may possibly mull over this as a ideal opening to molest the airports in loads of diverse ways. We outline here the need, establishment, advancing progressions and research endeavors with respect to the establishment of cyber security standards and best practices with uncommon highlight on cyber security awareness.

Keywords

SCADA, Critical Infrastructures, Cyber Security

1. INTRODUCTION

Over the last decade, airports have made an incredible increase into the sprouting age of technology. User-friendly airline and airport websites, online check-in, unmanned border controls, computerized checked baggage systems, Wi-Fi networks, the list goes on. Nevertheless, networked hyper-connectivity exposes us to cyber-threats. And just as technology swiftly progress, cyber-threats are doing so too. In order to carry on the worldwide aviation system operating efficiently, the industry relies on information and communications technology (ICT) to bring critical information, allowing the people working inside the network. It is obvious that airport infrastructure holds up a lot of diverse operations that are critical for the effectiveness and success of the air transport system. The US Federal Aviation Administration's (FAA's) National Airspace System (NAS) comprises the US airspace, air navigation facilities, equipment services, plane terminals, aeronautical charts, information/ services, rules, regulations, techniques, specific information, labor, and material. The FAA, in conjunction with the Joint Planning and Development Office (JPDO), is presently masterminding and realizing the Next Generation Air Transportation System (NextGen), which addresses an improvement from a ground-based plan of air terminal regulation to a satellite-based course of action of air traffic control with more vital correspondence or communication connections and services. The NAS advanced security development displaying is changing profoundly to reinforce NextGen use by approving all network traffic to use one of the going hand in hand with action portrayals: External Boundary Protection (EBP), Certified Software Management (CSM), Intrusion Detection and Response (IDR), and Internal Policy Enforcement (IPE) [mitre.org]. The latest type of the Roadmap to Secure Control Systems in the Transportation Sector orchestrated by the transportation aggregate and energized by US Department of Homeland Security's (DHS's) National Cyber- security Division (NCSD), Control Systems Security Program (CSSP), perceives that the NAS starting now has a created cyber security program. Along these lines, the Roadmap basically focuses on control systems associated with elevated transport information services and voyager information and entertainment services, widely suggested as the carrier control systems [us-cert.gov]. The Roadmap [us-cert.gov] sees that, with the presentation of new generation e-enabled air transport, (for instance, Boeing 787, Airbus A380, et cetera.) and the marvelous measure of new developments they support (e.x., IP-enabled frameworks, Commercial Off-The-Shelf [COTS], wireless connectivity, GPSs), plane cyber security vulnerabilities have extended exponentially. Additionally, the two-way trade/transfer of fundamental information between the air transport systems and the air terminal systems, by method for GateLink, Wireless LANs (WLANs), Avionics Full Duplex Switched Ethernet (AFDX) Networking, engine Health and Usage Monitoring Systems (HUMSs), and Electronic Flight Bags (EFBs), can basically influence the cyber security of both the flying machine and the plane terminals [us-cert.gov]. Aeronautical transports have similarly seen the necessity for interminable change of information security industry to plan for advanced perils. Case in point, Boeing is working with the flight business and the information security industry to add to a united advanced methodology. It is moreover successfully building up a Cyber Technical Center that will be brought into play for coordinating cyber danger and vulnerability assessments, layout cyber security for Boeing planes and thusly supports the cyber security needs of their bearer customers [Securing airline Information]. The lately released 2013-2023 Transportation Industrial Control Systems (ICS) Cyber-security Standards Strategy organized by the DHS saw that there is starting now no cyber security standards developed for air terminals as the present benchmarks have basically based on plane Control System (CS) [trbcybersecurity]. Case in point, the going hand in hand with affiliations has together conveyed a couple records to propel the cyber security benchmarks in the flight business. The DHS's transportation ICS cyber security standards framework [trbcybersecurity] recognizes air terminal ICS cyber security as another thought and proposes to work with the Airport Council International – North America (ACI-NA) Business Information Technology (BIT) Committee to make air terminal ICS advanced efforts to establish safety. The ACI-NA BIT Committee is the structure for people with airport related IT commitments to network, communicate, offer data, conduct research and stay up with the most recent with the latest creative progressions. The middle districts of the BIT Committee consolidate airport information management system, private and open communication services, Intranet and Internet PC networking, system framework/design and utilization of up-to-the-minute advancement [aci-na.org 2012].

2. CYBER-RISKS TO THEINTERNAL OPERATIONS OF AIRPORT

Commercial airports have allotted domains that have varying levels of security, known as secured locales or areas, security Identification Display Areas (SIDA), Air Operations Area (AOA), and sterile areas. The SIDA and AOA generally fuse stuff stacking areas, ranges close terminal buildings, and distinctive regions close to parked plane and airport facilities. Note that some airport managers may appoint all AOAs as SIDAs [gao.gov]. Just by uprightness of the system itself, airports are particularly helpless against inside and external cyber perils and strikes from criminals, terrorists, or outside on-screen characters [aviationpros.com]. Beside the customary IT establishment, for instance, the email and the Internet, a couple of potential targets for cyber ambushes exist within the area of internal airport operations [aviationpros.com].

a. Perimeter intrusion and access control systems
b. e-Enabled aircraft systems
c. Credentialing and Document management systems (CAD)
d. Supervisory Control and Data Acquisition (SCADA) based ICSs
e. Radar systems,
f. Ground radar
g. Network-enabled bagged systems
h. Wired and wireless network systems
i. Utilities
j. HVAC (Heating, Ventilation and Air Conditioning)
k. Facility management

Further than physical security at airports, cyber risks to internal operations of airport are ascending to be a fundamental concern especially with the growing use of flexible applications and compact equipment (mobile hardware). To give an example, Heathrow's Terminal 5 tremendous IT system sponsorships limits, for instance, a 1,500 camera CCTV structure, 1,100 ensured access control points, a remote LAN with 750 access points, and 2,800 telephones in light of a hybrid structural design of analogue, digital and IP telephony which are all weak against cyber threats. In fact, even undersized airports are energetically dependent on organized networked computer systems for step by step operations and are subsequently weak against advanced risks. [aci-na.org] if insights with respect to different cyber scenes at Los Angeles World Airports (LAWA) related to private network baggage system interference by a malware, zombie equipped power “a collection of internet-connected computers whose security resistances have been cracked and set up to forward spam without the proprietors' data” or botnet grasping community wellbeing private network, a couple of million hacking attempts and countless misuse and ill-treatment tries. The networks of airports are unprotected/vulnerable against cyber risks through number of ways [aci-na.org] [fortinet.com]:

a. Wireless access centers
b. Laptops and notebooks
c. USB drives
d. Various USB in the form of cameras, MP3 players, et cetera
e. Employees make use of others machines or devices,
f. The Trojan Human (aggressors who visit sites disguised as laborer work power or developers
g. Optical media in the form CDs, DVDs, et cetera
h. Lack of member of staff attentiveness
i. E-mail,
j. Social networking
k. Online blackmailing
l. Smartphone’s
m. Targeted botnet attacks
n. Click jacking and cross-site scripting web ambushes
o. Distributed Denial-of-Service (DDoS) attacks
p. Data exfiltration and insider risks
q. Cloud computing concerns

Recently, iPhones, iPads, Androids, and Tablets are a normal sight in workplaces, suggested as Bring Your Own Device (BYOD). This example is moreover compensating for lost time at airports where the airport customers and additionally even the airport staff wish to bring their own devices into the workplace. Regardless, if these devices coordinate with enormous business systems, for instance, email and VPN access, they can possibly be employed subtly amass private information or bring in viruses. Airport staffs require only their attempt login capabilities to have the ability to connect their unapproved individual contraptions/devices to even a WPA2/802.1x secured network, obliging no approval from the head and introducing the network to security perils. A late investigation of IT specialists coordinated by AitTight Networks revealed basic security concerns joined with unmanaged individual devices, i.e., BYOD [airtightnetworks.com]. Wireless Intrusion Prevention System (WIPS), Network Access Control (NAC), and Mobile Device Management (MDM) were recognized as a couple of progressions to deal with the relentlessly fundamental danger of unmanaged contraptions/devices joining with corporate frameworks/networks. Additionally, the creating use of adaptable Wi-Fi hotspots can act bonafide advanced perils since hardware decisions for mobile hotspots, for instance, Mi- Fi devices and USB Wi-Fi switches can be viably brought into airport premises and gadgets for sensitive hotspot creation are instantly available on illustrative mobile phones.

It has been surveyed that practically 20 percent of associations have Rogue Access Points (APs) in their networks eventually which opens up the networks to different concentrated cyber ambushes/threats or attacks. Staff can unknowingly exhibit viruses and license wretched customers access to huge business systems by passing trustworthy websites, tapping on an association in an email, passing by internet organizing destinations, or by embeddings a corrupted USB drive in their PC or contraption/device. In a late study, Gartner Mobile and AirTight Networks attempted wireless security at fourteen airports in the US, Canada, and Asia [infosecurity-magazine]. The study revealed that each one of the fourteen air terminals or airports is using open or insufficiently secured wireless networks. Among the Wi-Fi frameworks recognized by the investigators at the airports, 77 percent were private (non - hotspot) networks and of those, 80 percent were unsecured or using legacy WEP (Wired Equivalent Privacy) encryption, considered as a mortally blemished encryption protocol by the business/industry. Beside the ticketing systems, baggage systems, shops, and restaurants, some of these Wi-Fi networks are also brought into play for fundamental airport logistics and operations. The study in like manner uncovered that only three percent of the each mobile customer were exercising VPNs while ten percent of the tablets recognized in the midst of the breadths were defiled with a viral Wi-Fi network [infosecurity-magazine].

3. VULNERABILITIES ASSESSMENT & ITS METHODOLOGIES

Airports routinely rely on upon SCADA based Industrial control systems (ICS) for HVAC (Heating, Ventilation and Air Conditioning), utilities, baggage systems, and business methods, for instance, facility management. In view of their limited or unlucky deficiency of web access, SCADA-type systems may emit an impression of being more secure, on the other hand they too are defenseless against cyber perils. While cyber frailty or vulnerability assessments have transform into a regulated process in IT, they have pretty much starting late got hugeness in SCADA circumstances. Demand from the IT side has driven the progression of evaluation gadgets, test methods, impact scoring and reporting frameworks to help with the unflinching quality and efficiency of the examination strategy. The resemblances between ordinary IT and SCADA structures/systems should ensure a touch of IT assessment frameworks have some real nature to SCADA milieu. The airport SCADA-type ICS work in a general sense the same to SCADA systems used as a piece of the power base infrastructure systems or some other industry. The evaluation of cyber vulnerabilities in industry control systems and critical infrastructure systems have been a renowned zone generally examine. The Idaho National Laboratory (INL) has developed the National SCADA Testbed (NSTB) which bestows a resource for evaluate separating/critical vulnerabilities in pragmatic SCADA systems [National Scada testbid] INL has given investigation recording cyber vulnerabilities consistently found in SCADA systems and has similarly given a layout of instruments and techniques exercises to carry out this examination [common cybersecurity vulnerabilities 2008]; [Permann et al]. Research at Sandia National Laboratory has bestowed guidance on performing a cyber frailty or vulnerability assessment on a SCADA system [guide to cir]. Additional work has had a tendency to mindfulness toward performing penetrations tests on control systems [Duggan et al]. At Iowa State University, [Hahn et al] have added to the PowerCyber testbed to give a practical SCADA system to cyber vulnerability assessment [Hahn et al]. The testbed uses certifiable hardware and software to furnish a careful representation of a SCADA system. The parts contained in the testbed join human-machine interfaces (HMIs), SCADA servers, remote terminal units (RTUs), overcurrent protection relays, historian servers and virtual private network (VPN) devices. The HMI gives the head an interface to the SCADA server. This is utilized to perform checking and control of the system operations. The SCADA server interacts with the RTUs in the best possible substations and relays commands from the HMI. The RTU gives a joined system within a substation to relate with diverse intelligent electronic devices (IEDs). The testbed has a control center, two substation automation systems, and a couple of virtual substation systems. The control center contains the HMI, SCADA server, and historian server. Each substation contains a RTU which is joined with a relay. Correspondence or communication between the control center and substation is with the VPN devices which endow with a safe and sound channel.

3.1. Methodologies

Vulnerability assessments are frequently executed as white-box tests where analyzers have access to personnel, documentation, and configuration with a particular deciding objective to obtain a full cognizance of all prospective security flaws. In the midst of a vulnerability assessment security concerns are filed, yet no abuse happens.

A. Infiltration or Penetration testing: This comprises endeavors to takes advantage of deficiencies to endorse its reality and settle on the reasonableness of a cyber attack. From a SCADA perspective, vulnerability assessments will typically be supported as they give a complete overview of the security stance. Additionally, it is generally not endorsed to perform penetration testing on production SCADA systems [Duggan et al].

B. Acquiescence or compliance requisites:

A basic focus for a cyber security assessment procedure is the ability to make sense of if consistence necessities have been sufficiently meet. Since SCADA systems supporting the mass power system are obliged to be NERC Critical Infrastructure Protection (CIP) compliant, an effective SCADA test strategy must survey each individual requisite.

C. Analysis/review of Network Traffic: The analysis or review of network traffic is obliged to get an escalated appreciation of the network communication. The review or analysis of network traffic bestows the analyzer a perception of what services of network are being gotten to and what data is being experienced the network.

D. Analysis/review of System Configuration: The analysis or review of a system configuration is liable to data or knowledge of known security dilemmas within the software and current best practice. While there are all around chronicled security baselines for some celebrated IT software products, most SCADA software has not experienced equivalent examination.

E. Network Detection, Protocol and Port recognition: Although information about network host and communication protocols should be clearly seen by the network operators, the discovery or detection process is critical to acknowledge any suppositions.

F. Scrutinizing or Inspection of vulnerability: The cyber vulnerability assessment guide built up by the United States Computer Emergency Readiness Team (US-CERT) and NIST perceives the going hand in hand with key vulnerabilities: remote access points, network access points, unsecured SQL databases, ineffectually configured firewalls, interconnected peer networks with delicate security, and so forth.

Protecting SCADA systems in airports from cyber risks obliges strapping cyber security to set up wellbeing and routine cyber vulnerability assessments. The appraisal of contemporary cyber security examination instruments/tools has given a couple concerns in regions where additional exploration is requisite. The going with are a couple of cleft that have been found while performing a past cyber security evaluation as a result of differences in IT and SCADA milieus: significant reliance on prohibitive network protocols, undocumented software versions, unlucky deficiency of documentation addressing ample configurations, and system steadfastness concerns in the midst of an assessment.

4. INFORMATION ASSURANCE AND SECURITY INSTRUCTIONS

Information security or assurance has transform into a commonplace term used by various, often in reference to a dispute amidst hackers/intruders and security specialists, or what various see as a war of the geeks. The term information security can have various definitions; some use it as a general term portraying all security-related concerns with advancement, while others use it as a sub-portrayal of a more broad class, for instance, information insistence. Fundamentally, assurance is the strategy of protecting information from risks. This can be further elucidated through what is routinely implied as the C-I-A model: i) Confidentiality - keeping unapproved customers away from examining or getting to information, ii) Integrity - ensuring that an unapproved customer has not changed information, iii) Availability - checking that information can be gotten to when needed by affirmed customers [Jacobson et al]. Routine IT security consistently focuses on the utilization of security controls additionally frameworks at the application, operating system, network, or physical technology layers. With the extended usage of BYOD at airports, there is a need to make cyber security get ready materials that instruct and educated the staff of airport from the perspective of the customer/user-layer – the affiliations or interactions all customers experience with development or technology reliably paying little regard to concentrated capacity. The vital framework or mechanism for educating the general populace about cyber security has been to create top-ten security list. Top ten lists communicates a confused feeling all is well and great to its perusers as it deduces all that is imperative to fulfill security is to make after these wide strides. What happens – and it will happen, frequently – when a customer is given a condition that is not secured by a bullet point or visual prompt? [Jacobson et al]. Notwithstanding the way that the underpinnings of PC security are of a particular nature, different thoughts are of a sensible nature and can be detached to the customer or user layer. In case PC security guideline is abstracted viably, realistic security education can be made open to both airport staff and users with immaterial specific or technical establishments. Everyone performs the same key timetables on our PCs and the Internet consistently. In the midst of a typical day, people use passwords, interface with the Internet on an unsecure remote connection, offer media through external devices, surf the web, tap on hyperlinks, offer information by method for long range interpersonal communication, and much, altogether more. Each of these exercises incorporates a potential risk and can realize poisonous results; countless the ordinary non-concentrated or non-tehnical customer is oblivious [Jacobson et al]. In making manuals and multi-media materials for training staff of airport and customers in potential cyber vulnerabilities and cyber-security best practices, the going with key principles of information affirmation must be thought about over [Jacobson et al]:

i. Security is a subject to budgetary angles: When picking what information to guarantee and how to protect it, the first question that should be inquired is, is it legitimized, in spite of all the hassle? In a manner of speaking, security costs time and money, and if the information or entity that is being guaranteed has little regard, it doesn’t look good to spend advantages for secures it.

ii. Security ought to be made out of layers of defenses: There is no one solitary security approach that can shield all information from prospective molests. A layered system will construct it more troublesome for some person to become acquainted with your information since an interloper must avoid different security schedules or approaches to acquire right of entry. If one layer falls short, there are additional layers situated up to compensate and keep away a break of security.

iii. Unconditional security does not exist: We can't secure next to each potential event, especially when we can't suspect every potential security hazard. No security system can be admired in overseeing either the physical or the PC world. By utilizing a defense-in-depth method, one can exceptionally upgrade the general security of computing devices and the protection of modernized information.

iv. Security is conflicting with expediency: In the physical world, security frequently incorporates extra steps or frameworks to guarantee a regarded thing. The more security segments added to a computer system, the more intrusive endeavors to build up wellbeing may be, much of the time bringing on customer frustration. While added measures provide improved security, they are similarly conflicting with settlement or convenience and over the long term solace tends to trump security.

In rundown, regardless of most of the technology advances, there does not exist a versatile thing to shield airport IT structures/systems from all potential cyber perils.

5. SUMMARY

The prospect smart airports will have progressive and augmented communication critical infrastructures and structural design that will support e-enabled airplanes in the NextGen air transportation structure and give an open stage to end-to-end services and sponsorships applications for all, with extended jeopardy allied with cyber intimidations. Notwithstanding the way that the extending perils associated with cyber risks can't be wiped out, realizing industry gages/standards, extraordinary cyber endeavors to build up wellbeing, best practices, and an informative venture for all airport delegates, staff and customers or users can lend a hand ease them. A defense-in-depth approach is suggested in securing airports from cyber vulnerabilities where one does not rely on upon any one security framework to keep each potential peril. Hence, in perceiving and retorting to atypical development, airports can impact their present association with neighborhood, state, and government law agencies to facilitate them to guarantee a fitting response and determination.

6. REFERENCES

[1] ”Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment. Technical report, Sandia National Laboratories, 2007 by ”Parks, R.C.”,.

[2] ”Hahn, et al”. ”Development of the PowerCyber SCADA security testbed. 2010”. In Proceedings of the CSIIRW ’10.

[3] ”Securing Airline Information on the Ground and in the Air. The Boeing Company, Aero Quarterly, QTR_03. 25-28 by ”Rencher, et al..”..

[4] ”http://trbcybersecurity. erau.edu/files/Transportation-Standards-Plan.pdf”.

[5] ”http://www.airtightnetworks.com/fileadmin/pdf/ AirTight-BYOD-Survey-April-2012.pdf”.

[6] ”Penetration Testing of Industrial Control Systems. Technical report, Sandia National Laboratories by ”Duggan et al..”.

[7] ”http://www.gao.gov/ new.items/d09399.pdf”.

[8] http://www. fortinet.com”.

[9] ”http://www.mitre.org/work/tech_ papers/2011/10_4169/10_4169.pdf”

[10] ”http://www.us-cert.gov/control_systems/ pdf/TransportationRoadmap083112.pdf”.

[11] ”Computer Security Literacy: Staying Safe in a Digital World. Chapman & Hall/CRC Press, First Edition, Boca Raton by ”Jacobson, et al”, USA.

[12] National SCADA Test Bed: Fact Sheet. Idaho National Laboratory (INL), Idaho, INL. 2007..

[13] http://www.infosecurity-magazine.com/view/1206/cyber-security-lacking-at-airports.

[14] Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. Technical report, Idaho National Laboratory (INL), INL. 2008..

[15] ”http://www.aviationpros.com/ article/10522704/cyber-security-for-airports”.

[16] ”http://aci-na.org/sites/default/files/ cheong-cybersecurity-bit.pdf”.

[17] ”Cyber Assessment Methods for SCADA Security. Technical report, The Instrumentation, Systems and Automation Society (ISA) by ”Permann, et al...”.

[18] ”http://www.aci-na.org/sites/default/files/ bit_committee_participation_2012.pdf”.