International Journal for Traffic and Transport Engineering, 2013, 3(4): 365 - 376
DOI: http://dx.doi.org/10.7708/ijtte.2013.3(4).02 UDC: 351.814.31 ; 656.71.08

CYBER SECURITY FOR AIRPORTS

Kasthurirangan Gopalakrishnan[1], Manimaran Govindarasu[2], Doug W. Jacobson[3], Brent M. Phares[4]

[1] *Department of Civil, Construction and Environmental Engineering, Iowa State University, USA*
[2, 3] *Department of Electrical and Computer Engineering, Iowa State University, USA*
[4] *Bridge Engineering Center, Institute for Transportation, Iowa State University, USA*

Received 19 June 2013; accepted 19 August 2013

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.

1. 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. A conceptual schematic of the major inter-connected components of the NAS are depicted in Fig. 1 (Williams and Signore, 2011).

The FAA, 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 satellite-based system of air traffic management with greater communication connections and services. The NAS cyber security architecture is changing drastically to

[1] Corresponding author: rangan@iastate.edu

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) (Williams and Signore, 2011).

The latest version of the *Roadmap to Secure Control Systems in the Transportation Sector* (Version 3.0, August 31, 2012) 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, 2012).

The Roadmap (TSWG, 2012) 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 Off-The-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, 2012). 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., 2012).

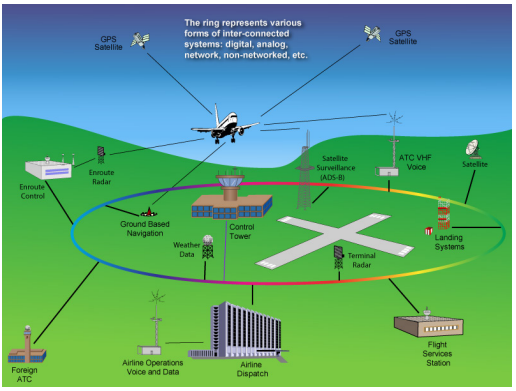

Fig. 1.
Major Components of US FAA's National Airspace System (NAS)
Source: Williams and Signore (2011); figure reproduced with permission from MITRE

The recently released *2013-2023 Transportation Industrial Control Systems (ICS) Cyber-security Standards Strategy* prepared by the DHS noted that there is currently no cyber security standards established for airports as the existing standards have mainly focused on aircraft Control System (CS) (Kaiser, 2012). For instance, the following organizations have together produced several documents (not available for public viewing at this time) to promote the cyber-security standards in the aviation industry, but mainly pertaining to aircraft CS:

- Airlines Electronic Engineering Committee (AEEC),
- Aircraft Information Security Subcommittee,
- Radio Technical Commission for Aeronautics (RTCA),
- Aeronautical Radio Incorporated (ARINC), and
- European Organization for Civil Aviation Equipment (EUROCAE).

The DHS's transportation ICS cyber security standards strategy (Kaiser, 2012) identifies airport ICS cyber-security as a new concept and proposes to work with the Airport Council International – North America (ACI-NA) Business Information Technology (BIT) Committee to develop airport ICS cyber-security standards. The ACI-NA BIT Committee is the form for members with airport-related information technology responsibilities to network, communicate, share data, conduct research and keep up-to-date with the latest technological developments. The focus areas of the BIT Committee include airport information management systems, private and public communication services, Intranet and Internet computer networking, system design and application of new technology (ACI-NA, 2011). The DHS's strategy also proposed to work with ACI-NA and with major and minor airports in compiling common control systems and best practices for airport ICS cyber-security. An ongoing Airport Cooperative Research Program (ACRP) project in the U.S. is developing a guidebook to help airports develop and a cyber-security program and multi-media materials that address risk awareness by highlighting the different cyber security threats likely to be confronted by airports that can be used by cyber security/IT professionals to educate airport staff.

2. Cyber Threats to Internal Airport Operations

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 (Fig. 2). Note that some airport operators may designate all AOAs as SIDAs (GAO, 2009).

Just by virtue of the system itself, airports are particularly vulnerable to internal and external cyber threats (Fig. 3) and attacks from criminals, terrorists, or foreign actors (McAllister, 2011). 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, 2011):

- 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.

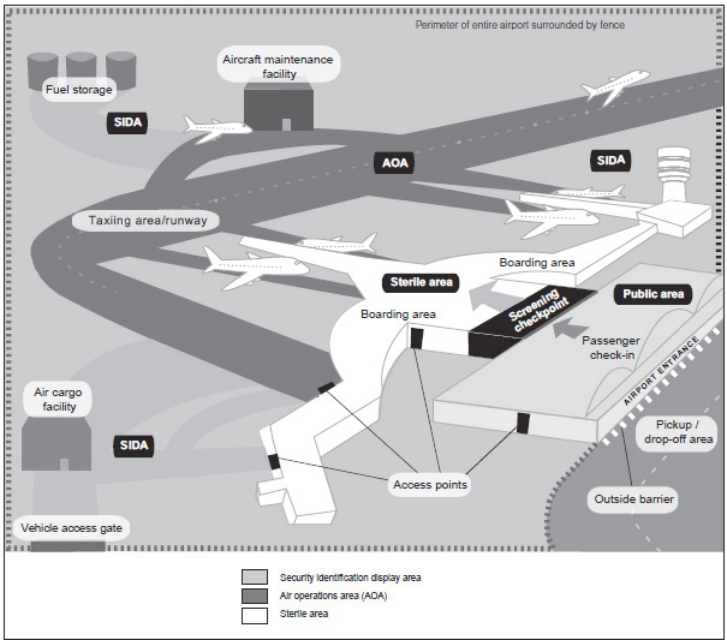

Fig. 2.
Commercial Airport Areas with Varying Levels of Physical Security
Notes: SIDA – Security Identification Display Areas; AOA – Air Operations Area
Source: GAO (2009)

Beyond physical security at airports, cyber threats to the internal airport operations are emerging to be a primary concern especially with the increasing use of mobile applications and mobile hardware. To give an example, Heathrow's Terminal 5 massive IT infrastructure supports functions such as a 1,500 camera CCTV system, 1,100 secure access control points, a wireless LAN with 750 access points, and 2,800 telephones based on a hybrid architecture of analogue, digital and IP telephony (Fig. 4) which are all vulnerable to cyber threats. Even small airports are heavily dependent on networked computer systems for daily operations and are therefore vulnerable to cyber threats. Cheong (2011) reported on a number of cyber incidents at Los Angeles World Airports (LAWA) related to private network baggage system intrusion by a malware, zombie army (a collection of internet-connected computers whose

security defenses have been breached and set up to forward spam without the owners' knowledge) or botnet taking hold of public safety private network, a couple of million hacking attempts and tens of thousands of internet misuse and abuse attempts.

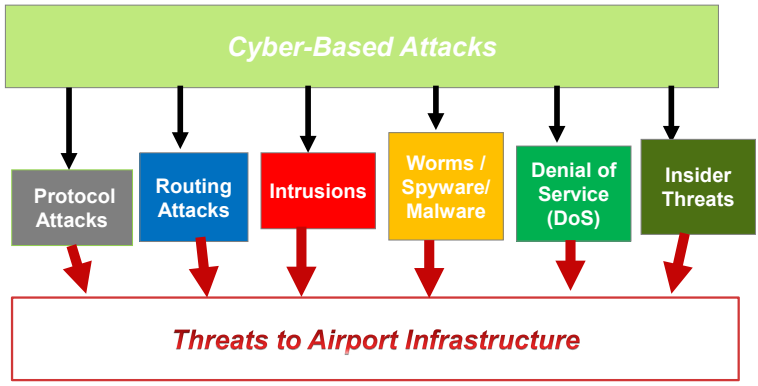

Fig. 3.
Cyber-Based Threats to Airports

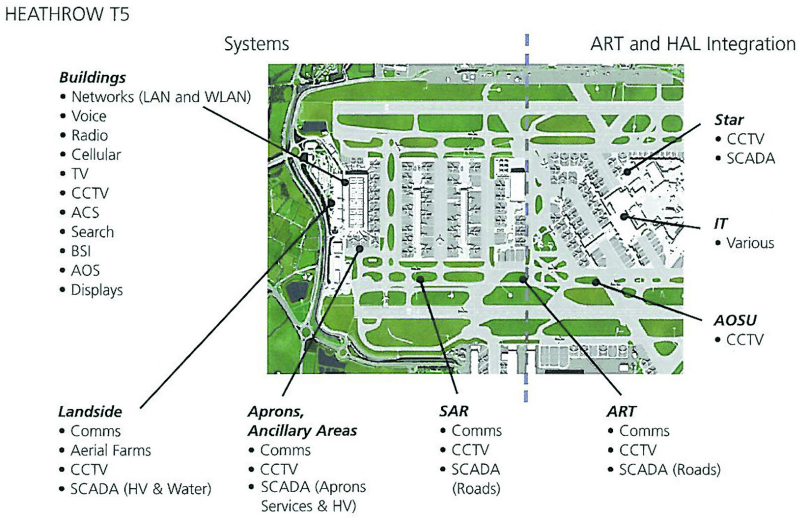

Fig. 4.
Services Supported by the Information Technology Infrastructure at London Heathrow's International Airport Terminal 5 Designed to Handle 35 Million Passengers Annually
Notes: HAL – Heathrow Airport Limited; ART – Airside Road Tunnel; BSI – Building Systems Integration; ACS – Access Control System; AOS – Airport Operational Systems; AOSU – Airside Operational Safety Unit
Source: Cook (2010)

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, 2012). 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.

In a recent study, Gartner Mobile and AirTight Networks tested wireless security at fourteen airports in the US, Canada, and Asia (Infosecurity, 2008). The study revealed that all fourteen airports are using open or poorly secured wireless networks. Among the Wi-Fi networks detected by the researchers at the airports, 77% were private (non-hotspot) networks and of those, 80% were unsecured or using legacy WEP (Wired

Equivalent Privacy) encryption, considered as a fatally flawed encryption protocol by the industry. Apart from the ticketing systems, baggage systems, shops, and restaurants, some of these Wi-Fi networks are also used for critical airport logistics and operations. The study also revealed that only three percent of the all mobile users were using VPNs while ten percent of the laptops detected during the scans were infected with a viral (ad-hoc) Wi-Fi network (Infosecurity, 2008).

3. Evaluation of Cyber Vulnerabilities in Airport Industrial Control Systems

Airports typically rely on SCADA-type industrial control systems for HVAC, utilities, baggage systems, and business processes such as facility management. Due to their limited or lack of internet access, SCADA-type systems may appear to be more secure, but they too are vulnerable to cyber threats. While cyber vulnerability assessments have become a standardized process in IT, they have only recently gained importance in SCADA environments. Demand from the IT side has driven the development of evaluation tools, test methodologies, impact scoring and reporting procedures to assist with the reliability and efficiency of the assessment process. The similarities between traditional IT and SCADA systems should ensure a portion of IT assessment methods have some applicability to SCADA environments.

The airport SCADA-type industrial control systems function very similar to SCADA systems used in the power infrastructure systems or any other industry. The evaluation of cyber vulnerabilities in industry control systems and critical infrastructure systems have been a popular area of recent research. The Idaho National Laboratory (INL) has established the National SCADA Testbed (NSTB) which provides a resource to evaluate critical vulnerabilities in realistic SCADA systems (INL, 2007). INL has provided research documenting cyber vulnerabilities commonly found in SCADA systems and has also provided an overview of tools and techniques utilizes to perform this analysis (INL, 2008; Permann and Rohde, 2005). Research at Sandia National Laboratory has provided guidance on performing a cyber vulnerability assessment on an SCADA system (Parks, 2007). Additional work has addressed concerns for performing penetrations tests on control systems (Duggan, 2005).

At Iowa State University, Hahn et al. (2010) have developed the PowerCyber testbed to provide a realistic SCADA system for cyber vulnerability evaluation (Hahn et al., 2010). The testbed utilizes real-world hardware and software to provide an accurate representation of a SCADA system. The components contained in the testbed include human-machine interfaces (HMIs), SCADA servers, remote terminal units (RTUs), overcurrent protection relays, historian servers and virtual private network (VPN) devices. The HMI provides the operator with an interface to the SCADA server. This is utilized to perform monitoring and control of the system operations. The SCADA server communicates with the RTUs in the appropriate substations and relays commands from the HMI. The RTU provides a centralized system within a substation to communicate with various intelligent electronic devices (IEDs), such as the relays. The testbed has a control center, two substation automation systems, and several virtual substation systems. The control center contains the HMI, SCADA

server, and historian server. Each substation contains a RTU which is connected to a relay. Communication between the control center and substation is protected with the VPN devices which provide a secure channel.

3.1. Assessment Methodologies

Technical security evaluations are often categorized as either vulnerability assessments or penetration tests. While both share common techniques, there are significant differences in how they are performed and their impact on the target systems. Vulnerability assessments are an evaluation of technical vulnerabilities in a system. Vulnerability assessments are typically performed as white-box tests where testers have access to documentation, configurations and personnel in order to obtain a full understanding of all potential security weaknesses. During a vulnerability assessment security concerns are documented, but no exploitation occurs.

- *Penetration testing*: This involves attempts to exploit weaknesses to validate its severity and determine the feasibility of a cyber attack. From a SCADA perspective, vulnerability assessments will typically be preferred as they provide a comprehensive review of the security posture. In addition, it is generally not recommended to perform penetration testing on production SCADA systems (Duggan, 2005).

- *Compliance Requirements:* An important objective for a cyber security assessment methodology is the ability to determine whether compliance requirements have been sufficiently meet. Since SCADA systems supporting the bulk power system are required to be NERC Critical Infrastructure Protection (CIP) compliant, an effective SCADA test methodology must evaluate each individual requirement.

- *Network Traffic Review:* The review of network traffic is required to gain a thorough understanding of the network communication. The review of network traffic provides the tester with an understanding of what network services are being accessed and what data is being passed through the network.

- *System Configuration Review:* The review of a system's configuration is dependent on knowledge of known security issues within the software and current best practice. While there are well documented security baselines for many popular IT software products, most SCADA software has not undergone comparable analysis.

- *Network Discovery, Port and Protocol Identification:* Although information about network host and communication protocols should be well known by the network administrators, the discovery process is necessary to validate any assumptions.

- *Vulnerability Scanning:* The cyber vulnerability assessment guide developed by the United States Computer Emergency Readiness Team (US-CERT) and NIST identifies the following key vulnerabilities: wireless access points, network access points, unsecured SQL databases, poorly configured firewalls, interconnected peer networks with weak security, and several others.

Securing SCADA systems in airports from cyber threats requires strong cyber security measures and routine cyber vulnerability assessments. The evaluation of current cyber security assessment tools has provided some concerns in areas where additional research is required. The following are some gaps that have been found while performing a previous cyber security assessment due to differences in IT and SCADA environments: heavy reliance on proprietary network protocols, undocumented software versions, lack of documentation addressing appropriate configurations, and system stability concerns during an assessment.

4. Airport Information Assurance and Cyber Security Education

Information security has become a common term used by many, often in reference to a conflict between "hackers" and security professionals, or what many see as a war of the geeks. The term information security can have many definitions; some use it as an overarching term defining all security-related issues with technology, while others use it as a sub-classification of a broader category, such as information assurance. Simply put, *security/assurance is the process of protecting information from threats*. This can be further explained through what is often referred to as the C-I-A model: (1) *Confidentiality* - preventing unauthorized users from reading or accessing information, (2) *Integrity* - ensuring that an unauthorized user has not altered information, (3) *Availability* - making sure that information can be accessed when needed by authorized users (Jacobson and Idziorek, 2012).

Traditional IT security typically focuses on the implementation of security controls and mechanisms at the application, operating system, network, or physical technology layers (Fig. 5). With the increased use of BYOD at airports, there is a need to develop cyber security training materials that seeks to educate airport employees from the perspective of the user-layer – the interactions all users experience with technology on a daily basis regardless of technical prowess. The primary method for educating the general public about cyber security has been to construct top-ten security lists. Top ten lists communicate a false sense of security to its readers as it implies all that is necessary to achieve security is to follow these broad steps. What happens – and it will happen, often – when a user is presented with a situation that is not covered by a bullet point? (Jacobson and Idziorek, 2012).

Although the underpinnings of computer security are of a technical nature, a number of concepts are of a practical nature and can be abstracted to the user-layer. If computer security education is abstracted correctly, practical security education can be made accessible to both airport users and airport employees with minimal technical backgrounds. Everyone performs the same basic routines on our computers and the Internet each day. During an average day, people use passwords, connect to the Internet on an unsecure wireless connection, share media via external devices, surf the web, click on hyperlinks, share information via social networking, and much, much more. Each of these actions involves a potential risk and can result in malicious consequences, many of which the average non-technical user is unaware (Jacobson and Idziorek, 2012).

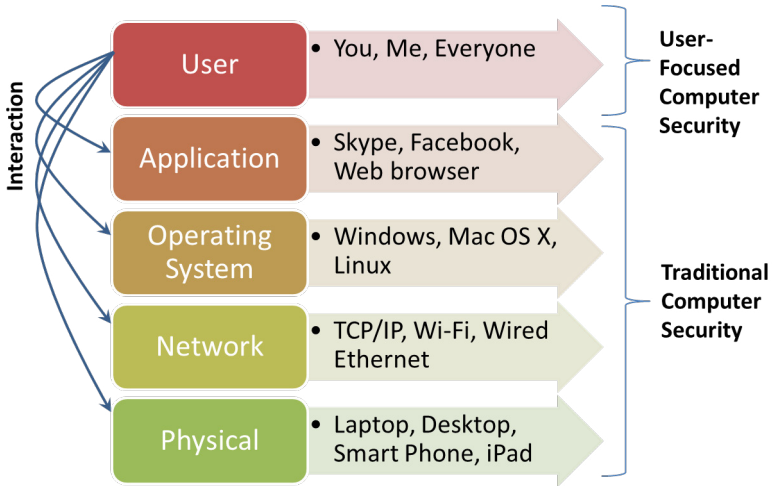

Fig. 5.
Need for User-Focused Computer Security at Airports in the BYOD Era

In developing manuals and multi-media materials for educating airport employees and users in potential cyber vulnerabilities and cyber security best practices, the following key principles of information assurance must be pondered over (Jacobson and Idziorek, 2012):

- *Security is a matter of economics:* When deciding what information to protect and how to protect it, the first question that should be asked is, Is it worth it? In other words, security costs time and money, and if the information or object that is being protected has little value, it does not make much sense to spend resources to protect it.

- *Security should be composed of layers of defenses:* There is no one single security mechanism that can protect all information from potential attacks. A layered approach will make it more difficult for someone to gain access to your information since an intruder must bypass multiple security methods to gain access. If one layer fails, there are additional layers in place to compensate and prevent a breach of security.

- *Absolute security does not exist:* We cannot protect against every possible event, especially when we cannot predict every potential security threat. No security system can be perfect in dealing with either the physical or the computer world. By employing a defense-in-depth strategy, one can greatly improve the overall security of computing devices and the protection of digital information.

- *Security is at odds with convenience:* In the physical world, security often involves extra steps or procedures to protect a valued object. The more security mechanisms (e.x., passwords) added to a computer system, the more intrusive security measures might be, often causing user frustration. While added measures provide enhanced security,

they are also at odds with convenience and over time convenience tends to trump security.

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-in-depth 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 (2013), 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.

5. 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-to-end 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 belt-and-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.

References

ACI-NA. 2011. ACI-NA Business Information Technology Committee Participation Plan. Airports Council International of North America. Available from Internet: <http://www.aci-na.org/sites/default/files/bit_committee_participation_2012.pdf>.

AirTight Networks. 2012. Impacts of Bring Your Own Device (BYOD) on Enterprise Security. A Survey by AirTight Networks, Inc. Available from Internet: <http://www.airtightnetworks.com/fileadmin/pdf/AirTight-BYOD-Survey-April-2012.pdf>.

Cook, C. 2010. *Heathrow Terminal 5: An IT Infrastructure success story*. Airports International Magazine, Key Publishing Ltd.

Cheong, B. 2011. Cyber security at airports. Airports Council International of North America. Available from Internet: <http://aci-na.org/sites/default/files/cheong-cybersecurity-bit.pdf>.

Duggan, D.P. 2005. SAND2005-2846P: Penetration Testing of Industrial Control Systems. Technical report, Sandia National Laboratories.

Fortinet. 2012. Top 10 Network Security Threats. Fortinet, Inc. Available from Internet: <http://www.fortinet.com/>.

GAO. 2009. Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls. GAO-09-399. Report to Congressional Requesters, US Government Accountability Office (GAO), Washington, D.C. Available from Internet: <http://www.gao.gov/new.items/d09399.pdf>.

Hahn, A.; Kregel, B.; Govindarasu, M.; Fitzpatrick, J.; Adnan, R.; Sridhar, S.; Higdon, M. 2010. Development of the PowerCyber SCADA security testbed. 2010. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, CSIIRW '10.

Infosecurity. 2008. Cyber security lacking at airports. Available from Internet: <http://www.infosecurity-magazine.com/view/1206/cyber-security-lacking-at-airports-/>.

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

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

Jacobson, D.; Idziorek, J. 2012. *Computer Security Literacy: Staying Safe in a Digital World*. Chapman & Hall/CRC Press, First Edition, Boca Raton, USA.

Kaiser, L. 2012. 2013-2023 Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy. U.S. Department of Homeland Security. Available from Internet: <http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf>.

McAllister, B. 2011. How to be Cyber Secure. Aviationpros. Cygnus Business Media. Available from Internet: <http://www.aviationpros.com/article/10522704/cyber-security-for-airports>.

Nessi, D. 2013. Knowing Your Virtual Vulnerabilities. Aviationpros. Cygnus Business Media. Available from Internet: <http://www.aviationpros.com/article/10898119/know-your-virtual-vulnerabilities>.

Parks, R.C. 2007. SAND2007-7328: Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment. Technical report, Sandia National Laboratories.

Permann, M.R.; Rohde, K. 2005. Cyber Assessment Methods for SCADA Security. Technical report, The Instrumentation, Systems and Automation Society (ISA).

Rencher, R.; Whitlock, S.; Francy, F. 2012. Securing Airline Information on the Ground and in the Air. The Boeing Company, Aero Quarterly, QTR_03. 25-28.

TSWG. 2012. Roadmap to Secure Control Systems in the Transportation Sector. Version 3.0, Prepared by the The Roadmap to Secure Control Systems in the Transportation Sector Working Group. Available from Internet: <http://www.us-cert.gov/control_systems/pdf/TransportationRoadmap083112.pdf>.

Williams, J.H.; Signore, T.L. 2011. National Airspace System Security Cyber Architecture. Case #10-4169, Approved for Public Release by the FAA. Available from Internet: <http://www.mitre.org/work/tech_papers/2011/10_4169/10_4169.pdf>.