Enterprise Network for Cyber Physical Systems (CPS): A Casestudy of SCADA Threats in Airports*

*Learner Centered Learning (LCL) Project Mid-Review, written for the course EE-424, offered at Habib University, 75300

Ahsan Ali*, Abeera Farooq Alam†
Karachi, Pakistan
Email: *aa05201@st.habib.edu.pk, †aa05420@st.habib.edu.pk

***Abstract*—Cyber Physical systems are one of the most significant advances in the development of computer science, information and communication technologies. These systems employ computer-based algorithms that interact with the physical world and its on going processes. CPS provide and use, data accessing and data processing services available on the internet at the same time. At the center of the 4th industrial revolution are these cyber physical systems which can help transform the way humans and computers interact with the world around them. Industries can be made almost completely automated with humans only having to oversee the operations carried out by CPS. This paper explores the application of CPS networking SCADA systems in airports and evaluates the potential improvements that can be made for increased security to decrease the vulnerability of the system.**

***Index Terms*—CPS, SCADA, TCP, DHCP, DNS, PXE, cyber security, enterprise network, modern aviation,**

I. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are critical infrastructure responsible for maintaining electrical power systems, water, gas, networking and other utilities in transportation systems such as in airport. They provide physical isolation and technical uniqueness against cyber-attacks by playing crucial role in enterprise and corporate networks management and maintenance. SCADA systems are now being integrated into information technology systems network using TCP/IP technologies to improve the security and privacy parameters of these crucial systems [8].

The design and implementation of an enterprise communication network for SCADA systems of infrastructures such as of airport requires extensive investigation of parameters for security, quality and reliability. Various utilities are employed to construct a highly secure network for airport which includes crucial operations ranging from flight timing control, airplanes coordination, passenger services, internet accessibility, automated apparatus etc.

The potential utilities for such a network would include hardware firewalls, IP access control, MAC address port security, domain servers, proxy servers, failover firewall utility, Pre-boot Execution Environment (PXE) server, Dynamic Host Configuration Protocol (DHCP) server, Domain Name System (DNS) and cabled connections. These utilities are configured to provide a secure and reliable environment for various parties such as Management Authority, Flight Service Provider and Guests to intercommunicate and prevents compromising of sensitive information such as flight management and service providers data to potential attackers.

The aim of this paper is to construct a potential paradigm of communication network for an airport that will facilitate majorly three groups namely Airport Authority, Flight Service Providers (FSP's) and Guest Members through assignment of appropriate network privileges and functionality to perform relevant and specified tasks. It will also survey and analyze appropriate yet scaled-down measures of cybersecurity for cabled connections, virtual LANs, subnetting, firewall and isolation to furnish the security of the network against data breaches and threats [10].

Section II of this paper would overview the Cyber Physical Systems framework followed by its security and privacy parameters and taxonomy in section III. It will then explore integration and role of SCADA in CPS followed by its context in Airport in section V. The paper then surveys the modern Airports networking paradigm and potentiality of threats in it in section VI and VII respectively. In the end, a simulation framework is provided which provides a potential deployment framework for networking security at airports in section VIII.

II. Enterprise CPS Network Framework

A cyber-physical system is usually a closed-loop system of networked sensors and actuators, where data collected by sensors are communicated to embedded systems (controllers) that adjust the system's operation through the actuators as shown in Fig 1 for a typical transportation network [11]. Today, examples of cyber-physical systems include computerized and networked medical equipment, manned and unmanned vehicles, home automation systems, intelligent traffic management systems, industrial control systems, among others. An airport is an example of a SCADA based cyber-physical system, where information must be available accurately and in a timely fashion. Passengers must know when a flight is scheduled to arrive or depart, and the airport administration must provide flight service providers (FSP's) database access and facilitate information exchange between them and passengers. These time critical operations are realized with a highly secure, qualified and reliable communication network infrastructure.

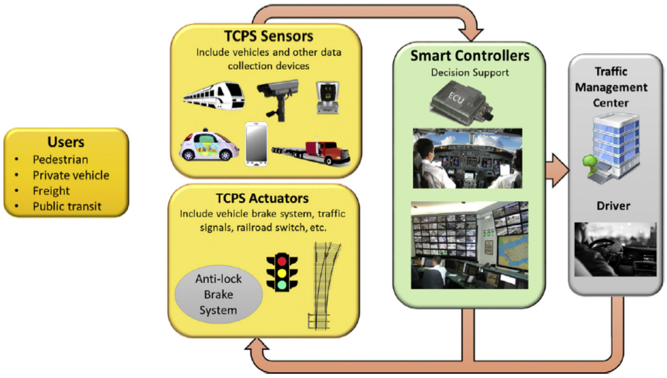

Users
Pedestrian
Private vehicle
Freight
Public transit
TCPS Sensors
Include vehicles and other data collection devices
TCPS Actuators
Include vehicle brake system, traffic signals, railroad switch, etc.
Anti-lock Brake System
Smart Controllers
Decision Support
ECU
Traffic Management Center
Driver

Fig. 1. A conceptual overview of Transportation Cyber-Physical System (TCPS)

III. CPS Network Privacy Taxonomy

With rapid growth of CPS, the capability of conventional cyber-attacks and cross-domains attacks penetrating SCADA systems is ever great. The most common among these attacks is the Stuxnet attack which reportedly damaged over 1000 centrifuges at an Iranian Uranium Enrichment Plant [12]. Stuxnet infects targeted system, manipulating the cyber-space and physically damages the industrial infrastructure. These attacks can be extended to modern car electronics, remotely controlled UAV via GPS spoofing, attacks infecting maintenance computer. These attacks are usually based on two main factors: Interconnection of all devices and usage of common solutions including OS and Networking protocols. Additionally we have DoS and DDos attacks that are more threatening to real-time operating systems (RTOS) since even a minor disruptionn in these systems can lead to significant damage of system functionality in real-time applications.
These attacks are further classified by multi-dimensional characterization, attack description and identification which gives rise to various attack groups such as traffic analysis, active eavesdropping, unauthorised access, man-in-the-middle, session hijacking and replay attacks. Other categorization of these attacks are based on attack vectors (attack route methodology), attack targets, exploited vulnerabilities, additional payload effects and layer specific attacks as shown in Fig 2 [5].

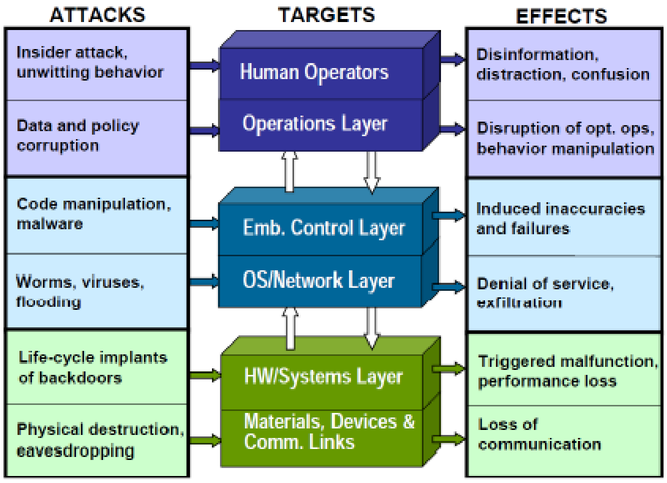

ATTACKS
TARGETS
EFFECTS
Insider attack, unwitting behavior
Data and policy corruption
Code manipulation, malware
Worms, viruses, flooding
Life-cycle implants of backdoors
Physical destruction, eavesdropping
Human Operators
Operations Layer
Emb. Control Layer
OS/Network Layer
HW/Systems Layer
Materials, Devices & Comm. Links
Disinformation, distraction, confusion
Disruption of opt. ops, behavior manipulation
Induced inaccuracies and failures
Denial of service, exfiltration
Triggered malfunction, performance loss
Loss of communication

Fig. 2. Layer specific attacks on CPS

IV. CPS and SCADA Systems

Cyber Physical Systems (CPS) act as a bridge between the physical environment and the virtual world via a group of coordinated sensors and actuators that are being controlled by an intelligent decision control systems. Remote activities of CPS systems are monitored and controlled by specialized computing systems called industrial control systems (ICSs) or supervisory control and data acquisition (SCADA) systems. A SCADA system is a purely software package that is positioned on top of hardware to which it is interfaced, in general via Programmable Logic Controllers (PLCs), or other commercial hardware modules [1]. To prevent any cyber attack from occurring and affecting the system and associated functions, that may include national safety, illegal disclosure of proprietary information, economy and/or human life, these systems must be designed and implemented following the most practical security practices as defined by well-known standards.

V. SCADA Systems in Airports

Digital-based SCADA airport investment will grow by 40% in 2020 with the objective to improve operations and capacity, and to provide a better customer experience [7]. Airports are working towards digitalization, launching dedicated apps (like Changi, Incheon, Schiphol, Heathrow, Frankfurt, Munich, Zurich or Copenhagen Airport) and covering key areas where digitization has the greatest impact: operations, security, passengers and retail. Thus, digitization has become a different way to do business, generating more than $300 billion profit. This digitization model of airports typically looks like one in Fig 3 [7].

The following levels of airport digitalization mirror the objectives regarding operational efficiency and passenger experience enhancement [7].

- **Airport operations.** The efficiency of overall airport operations aims to optimize resources and improve processes related to maintenance, handling operations, security services, thus eliminating delays or other operational risks.
- **Passenger journey.** Targets to improve passenger perception and experience by handling congestion, ensuring a continuous flow, thus minimizing queues and maximizing passenger's time spent in retail areas.
- **Ancillary revenues**. Non-aviation revenues can be increased by amending retail area attractiveness, provide commercial information through mobile apps or digital walls and use digital capabilities to perform online orders.

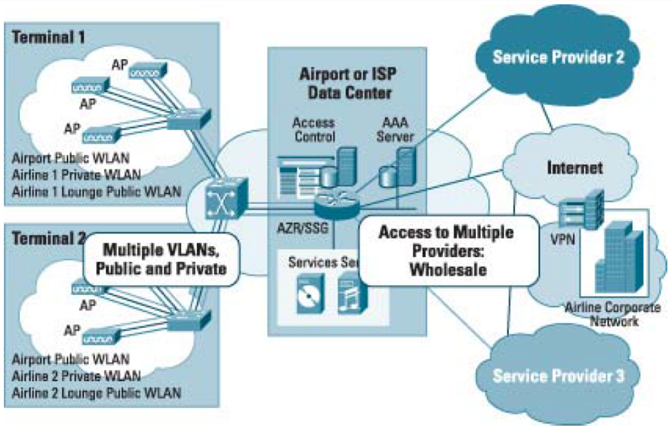


Fig. 3. Airport Networking Infrastructure

VI. Cyber Security in Modern Aviation

Developing technologies are giving rise to whole new arena of cyber-attacks and the need for robust privacy and security systems are ever great. For example, according to Chief IT Officer of Los Angeles airport, there were 6400 reported attempts to hack into file server after 2 days it was employed; and about 59,000 internet misuse cases and abuse attempts were reportedly block; and over one year period, about 2.9 million hacking attempts were blocked [8]. Most of these vulnerabilities lie in poor and partial configuration of Wireless Access Point (WAP), Network Access Points (NAP), unsecured SQL databases, poorly optimized and configured firewalls, interconnected peer networks with compromised security and several others.

In case of airports, most common cyber attacks takes place in form of Speak-Phishing emails containing malware packages like Sykipot that when is running target machine will establish an SSL connection to command and control server, where more malicious files are then downloaded and installed in victim's computer. Information of airport network layout, flight timings, routes, passengers' details and airport facilities are compromised. According to one of the studies [8], 77 percent of Airtight networks were non-hotspot out of which 80 percent were unsecured or using legacy WEP encryption, fatally flawed protocol.

VII. SCADA Network and Cyber Security Threats in Airports

In a general SCADA Network, the three main security concerns are Policy Management, Data Integrity and Weak Communication. If an intruder is able to access the data, the intruder can control the entire system. The threat magnifies if the system is connected to the internet. Even if an attack doesn't make the data accessible to the threat, the attack can make a service unavailable. This can be done in numerous ways such as DoS or DDos. The purpose of such attacks is to overload the computer resources so that it is not able to perform the required services. The communications link of SCADA are also vulnerable to attacks due to the absence of encryption and authentication mechanisms.

These vulnerabilities can be addressed by having intrusion detection systems, and updated firewall to keep the system under constant supervision and carrying out regular risk assessments and improving security plans and their implementations. Another challenge would to be enable secure access control, this can be done by improving authentication passwords and smart cards to reduce of risk of an attacker guessing the system's credentials.

An attacker targeting the ICS/SCADA systems are not in one trial but through a bulkiness of efforts and methods to gather the most applicable and adequate information to create a great negative cause [2]. If an attacker has no harm objective, they might just be satisfied with using DoS (Denial of Service). However, if they wish to manipulate operational processes to harm the structure, equipment, data and human, then a systematically huge attacking method will be used.

In an Airport SCADA Network, there are multiple channels through which a threat can be posed. By allowing employees and guests to use their own devices, an airport system becomes more vulnerable to malicious software attacks. Research experiments have shown that any malicious passenger or employee, equipped with a smart device infected with malware, may be able to access the aircraft's system and even influence system's integrity [3]. Infected user devices give malicious attackers an opportunity to hack into the system. One such incident happened in September 2016, at Vienna Airport, where employees computers and servers were infected with malware. Similarly, on June 22, 2015, an attack limited clean carrier grounded all flights, adversely affecting about 1400 travellers [6].

VIII. Simulation Framework for Airport SCADA Network

Operationally, critical threat, asset, and vulnerability assessment (OCTAVE) level of risk and planning defenses against cyber attacks is determined by a security framework. Framework organizations are likely to help reduce the risk of threats to determine the likely outcome of an attack is successful and defines a method for dealing with attacks. In OCTAVE, people within the organization get leverage, and so, the experience and expertise is built. The first step that they pose is to build threats based on risk profiles. The process to conduct a risk assessment, relevant to the organization, goes on [9]. There are three steps to OCTAVE; Asset-based risk profiles, Identify infrastructure vulnerabilities and develop security strategy and plans. One security problem that can be identified from this risk assessment process and that which has already been mentioned above within classification of cyber-attacks on SCADA systems in CPS is Service Forswearing, also known as Denial of Service (DoS). DoS is is an extremely effective attack which hinders or suspends the Internet-related administration of a host. Avionics infrastructure are extremely susceptible to DoS and DDoS attacks [4].

In our proposed solution, if a DoS attack is identified, the targeted data is diverted to the back-end SPI OACI for treatment after which only filtered legitimate data is allowed to flow to maintain system continuity. Fig 4 and Fig 5 gives the flow of this proposed solution for identification and treatment of DDoS attack for a network comprising three main entities namely Guests, Airport Security and Authority, Flight Service Providers with their own distinct networks. In case of DDoS attack, we will analyze and filter out illegitimate flows from traffic and will forward the legitimate traffic to servers. Currently, the scenario is proposed to be implemented in CISCO Packet Tracer but additional tools might be used to incorporate real scenario of the DDoS attack [13].

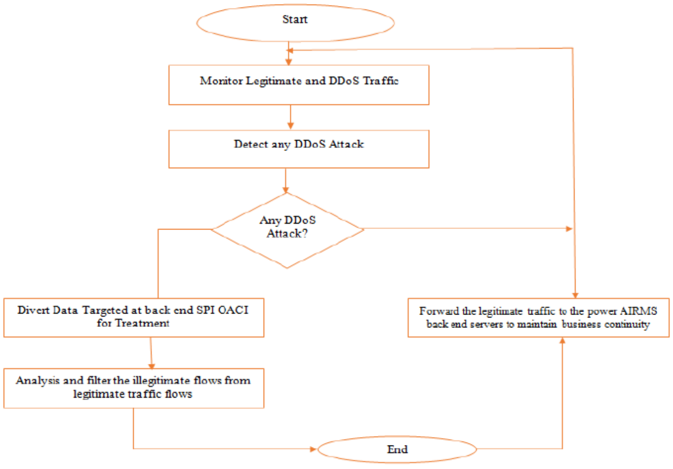

Start
Monitor Legitimate and DDoS Traffic
Detect any DDoS Attack
Any DDoS Attack?
Divert Data Targeted at back end SPI OACI for Treatment
Forward the legitimate traffic to the power AIRMS back end servers to maintain business continuity
Analysis and filter the illegitimate flows from legitimate traffic flows
End

Fig. 4. Flow Diagram of Proposed Solution

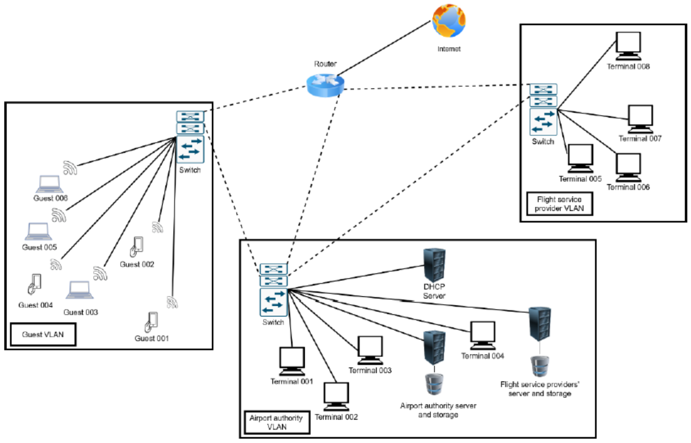


Fig. 5. Proposed Solution Topology

IX. Airport Enterprise Network Simulation on Packet Tracer

Figure 6 shows the topology of the Cisco® Packet Tracer (PT) of an airport network design. This design is adapted from [14] which models an enterprise network, and the design of the topology is validated from [15] as depicted in Figure 7. Major access restriction is done by the access-list control feature in PT. There are three virtual local area networks (VLAN's), namely Guest, Flight control (FC) and Airport authority (AA). Access is controlled such that:

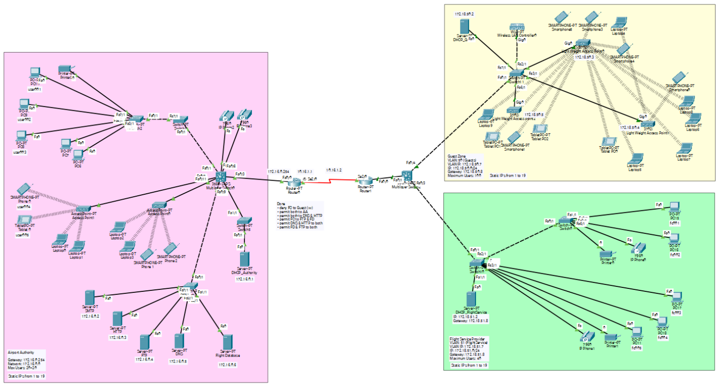


Fig. 6. Airport Enterprise Network Topology

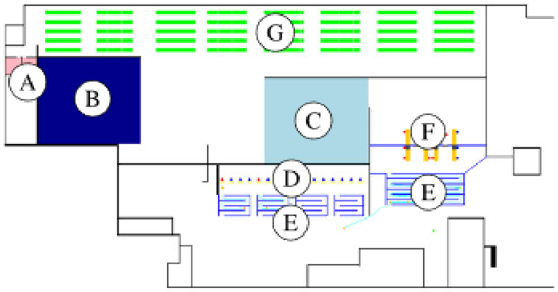


Fig. 7. The airport layout of the case study, with indicators for different areas. A, B, and C are facility areas. D is the check-in area and E is the queuing area. F is the checkpoint area and G is the gate area. The airport authority area in our simulation models the facilities area and flight control area, while the guests area models the checkpoint, queue and gate area [16].

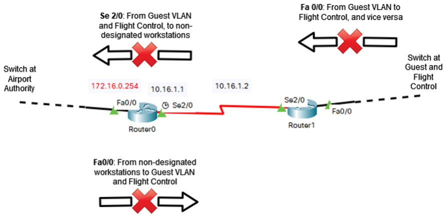
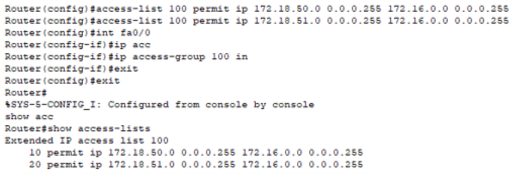
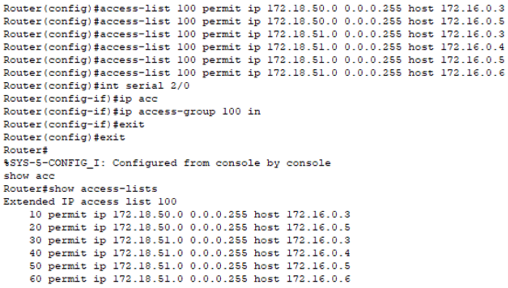

Se 2/0: From Guest VLAN and Flight Control, to non-designated workstations
Fa 0/0: From Guest VLAN to Flight Control, and vice versa
Switch at Airport Authority
172.16.0.254
10.16.1.1
10.16.1.2
Switch at Guest and Flight Control
Fa0/0
Se2/0
Router0
Se2/0
Fa0/0
Router1
Fa0/0: From non-designated workstations to Guest VLAN and Flight Control

Fig. 8. The access-list implementation on the routers in the simulated network (see Figure 6). The specific interface of the routers where the access-list is implemented are also specified.



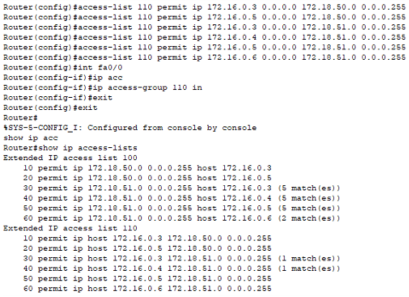
```
Router(config)#access-list 100 permit ip 172.18.50.0 0.0.0.255 172.16.0.0 0.0.0.255
Router(config)#access-list 100 permit ip 172.18.51.0 0.0.0.255 172.16.0.0 0.0.0.255
Router(config)#int fa0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show acc
Router#show access-lists
Extended IP access list 100
    10 permit ip 172.18.50.0 0.0.0.255 172.16.0.0 0.0.0.255
    20 permit ip 172.18.51.0 0.0.0.255 172.16.0.0 0.0.0.255
```

Fig. 9. The access-list coding on Router1.



```
Router(config)#access-list 100 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.3
Router(config)#access-list 100 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.5
Router(config)#access-list 100 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.3
Router(config)#access-list 100 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.4
Router(config)#access-list 100 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.5
Router(config)#access-list 100 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.6
Router(config)#int serial 2/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show acc
Router#show access-lists
Extended IP access list 100
    10 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.3
    20 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.5
    30 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.3
    40 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.4
    50 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.5
    60 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.6
```

Fig. 10. The access-list coding on Se2/0 port of Router0.



```
Router(config)#access-list 110 permit ip 172.16.0.3 0.0.0.0 172.18.50.0 0.0.0.255
Router(config)#access-list 110 permit ip 172.16.0.5 0.0.0.0 172.18.50.0 0.0.0.255
Router(config)#access-list 110 permit ip 172.16.0.3 0.0.0.0 172.18.51.0 0.0.0.255
Router(config)#access-list 110 permit ip 172.16.0.4 0.0.0.0 172.18.51.0 0.0.0.255
Router(config)#access-list 110 permit ip 172.16.0.5 0.0.0.0 172.18.51.0 0.0.0.255
Router(config)#access-list 110 permit ip 172.16.0.6 0.0.0.0 172.18.51.0 0.0.0.255
Router(config)#int fa0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip acc
Router#show ip access-lists
Extended IP access list 100
    10 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.3
    20 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.5
    30 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.3 (5 match(es))
    40 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.4 (5 match(es))
    50 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.5 (5 match(es))
    60 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.6 (2 match(es))
Extended IP access list 110
    10 permit ip host 172.16.0.3 172.18.50.0 0.0.0.255
    20 permit ip host 172.16.0.5 172.18.50.0 0.0.0.255
    30 permit ip host 172.16.0.3 172.18.51.0 0.0.0.255 (1 match(es))
    40 permit ip host 172.16.0.4 172.18.51.0 0.0.0.255 (1 match(es))
    50 permit ip host 172.16.0.5 172.18.51.0 0.0.0.255
    60 permit ip host 172.16.0.6 172.18.51.0 0.0.0.255
```

Fig. 11. The access-list coding on the Fa0/0 port of Router0.

1) Guest cannot access any terminal in FC and vice versa.
2) Both Guest and FC cannot access any terminal in AA except the DNS server and HTTP server. Additionally, FC can only also access FTP server and Flight database server.
3) AA terminals cannot access any terminals in FC or Guest VLAN, except for the servers listed prior.

Figure 8 shows the main access control implemented, and Figures 9 through 13 show the access list coded onto the routers using the command-line interface in PT. Further security features are implementable in PT, such as wide area network (WAN) emulation with firewall protection and NAT implementation (using Cisco® Adaptive Security Appliances (ASA's)), to demonstrate an attack from an outside agent; NAT is especially useful when we want communication to occur on specific ports [17].

In an airport, it is not only individual devices that need to be protected but all devices within the airport need to be secured to prevent threats like malware attacks and such. According to Chadwick's study in (2001) firewalls have some advantages: They can stop incoming requests to inherently insecure services, e.g. you can disallow login, or RPC services such as NFS. They can control access to other services e.g.Bar callers from certain IP addresses, filter the service operations (both incoming and outgoing), e.g. stop FTP writes hide information e.g. by only allowing access to certain directories or systems. They are more cost-effective than securing each host on the corporate network since there is often only one or a few firewall systems to concentrate on. They are more secure than securing each host due to: The complexity of the software on the host - this makes it easier for security loopholes to appear. In contrast, firewalls usually have simplified operating systems and don't run complex application software, the number of hosts that need to be secured (the security of the whole is only as strong as the weakest link). [18] Devices inside the airport network are can be accessed through any website from the Internet since the outside security level hasn't been set up and is therefore 0. High security level can be established to prevent outside activities from entering the local network. The airport network system will be made inaccessible to hackers and untrusted devices through this configuration. Each port can then be assigned to specific inside VLAN port which has security level set to 100 and outside VLAN ports with security level set to 0.

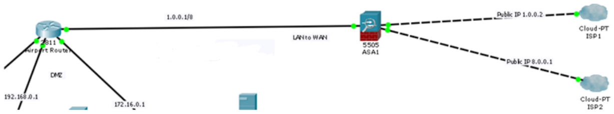
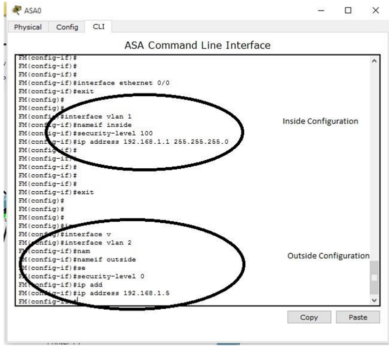


Fig. 12. Including firewall in our topology to filter out traffic



```
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#interface ethernet 0/0
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#interface vlan 1
FM(config-if)#nameif inside
FM(config-if)#security-level 100
FM(config-if)#ip address 192.168.1.1 255.255.255.0
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#
FM(config)#i
FM(config)#interface v
FM(config)#interface vlan 2
FM(config-if)#nam
FM(config-if)#nameif outside
FM(config-if)#se
FM(config-if)#security-level 0
FM(config-if)#ip add
FM(config-if)#ip address 192.168.1.5
FM(config-if)#
```

Fig. 13. Configuring Firewall to secure internal network

X. Conclusion

With the increasing use of CPS infrastructure in controlled systems, the need for proper security becomes crucial. In this paper, we have discussed a framework that can be implemented for risk assessment of cyber systems and more particularly an airport network system and a simulation framework is provided. Risk assessment process is essential for an organization to determine the assets that are more vulnerable to attacks and to help define the necessary protocols to overcome those risks. Any critical system that can be potentially harmed is identified within this risk assessment.

References

[1] A. Daniels and W. Salter, ”What is SCADA?”, 1999. [Accessed 5 November 2021].

[2] S. ALI, CYBER SECURITY FOR CYBER PHYSICAL SYSTEMS. [S.l.]: SPRINGER, 2019, pp. 89-97.

[3] G. Lykou, A. Anagnostopoulou and D. Gritzalis, ”Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls”, Sensors, vol. 19, no. 1, p. 19, 2018. Available: 10.3390/s19010019 [Accessed 5 November 2021].

[4] F. N. Ugwoke, K. C. Okafor and V. C. Chijindu, ”Security QoS profiling against cyber terrorism in airport network systems,” 2015 International Conference on Cyberspace (CYBER-Abuja), 2015, pp. 241-251, doi: 10.1109/CYBER-Abuja.2015.7360516.

[5] Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, and Janos Sztipanovits. 2013. Taxonomy for description of cross-domain attacks on CPS. In Proceedings of the 2nd ACM international conference on High confidence networked systems (HiCoNS ’13). Association for Computing Machinery, New York, NY, USA, 135–142. DOI:https://doi.org/10.1145/2461446.2461465

[6] Kreutz, Diego, Oleksandr Malichevskyy, Eduardo Feitosa, Hugo Cunha, Rodrigo da Rosa Righi, and Douglas DJ de Macedo. ”A cyber-resilient architecture for critical security services.” Journal of Network and Computer Applications 63 (2016): 173-189.

[7] S. E. Zaharia and C. V. Pietreanu, “Challenges in airport digital transformation,” Transportation Research Procedia, vol. 35, pp. 90–99, 2018.

[8] J. McCarthy and W. Mahoney, “SCADA threats in the modern airport,” International Journal of Cyber Warfare and Terrorism (IJCWT), vol. 3, no. 4, pp. 32–39, 2013.

[9] Alberts, C. J., Behrens, S. G., Pethia, R. D., &Wilson, W. R. (1999). Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework (Vol. 1).

[10] Ali, A., 2021. Enterprise Network Design and Implementation for Airports. [online] ValpoScholar. Available at: ¡https://scholar.valpo.edu/msittheses/2/¿ [Accessed 7 December 2021].

[11] Lipika Deka, Sakib M. Khan, Mashrur Chowdhury, Nick Ayres, Transportation Cyber-Physical System and its importance for future mobility, Elsevier, 2018, Pages 1-20, ISBN 9780128142950, https://doi.org/10.1016/B978-0-12-814295-0.00001-0.

[12] Loukas, G. (2015). Cyber-physical attacks: A growing invisible threat. https://www.worldcat.org/title/cyber-physical-attacks-a-growing-invisible-threat/oclc/910102749

[13] Okafor, K.C., Okoye, J.A., & Ononiwu, G. (2016). Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective. International Journal of Computer Applications, 138, 18-30.

[14] A. H. Ali, “Enterprise network design and implementation for airports,” Valpo.edu, 27-Apr-2016. [Online]. Available: https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1001&context=ms_ittheses. [Accessed: 08-Dec-2021].

[15] imsiddhant, “Computer-Networking-Project-1.” [Online]. Available: urlhttps://github.com/imsiddhant/Computer-Networking-Project-1. [Accessed: 08-Dec-2021].

[16] S. Janssen, A. Sharpanskykh, and R. Curran, “AbSRiM: An Agent-Based Security Risk Management Approach for Airport Operations,” Risk Analysis, vol. 39, 02 2019.

[17] danscourses, “Configuring NAT basics for the CCNA with Packet Tracer,” Danscourses.com, 30-Apr-2017. [Online]. Available: urlhttp://danscourses.com/configure-nat-basics-ccna-packet-tracer/. [Accessed: 08-Dec-2021].

[18] Chadwick, D. W. (2001). ”Network Firewall Technologies.” NATO SCIENCE SERIES SUB SERIES III COMPUTER AND SYSTEMS SCIENCES, 178, 149-168.

XI. Acknowledgements

The work was partially contributed by Muhammad Abeer Sohail in addition to the above two mentioned authors, primarily in light of research conducted for SCADA systems, specifically employed in Airports.