**Unit 4 Seminar – Threat Modelling Exercise**

**Introduction**

This threat modelling exercise enumerates the threats associated with a large international airport based in the United States of America. The threat model adopted in this exercise is an attack tree. Shostack (2014) enunciates that the attack trees main goal is the root note, while the different ways to achieving the goal are the leaf nodes.

The US Federal Aviation Administration (FAA) has admitted that the nation’s air-traffic control systems are vulnerable to cyberattack following a top-level probe into systems security (Turner, 2009). Florido-Benitex has argued that airports are a nation’s critical infrastructure, as any attack/breach will have devastating impact on businesses and individuals alike.

**Attack Tree**

Goal: Hijack an Aircraft

1. Take control of cockpit
2. Sneak into cockpit and coerce pilot to obey directives
3. Have an experienced pilot among the hijack crew
4. Bribe a pilot for his service
5. Scare pilot with weapons explosives
6. Releasing biological attacks to disarm pilot.
7. Contaminate food or water supply
8. Overpower crew and passengers
9. Scare them with weapons and explosives
10. Abduct passengers
11. Restrain their movement
12. Disable security systems
13. Manually disable the systems
14. Remotely disable the systems
15. Bribe an airport official to disable them
16. Releasing biological attacks to crew, passengers and other security personnel on board
17. Contaminate food or water supply
18. Bribe a kitchen staff
19. Sneak into kitchen to contaminate the food
20. Breach into the network to hijack food/water order – to route order to a malicious vendor.
21. Carry weapons onto aircraft
22. Bypass security checkpoint
23. Scale over checkpoint
24. Bribe security personnel
25. Corrupt detection device so as not to detect weapons or explosives
26. Use a stolen gate pass
27. Bribe airport official
28. Sneak the bomb into passengers luggage
29. Use drones to deliver weapons to aircraft
30. Cyber Attack
31. Insert multiple ghost aircraft transmitting emergency beacons on an air traffic control screen (ATC)
32. Bribe a staff to do this
33. A hijacker luckily walks into the control room to corrupt the system
34. A hijacker sneaks into the control room to hijack the system
35. Attack airline server
36. Easy access to server room
37. Remotely attack server, and IDS
38. Attack airline technology providers and sub-contractors
39. Breach passenger data systems
40. Compromise baggage handling
41. Use drones to carry payload
42. Infiltrate restricted areas
43. Sneak in through the door
44. Faulty doors
45. No presence of security
46. Just being lucky for the doors to be open
47. Bypass security checkpoints
48. Scale over checkpoint
49. Bribe security personnel
50. Corrupt detection device so as not to detect weapons or explosives
51. Use a stolen gate pass
52. Have a member hijack crew as a passenger
53. Book flight as a normal passenger
54. Attack airport database and inject data of hijacker into database
55. Walk up to the airport and board the plane being lucky
56. Scaling perimeter fences
57. Tailgating vehicles or staff through gates
58. Make friends with a staff member
59. Bribe an official
60. Stealthily use gate pass of a staff without their knowledge
61. Exploiting blind spots (areas not monitored properly)

**Conclusion**

The airport would need to ensure adequate and regular threat assessments to forestall any breaches. Incidents need prompt reporting, and law enforcement personnel need to stay alert to ward off attacks.

**Reference**  
Florido-Benítez, L., 2024. Identifying and classifying cyberattacks on airports. Cyber Security: A Peer-Reviewed Journal, 8(1), pp.63-79.

Shostack, Adam. *Threat Modeling : Designing for Security*. 1st edition. Indianapolis, IN: John Wiley and Sons, 2014. Print.

Turner, A. (2009), ‘FAA admits to air travel cyberattack’, FlightGlobal, available at https://www.flightglobal.com/faa-admits-to-air-travel-cyber-attack-threat/86299.article [Accessed 27th June 2023].