CASE STUDY

SMART AIRPORTS

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

PROJECT SNAPSHOT

In the future, smart devices connected to the internet will enable airline passengers to move seamlessly through Australian airports. The CSCRC is researching ways to make air travel more secure, by creating an intelligent risk evaluation tool that automatically detects and neutralises vulnerabilities in Internet of Things (IoT) devices.

WHO'S INVOLVED

This project is funded by the CSCRC in partnership with TCS and AFP, with research carried out by the University of New South Wales (UNSW Canberra).

WHAT'S THE ISSUE?

In modern airports, artificial Intelligence (AI) and IoT create huge benefits related to optimisation, efficiency, productivity, and automation. Likewise, smart devices allow us to access services faster, for example, via self-check-in, e-gates and automated bag drops. But while they are designed to make our lives easier, these technologies can potentially leave us open to danger. Airport CCTV systems, thermal cameras and body scanners, complimentary Wi-Fi and smart restrooms are all potential targets for cyber criminals. Cyber attacks can disrupt airport operations, causing significant financial loss, reputational damage and risk to life. Hence, shielding airports from cyber threats is now more important than ever to safeguard the economy and the community. Our researchers have discovered potential improvements to existing defence mechanisms allowing airports to better secure and maintain their smart systems and devices. The intelligent risk evaluation tool will help overcome weaknesses and enable a through-live cyber protection approach for IoT.

WHAT WERE THE OBJECTIVES?

- Examine cyber risks for airline passengers while transiting through airports
- Design a digital twin-based cyber testbed for examining physical and network vulnerabilities
- Determine solutions to reduce cyber threats and safeguard smart airports
- Develop a fully functional and automated vulnerability and mitigation tool to improve cyber defences

TECHNOLOGY DESCRIPTION

The project develops an intelligent risk evaluation tool and digital twin-based cyber testbed, capable of analysing network and IoT telemetry data to detect vulnerabilities an attacker can exploit to gain unauthorised access to a smart airport's internal networks. Such attacks could result in privacy breaches, data exfiltration and denial-of-service attacks. The project's novelty comes from developing new approaches that will automate the process of discovering attack surfaces and their attack vectors. Smart environments are large-scale data sources, as they constantly generate network and sensing data, which can potentially leave them more open and vulnerable to cyber attacks. Additionally, design flaws and resource limitations inherent in IoT networks put the stability of business processes at risk, which is why additional support is needed to avoid and protect against new threats.

APPLICATION

The project is currently at a Technology Readiness Level of between 3 and 5. The digital twin-based cyber testbed for smart airports has been designed and a proof of concept with a deep learning-based vulnerability detection model has also been established. Through experimentation using the digital twins' testbed, its prototype components are being tested.

The digital twins' testbed will be used for evaluating cyber risks of combat systems for a research project sponsored by the Defence Science and Technology Group (DSTG).

Researchers are receiving regular feedback from the Australian Federal Police (AFP) and Tata Consulting Services (TCS) on the progress of the project. The aim is to involve law enforcement at a national and international level in the application of this technology.