Network Manager
nominated by
the European Commission

EUROCONTROL

Invited Briefing Note

Five Defensive Measures to Improve the Cyber Security of European Air Traffic Management

by Prof. Chris Johnson, Glasgow University

The Assets

The last decade has seen a growing pace of interconnection across the aviation industry. We have seen a huge shift in the ways that people search for and book flights. At the same time, airlines depend upon increasing volumes of engineering and operational data exchanged over wired and wireless networks. Airport Operations Centres (APOCs) coordinate dispatchers, baggage handlers, customs and border staff, parking and even retail activities through digital infrastructures. Air traffic management (ATM) has served increasing traffic levels and delivered unparalleled levels of safety through corporate and enterprise Information Technology (IT) and the Operational Technology (OT) of CNS services. Both SESAR and NextGen reinforce these trends and offer new concepts of operation for ATM that can only be realised through tightly integrated digital networks.

The Threats

In the past, many aviation networks were isolated, preventing data or code from migrating between them and wider public networks. This provided a degree of protection that has gradually been eroded by the need, for instance, to use ATM data to trigger the APOC functions that service in-bound aircraft. Even when OT components, such as primary surveillance, are isolated there are ways to reach them (for example, through memory devices that carry data between the Internet and private ATM networks during software up-dates).

These developments expose ATM networks to a wide range of cyber threats. The Stuxnet/Olympic Games attacks on Iranian nuclear enrichment facilities have shown how to undermine operational technology even in networks that are isolated from the Internet. Recent attacks on Ukrainian infrastructures show that attackers can use network interfaces to transfer malware from enterprise information systems to safety-related operational networks.

We have only been able to meet the costs associated with digital innovation by maximising the use of mass market 'Commercial off the Shelf' (COTS) components – including the Linux operating system and the Internet Protocol (IP). An increasing number of people possess the necessary technical skills to launch successful attacks on ATM infrastructures – as a consequence of our increasing reliance on mass-market software systems.

The introduction of digital networks into ATM has often been in response to ad hoc operational demands. Consequently, many companies struggle to maintain clearly defined software architectures, sustaining a complex web of new and legacy applications. With finite internal engineering resources, it is hard for many ANSPs to understand every detail of the engineering that supports CNS infrastructures. Intellectual property barriers further complicate the defence against cyber attacks. In many European service providers, it is impossible to be sure if a process was inserted by an attacker or by a legitimate sub-contractor; the supply chain is not monitored and is a significant weak link.

Finally, the development of novel attack methods has (at least) matched the pace of digital innovation across the aviation industry. Commercial marketplaces have developed where relatively untrained adversaries can buy malware that is guaranteed to work against patched and unpatched systems. Command and control servers can be used to update that malware once it has infected a machine – in the same way that legitimate applications can be updated to fix security vulnerabilities. We have also seen great creativity in the use of social engineering attacks. An example is the use of personal information on social media accounts to tailor infected email attachments that will almost inevitably be opened by the recipient, no matter how much cyber security training they have received.

The Need for Coordination

We are running out of time. Given our reliance on digital integration through COTS software it is inevitable that systems will be attacked. Today most ANSPs lack adequate defences and recovery mechanisms.

The cyber security of critical infrastructures remains the responsibility of individual national governments. However, we need individual countries to work together across Europe. Operational aviation data are routinely exchanged without encryption or the ability to rapidly authenticate who sent the messages. Attackers can inject well-formed packets of information to misdirect ATM operations. No single country will benefit unless everyone replaces these systems. *All operational data in European ATM should be encrypted and authenticated by default within the next five years.*

As a parent and a passenger, I am acutely aware of the immediate need to fill the leadership vacuum in European aviation cyber security. We need leadership to ensure that existing network interfaces are defended and that investments by one country are not undermined by weaknesses in our neighbours. We also need leadership to ensure that our plans for future integration, operability and optimisation do not introduce new levels of vulnerability.

Five Defences to Improve European Cyber Security

In the long term, it is likely that we will have to increase the expenditure allocated to cyber defence in ATM networks. In the meantime, there are five measures for ANSPs to improve cyber security.

1. Ensure Competency

Ensure that you have a Chief Information Security Officer (CISO) who is competent for the task and who has the backing of their high level management. Within every ANSP there must be an individual who leads the technical, organisational and human defences against cyber threats. It is no longer justified to expect an expert in physical defence to have the technical expertise to also protect the digital foundations of critical national infrastructures. It is essential to encourage government to ensure minimum levels of competency for NSA staff in cyber security.

2. Maintain a Cyber Risk Assessment

It is important that we justify any resources that are allocated to cyber security. Investments have to be proportionate to the threat. In order to do this, we need to develop risk assessments. Several recent initiatives provide complicated, elaborate and expensive techniques for cyber risk assessment. In most cases, they waste resources that should be used to pay for defensive measures. It is important that any cyber risk assessment is updated at least every 6 months. Threats change with the discovery of new attack techniques and with changes in the political environment. Use low cost, simple and repeatable risk assessment techniques, know your key assets and get independent experts to validate them. If the worst happens you can use these risk assessments to justify the measures that protected your infrastructures.

3. Control the Supply Chain

Once you introduce defences identified in a risk assessment, suppliers can still undermine your cyber security. Ensure they follow a documented cyber security policy by enforcing appropriate contractual agreements – make this a requirement of all future procurement. The exact requirements should be proportionate to the access they have to your digital infrastructures. For companies that have direct physical access to your digital infrastructures, an appropriate policy is to scan all devices and media that enter your premises or are connected to your networks.

4. Exercise Cyber Resilience

Nobody can guarantee that they are totally secure against all cyber threats, especially the growing number of attacks coordinated by state agencies. Cyber risk assessments help identify potential attack scenarios. These can be used to exercise your ability to recover from a potential incident. Governments across Europe already support Computer Emergency Response Teams (CERTs). They can provide essential support for the technical recovery from an attack but know nothing about ATM operations. Conversely, NSAs in most ECAC states have very little expertise in cyber security yet they have a strong role to play in determining when it is acceptably safe to resume operations after any potential attack. It is important to work with these organisations before an incident takes place. Exercises should ideally be repeated annually to increase the resilience of both IT and OT infrastructures.

5. Act Now

Acknowledgement

I would like to thank Steven Shorock and Tony Licu (EUROCONTROL) as well as Denis Koehl (EASA) for encouraging and improving this briefing note. All errors and omissions remain my own.

Biography

Chris Johnson is Professor and Head of Computing at the University of Glasgow. His work focuses on the intersection between cyber security and safety-critical systems, particularly in the aviation and civil nuclear domains. He has held two fellowships from NASA and two fellowships from the US Air Force working with Langley AFB and Space Command. He is working with the US Navy/FAA (2015-) on network monitoring for safety and security and in 2017 worked on cyber incident response for the UK Department for Transport covering all aviation sectors. He helped write the business continuity case for LVNL (2015) and worked with Aeroports de Paris/Helios (2016) on the cyber-security of Airport Operations Centres. Johnson worked with the US government Pacific North Western Labs under contract to the United Nations supporting the cyber security of Chemical, Biological, Radiological and Nuclear facilities around the globe and helps lead forensic capability for the UK civil nuclear industry. He has some 300 peer reviewed publications.

This briefing note follows Prof. Chris Johnson's talk on cyber security at the EUROCONTROL CEO Safety Conference, hosted by DFS in Frankfurt, Germany, 10-11 May 2017.

Contact - EUROCONTROL
Tony Licu
antonio.licu@eurocontrol.int

Contact - Glasgow University
Prof. Chris Johnson
http://www.dcs.gla.ac.uk/~johnson