CHALLENGES OF SECURITY AND TRUST OF MOBILE DEVICES AS DIGITAL AVIONICS COMPONENT

Raja Naeem Akram, Konstantinos Markantonakis, Royal Holloway, University of London. Egham, UK

Abstract

Mobile devices are becoming part of modern digital avionics. Mobile devices can be applied to a range of scenarios, from Electronic Flight Bags to maintenance platforms, in order to manage and configure flight information, configure avionics networks or to perform maintenance tasks (including offloading flight logs). It can be argued that recent developments show an increased use of personal mobile devices playing an integral part in the digital avionics industry. In this paper, we look into different proposals for integrating mobile devices with various avionics networks – either as part of the Bring Your Own Device (BYOD) or Corporate Owned Personally Enabled (COPE) paradigms. Furthermore, we will evaluate the security and trust challenges presented by these devices in their respective domains. This analysis will also include the issues related to the communication between the mobile device and aircraft network either via wired or wireless channels. Finally, the paper puts forward a set of guidelines with regards to the security and trust issues that might be crucial when enabling mobile devices to be part of aircraft networks.

Introduction

In the aviation industry, there is a growing proliferation of mobile devices, including tablets, smart phones and portable computers. These devices are increasingly not only used by the passengers but also aircraft crew like pilots and maintenance staff. For example, a pilot can create a flight plan on his or her personal tablet (Electronic Flight Bag) and then upload it to the aircraft [1]. In this scenario, either the aircraft manufacturer or airline provides the pilot with the necessary software application to perform this task [2].

In addition to mobile devices being used by the on-board aircraft crew, it is also used off-board where it connects with the aircraft. Such connection might be for maintenance purposes – downloading or uploading necessary data.

Any form of mobile devices, whether used by on-board or off-board crew has to interface with the aircraft. Either using a wired or a wireless interface. These interface present their own unique set of security and operational issues.

It is projected that such devices might bring operational benefits to pilots, on-board crewmembers and maintenance crew. At the same time, it is documented that use of such technologies might increase automation bias, complacency, aircrew distraction and potential software errors [3]. Beside the listed concerns, these devices potentially create additional security and reliability issues. Depending upon the mobile device, there is a potential that a compromised mobile device might give a malicious entity a route to aircraft's on-board computers — and depending upon the function of these devices the malicious entity can cause the damage.

Another complication is who owns the mobile device, and this ownership might restrict of what an aviation organisation (airline, or aircraft manufacturer) can enforce. It is challenging to enforce a user to follow a particular policy on a device that is basically belongs to them. This is a traditional security problem of user's or human limitation in following a policy, and due to this users are usually considered the weakest link in a security related process or framework.

In the context of this paper, we define a mobile device as an off-the-shelve portable computer device that can be used by pilots, aircraft crew, or maintenance personal. These devices can display, store, process and communicate related information – with on-aircraft systems and off-aircraft systems alike, either using a wired or wireless medium. Examples of such devices include smart phones, tablets and

potentially laptop computers.

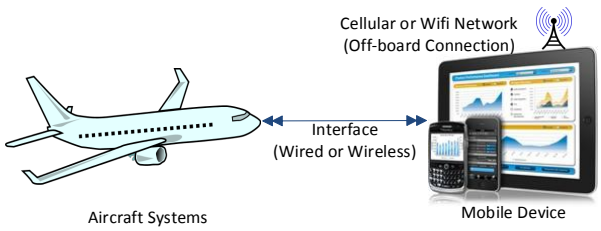

Figure 1. Mobile Device Connectivity with Aircraft Systems

Figure 1 illustrate mobile devices potentially connected to aircraft systems either by a wired or wireless connection, while some of the mobile devices might also have either cellular or Wi-Fi capability to connect to off-aircraft systems (i.e. airline network, aircraft manufacturer networks etc.). It has to be noted that in this paper we will solely focus on mobile devices and not the "installed devices" such as the Class 3 Electronic Flight Bags (EFB) defined in Federal Aviation Administration (FAA) Advisory 120-76 [4].

In this paper, we discuss different operational frameworks for incorporating mobile devices into on-board digital avionics, how these mobile devices can interface with the aircraft system(s), what security and reliability issues each of these schemes might present and finally how to resolve the security issues along with what technologies might be used to safeguard mobile devices.

Corporate Integration Mobile Device Paradigms

To major paradigms to incorporate mobile devices to either an organisational computer system or integrating mobile devices with aircraft's on-board avionics systems are COPE and BYOD. In this section, we will discuss COPE and BYOD, along with wired and wireless interface these devices can use to communicate with avionics systems. Table I provides a comparison between different integration paradigms that a corporate can deploy to bring in mobile devices. A detailed overview is provided in the following sections that explain the elements in the Table I.

Corporate Owned Personally Enabled (COPE)

In this paradigm, a corporate entity, for example, an airline, aircraft manufacturer or any other avionics related company acquires mobile devices and they customise these devices to suite their security needs [5]. After installing the management software and any other applications necessary for employees to perform their function, these devices are then given to individual employees. By acquiring the devices for employees, the corporation can make sure that only a high standard and secure device connects to their aircraft system. In addition to this, the devices allow users (employees) to also use it as they desire – by enabling them to download applications they prefer. Furthermore, as the devices are owned by the corporate entity, they can easily manage its enrolment as a secure device to connect and communicate with the aircraft systems.

Furthermore, the IT department of the corporation can keep a track of their mobile devices. If required push updates and also prohibit applications that are deemed dangerous to the secure functionality of their applications and functions. In this paradigm, corporate entity can exercise a stronger control over the mobile devices. However, at the same time employees might not get the same level of usability as they enjoy on their personal devices. Furthermore, if the mobile device were acquired off-the-shelve then the underlying platform and hardware would still be out of their control. Any loopholes in the underlying platform and hardware would require the mobile device manufacturer to fix and update. A brief explanation the Table I in the context of the COPE is as below:

- Device Ownership: As discussed before, the company acquires the devices and configure them as they desire before issuing it to their employees. The company has full control and in turn full responsibility of security in this model.
- Application Control: As the device is full control of company, they can install or delete any application they desire. Furthermore, they can also prohibit certain applications from be installed on to their device by its respective users (i.e. employee).
- Protecting Company Assets: As the IT department of the company has full control over the device, they can lock it down to have maximum

Criteria	COPE	BYOD	CYOD
Device Ownership	Company (IT Department)	Employee (User)	Company's Approved/Preconfigured Devices
Application Control	Full (IT Department)	Full (User)	Partial (IT Department and User)
Protecting Company Assets	Full (IT Department)	Partial (User)	Partial (IT Department and User)
Responsibility of Securing the Device	IT Department	User	Partial (IT Department and User)
User's Privacy Issues	Significant	Limited	Limited
Usability and Freedom of Use for Employees	Limited	Full	Limited

Table I. Comparison between COPE, BOYD and CYOD

assurance that no breach of data could be carried out on these device. Furthermore, the IT department might also be responsible for repairing the device, which helps limit the potential break carried out during the repair process by a third party.

- Responsibility of Securing the Device: IT department of the company is fully responsible for securing the device. After said that, user education regarding best practices to security might still be necessary to educate individual employees.
- Privacy Issues: Employees have no privacy protection. Any activity carried over the company device could potentially be captured by the IT department – either for operational or security reasons.
- Usability and Freedom of Use for Employees: As users access to the device would be restricted and she would not be able to install or delete applications, the freedom of use would be limited. However, usability would depend upon how the company design their services for their employees.

Keeping in mind that COPE model is closet to the traditional and much preferred by organisations model known as Corporate Owned Business Only (COBO).

Bring Your Own Device (BYOD)

In this paradigm, a user acquires a mobile device for her. The user can then approach her employer and request the company application/credentials to connect her device to the aircraft system [6]. The mobile device management system of the company that can either be an airline, aircraft manufacturer or maintenance contractors then enrol the given device to the system. The company can then also issue their application to the user and assign any associated credentials. To some extend the employer can exercise a limited control on the user's device. However, fundamentally the device belongs to the user and it is challenging to control user's activity on such devices.

Furthermore, the management of software updates to patch discovered vulnerabilities and any additional security software on such device might be at user's prerogative.

- Device Ownership: Users purchase the device and they own it.
- Application Control: Employer only has the control of their own application. Whereas, user is free to install or delete any applications they required. The employer would not be able to monitor what other applications are installed on the device.
- Protecting Company Assets: Although, IT department of the employer is responsible for protecting the company's digital assets but if some sensitive data is stored on the device (as part of the company's application). It is challenging to provide an assurance that such data might not be breached – either by the user or a malicious entity who gain access to the device.
- Responsibility of Securing the Device: The responsibility of updating the device in a timely manner and potentially have tools to protect against malicious intrusions falls under the purview of individual users (employees). This is a challenging prospect of the company to ensure that their employees take due care of their personal devices. User training and awareness of security concerns would be critical in this model but it has its limits.
- Privacy Issues: Employers can only monitor the user activity that she carries out using their applications or during access to their resources (i.e. company internet and website). Any other activities carried on the device are not monitored

thus provide a level of privacy to employees.
- Usability and Freedom of Use for Employees: User has full access to the device and she can use the device they way she deems right. As before, usability deals with the easy with which she can access her company's resources – something dependent upon company's design.

Choose Your Own Device (CYOD)

Potentially a compromise between the COPE and CYOD paradigm is referred as the CYOD. In this model, a company defines a list of preselected and pre-configured devices that are authorised to be brought into the company's network. Employees are then give the choice to buy any one of such devices and then use them to connect with the company's network [7]. As the company as preselected the device and might have pre-configured it to their security requirements, they might have more trust in the device. It can also facilitate the company to exercise some level of security management on the device, either managing the patch updates and applications that can be installed. However, all of this is dependent upon the employee-employer relationship. A user might decide agree on the company managing their own application on her mobile device but not enforcing her on what she can or cannot use the device for – as in this model the final owner is still the user because she has paid for the device.

- Device Ownership: Actual ownership of the device is with the employee as she is paid for it. However, the respective employer might exercise some privileges on such devices.
- Application Control: Employees can download applications on to their devices but the employer might have some security application installed on the device that employees cannot delete. Employee might be given free hand in installing and deleting any application they want except the ones that employer has installed.
- Protecting Company Assets: Employer has the lead role in this but employee?s assistance is necessary. Security updated and the employer can push patches to their employee's device. Employees have to use the device in a secure way that they might not become a route to breach company's data.
- Responsibility of Securing the Device: Responsibility of this lies at both the employer and employee.
- Privacy Issues: Limited privacy issues, more then BYOD but less then COPE. Company might still be able to capture the activities of the user but restrict itself to certain activities related to the security and reliability of their application.
- Usability and Freedom of Use for Employees: User has limited freedom to user the device as they desire as long as they do not try to infringe any company policies. Usability has the same level as discussed before in COPE and BYOD.

Interfacing with Aircraft Systems

The discussion of the interface is crucial as it defined the level of control and access to the aircraft systems can be designed. There are two interfacing medium, wired or wireless. In a wired medium, a mobile device connects with the aircraft system over a wired link either using a docking stations or a physical port connection. A physical access is required to such connection points, which might restrict certain attackers. Furthermore, as the communication medium is wired, gaining access to the communication traffic is challenging (if not impossible) that requires, again, a physical access to the communication wires.

Whereas, if the interface is over the wireless then a physically restricted adversary might be able to either (try) to connect to the aircraft systems or at least be able to listen to what is being communicated over the wireless channel. The security requirement of the wireless and wired interfaces is starkly different from an adversary, which do not have either access to the mobile device or physical access to the aircrafts.

However, for an adversary that compromises the mobile devices the notion of the security in terms of wired or wireless communication channel has not implications. What this adversary is restricted to or by is the on-device security mechanisms that might prevent a malicious code/entity interfering with the sensitive process/application related to the avionics ecosystem.

The objective of the discussion on the interfacing was the put the message across that for a holistic approach to the security for the mobile devices for avionics systems – interface restrictions is an important issue with pros and cons for both wireless and

wired options. However, neither of them completely isolates nor mitigates all potential security concerns.

Evaluation Case Studies

In the previous section, we discussed different deployment models for the mobile device integration with aircraft systems. In this section, we focus on three case studies where deployment of mobile devices might be relevant. In subsequent sections we will analyse how different deployment models in the context of these case studies influence the security of mobile devices.

Mobile Device as Electronic Flight Bag

An Electronic Flight Bag (EFB) is a management device that helps flight crew to perform flight management related tasks in an easy and convenient manner. According to the FAA Advisory Circular 120-76C, an EFB is an electronic display system intended primarily for cockpit/flight deck and/or cabin use [2]. In this paper we focus on Class 1 and Class 2 of EFB, as defined in the FAA Advisory [4].

A Class 1 and Class 2 EFB are off-the-shelves mobile devices that have no FAA design, production, or installation approval – as a whole device or its subcomponents. Devices in these two class can connect to the aircraft system data and the only difference between is whether the EFB is mountable or not [4].

Mobile Device as Maintenance Tool

Mobile devices that a maintenance crew has to offload the flight logs, perform diagnostics and potentially perform aircraft system configuration. Such devices might be operated either by boarding the aircraft or from ground while the aircraft is stationary on the ground. For this device, they can either connect directly with the aircraft subsystems like engine management systems or required to be connected via an aircraft central system or hub to communicate with any of its subsystems. As noted above, these devices might have the privilege to make changes to the aircraft's operating parameters/configurations. Thus making them a crucial case of mobile devices that connect with the aircraft systems.

Mobile Device as Operational Tool

These mobile devices are similar to the EFBs discussed in the previous sections. However, instead of these devices being operated in the cockpit or flight deck. The cabin crew to manage the inflight entertainment and ambience configuration uses these devices. These mobile devices might potentially replace the setting (configuration) console in the passenger cabins that the crewmembers use to control the cabin environment.

Threat Model

In previous section, we discussed three potential deployments of mobile devices as part of the digital avionics networks. These three deployment models have their own security and reliability concerns, which might be unique to each of their deployment scenarios and application/data they deal with. However, in this section we discuss two generic types of an adversary in the context of the mobile devices – as defined in this paper. Keeping in mind that this categorisation is made based on the level of access each adversary has to the mobile device and not on the basis of individual adversary's capability to compromise a given device.

On-Device Adversary

On-device adversaries are malicious users that can potentially compromise the mobile device. By doing so, depending upon the depth of compromise they can control the execution of any sensitive applications that connects with the aircraft system and communication relevant information. The closer an adversary in compromise to the hardware of the mobile device, the more powerful he or she is – with abilities to interrupt or modify the execution of and/or data communication from a sensitive application running on the device.

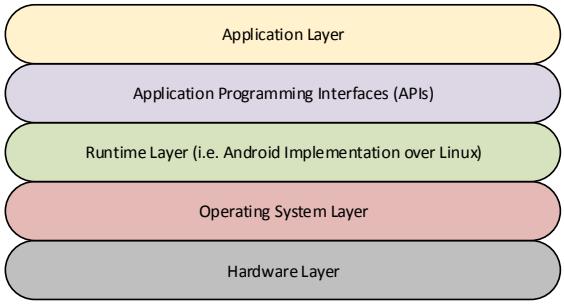

Figure 2. On-Device Adversary Target Layers

For an on-device adversary, the aim is the compromise any of the layers (semantically) represented in the Figure 2. The lower layers an adversary manages to compromise, the stronger the potential to influence an application and its data. The adversary might have compromised the device either at the manufacturing stage, by getting a physical access even for a short while or remotely by installing a malicious application on the device. Such adversary might be physically away from the compromised device but potentially still be able to control it.

Off-Device Adversary

Off-device adversaries are malicious users that have no access to the mobile devices – either physical or remote. These adversaries try to intercept the communication between a mobile device and aircraft system. Although, in the interface section we mentioned that it is comparative easy to intercept a wireless channel then a wired channel but for simplicity we assume that off device adversary has equal access to all communication medium between a mobile device and aircraft system.

Unlike the on device adversary, the off device adversary has to be near the geographic area of the mobile device to effective intercept its communication. This adversary does not need to compromise either the mobile device or the aircraft systems – they only need to have the ability to intercept the communication between the mobile device and the aircraft system.

Evaluation of Mobile Devices as Digital Avionics Component

In this section, we briefly evaluate the risk each of the mobile device case study might face from the two generic adversaries discussed in the previous section. In this section we are not evaluating any particular products that actually deploys mobile devices in the respective case studies but consider a generic high-level analysis of what security risks these deployment might face.

Mobile Device as Electronic Flight Bag

Mobile device as EFB might have strong access control and firewalls on the aircraft system side, which might prevent a non-authorised application from connecting and communicating potentially incorrect data. However, an on-device adversary can potentially control the execution of the sensitive application that is authorised to communicate with the aircraft system. Any cryptographic mechanism deployed for either authentication or encryption/signature on the data communicated from the device to the aircraft would potentially be vulnerable to the on-device adversary. Therefore, any security mechanism designed as part of the sensitive mobile application would not be effective if the adversary has access to the runtime environment or worse if have access to the hardware. It should be noted that any mechanism built on the aircraft side of this would have little to no effect in preventing an on-board adversary from interfering with the sensitive applications activity.

Off-device adversary, in theory, if have an access to the communication between the mobile device and aircraft systems they might be able to eavesdrop. An active off-device adversary might even be able to inject some data to this communications; however, if data integrity is not assured in this communication. This attack might work.

Mobile Device as Maintenance Tool

Similar to the EFBs, the mobile device as maintenance tool might have little defence against onboard adversary if any or all countermeasures implemented by the application developer are based on the applications. For instance if the mobile device adhere to BYOD; however, it should be noted that other mechanism also do not fair well against an advance adversary that has the ability to compromise the mobile device. If the aircraft configuration is generated on the mobile device and then using secure cryptographic mechanism communicated to the aircraft systems, then such an update would not be secure against on-device adversary. However, if the mobile device is just a communication conduit between the back-office system and aircraft system and all updates are secured end-to-end. In this case on-device adversary would not be able to modify the end-to-end communication channel.

Whereas, for the off-device adversary, if the communication is unencrypted or there is a vulnerability in the communication scheme then he or she might be able to potentially exploit it. However, as off-device adversary does not have the capability

to break the standard cryptographic algorithms that restricts it to what he or she can achieve.

Mobile Device as Operational Tool

Unlike the previous two cases, it can be argued that mobile devices as operational tools might pose the least amount of safety risk to the aircraft systems. As discussed in the previous sections, operational tool might deal with the in-flight entertainment and/or cabin ambience. The maximum an attacker can achieve would be modifying some parameters in such systems – if such a provision were allowed in the system. The on-device adversary, as by now realised to be a most advanced adversary can manage to interrupt the execution and potential can process any command as desired. whereas the off-board adversary can mount replay attacks, man-in-the-middle attacks and/or denial of service attack. However, replay attacks might pose the most significant danger as it might trigger certain cabin condition, which might perturb the cabin passengers.

Guidelines for a Secure and Trusted Integration

In the previous sections we discussed two categories of adversary, their capabilities and their risk potential for all three-use cases of mobile devices. The question arise is "how real is the threat of the on-board adversary?". A valid question and the potential of it being realised is not the realm of fantasy. There are examples in which devices were shipped with built-in Trojans [refs] and/or device were compromised by advance adversary after being issued to the users [ref] that have escalated privileges. As the aircraft safety is paramount and its reliability is stringently required, we consider that designing a system that is secure to such adversaries could only be the reasonable option. In this section, we list some of the security considerations that should be taken into account when deploying mobile devices to interface and communicate with aircraft systems.

Least Privilege Architecture

Each user and mobile device that connects with the aircraft system should be authenticated. The access privilege issued to the user and mobile device should be atomic. An atomic access is defined as individual users and devices have their own set of separate privileges – unique to each user and device. Only those privileges will be given to a user that the device is also permitted to have. Furthermore, each access privilege should have a clear and pre-defined time scale, after this time the user and device should re-authenticate themselves to the aircraft systems.

Certain aircraft systems should only allow access when certain environment conditions are met. For example, maintenance crew might only be allowed to access maintenance logs once the aircraft is grounded and stationary. Furthermore, a reconfiguration of a potential aircraft system is only allowed if the aircraft is grounded and in maintenance phase.

Trusted and Isolated Enrolment

Mobile devices and users have to be enrolled to relevant organisation's privilege system to gain access to aircraft systems. These organisations can be airline operator, aircraft maintainers and manufacturer. In any case, a mobile device and user enrolment should be closely monitored. There should be a robust system to vet users and potentially devices (if possible) at this stage.

Strong Function Classification

Each application issued to a user and device should have a restricted code base. Only the application code that is necessary to perform the relevant tasks should be there. Hiding functionality based on the access privilege is potentially not a preferable solution in this case.

Strong Binding with Aircraft and Operational-Environment

Each device and user account should be associated with the individual aircraft. This is to avoid and potential issue in which a user or device credentials are used to access an aircraft system when the person is no where near the aircraft or not working at the time of access. The access credentials and privilege to access an aircraft should be as unique as possible and a restricted in time and geographical location as possible. Furthermore, mobile devices (if possible) should have a strong bidding to the aircraft systems.

Hardened Firewall Mechanism

A strong firewall mechanism with in-depth packet inspection scheme should be taken into account for the mobile connectivity with the aircraft

systems. Furthermore, firewall should also be able to detect any covert channels and enforce strong information flow policies.

Strong Access Control Mechanism

Access control should be implemented on strong authentication schemes. Both user and device should be authenticated separately. User authentication is based on stronger mechanisms like biometrics (widely available on mobile devices now) and device authentication should be based on two-way challenge-response protocols.

Strong Secure and Trusted Channels

Any communication between a mobile device and the aircraft system, whether over the wired or wireless interface, should be protected using cryptographic mechanisms. For this purpose, a secure and trusted channel protocol should be deployed. In a secure and trusted channel protocol, not only the communicating entities authenticate to each other but also their internal states are also validated to be trustworthy. For validation of the software (and potential hardware) state of the aircraft application on the mobile device a trusted platform architecture could be deployed – discussed in subsequent sections. This will not only ensure that the communication channel is protected and devices are authenticated but also that the status of applications on the devices are also secure (and free of any malicious alterations). For an in-depth analysis and security recommendations for how to design a secure channel for digital avionics systems, please refer to [8].

Data Integrity, Traceability, and Validation

Any data loaded or off-loaded from an aircraft should provide a strong integrity, traceability and validation properties. A strong integrity mechanism provides an assurance that data is not be modified by any non-authorised entity during its storage and transit. For integrity mechanism, cryptographic primitives like hash functions and digital signatures can be deployed. Data traceability provides a mechanism in which data can be traced from its creation to destruction. Such a mechanism is necessary for data quality and forensics purposes. Data validation is a mechanism in which certain element of data is created in a way or certain errors are left in the data in a manner that a trusted entity can verify the origin of data. This mechanism can ascertain whether a data presented to the aircraft or data from an aircraft to airline/maintenance back office can be validated to be generated by the entity to which it is attributed.

Trusted Platform

There are many proposals that push forward the trusted platform architectures. In this section we will discuss three of these:

Trusted Platform Module: The definition of trust, taken from Merriam Webster's online dictionary[1] states that trust is a "belief that someone or something is reliable, good, honest, effective, etc."

The TPM specifications are maintained and developed by an international standards group called the Trusted Computing Group (TCG)[2] Today, TCG not only publishes the TPM specifications but also the Mobile Trusted Module (MTM), Trusted Multi-tenant Infrastructure, and Trusted Network Connect (TNC). With emerging technologies, service architectures, and computing platforms, TCG is adapting to the challenges presented by them.

The TPM chip, whose specification is defined by the Trusted Computing Group **TCG** is known as hardware root-of-trust into the trusted computing ecosystem. Currently it is deployed to laptops, PCs, and mobiles and is produced by manufacturers including Infineon, Atmel and Broadcom. At present, the TPM is available as a tamper-resistant security chip that is physically bounded to the computer's motherboard and controlled by software running on the system using well-defined commands. The TPM MOBILE with Trusted Execution Environment has recently emerged; its origin lies in the TPM v1.2 a with some enhancements for mobile devices [9] . The TPM provides:

1) The Roots of trust include hardware/software components that are intrinsically trusted to establish a chain of trust that ensures only trusted

[1]Website: http://www.merriam-webster.com/dictionary/trust

[2]Trusted Computing Group (TCG) is the culmination of industrial efforts that included the Trusted Computing Platform Association (TCPA), Microsoft's Palladium, later called Next Generation Computing Base (NGSCB), and Intel's LaGrande. All of them proposed how to ascertain trust in a device's state in a distributed environment. These efforts were combined in the TCG specification that resulted in the proposal of TPM.

software and hardware can be used (see the Mobile Trusted Module (MTM) section).

2) The Platform Configuration Register "PCR" in the most modern TPM includes 24 registers. It is used to store the state of system measurements. These measurements are represented normally by a cryptographic hash computed from the hash values (SHA-1) of components (applications) running on the platform. PCRs cannot be written directly; a process called extending the PCR can only store data.
3) The RSA keys: There are two types of RSA keys that TPM generates and which are considered as root keys (they never leave the TPM):
    a) Endorsement Key (EK): This key is used in its role as a Root of Trust for Reporting. During the installation of an owner in the TPM, the manufacturer generates this key with a public/private key pair built into the hardware. The public component of the EK is certified by an appropriate CA, which assigns the EK to a particular TPM. Thus, each individual TPM has a unique platform EK. For the private component of the EK, the TPM can sign assertions about the trusted computer's state. A remote computer can verify that those assertions have been signed by a trusted TPM.
    b) Storage Root Key (SRK): This key is used to protect other keys and data via encryption.
    c) Attestation Identity Keys (AIKs): The AIK is used to identify the platform in transactions such as platform authentication and platform attestation. Because of the uniqueness of the EK, the AIK is used in remote attestation by a particular application. The private key is non-migratable and protected by the TPM and the public key is encrypted by a storage root key (or other key) outside the TPM with the possibility to be loaded into the TPM. The security of the public key is bootstrapped from the TPM's EK. The AIK is generally used for several roles: signing/reporting user data; storage (encrypting data and other keys); and binding (decrypting data, used also for remote parties).

Trusted Execution Environment: A Trusted Execution Environment (TEE) provides necessary assurance that during the execution of an application, no on board application can interfere with its execution. Two of the main proposals for the TEE are ARM TrustZone and GlobalPlatofrom TEE – although in recent years these two proposals are converging but in this section we have briefly discussed them separately. The ARM TrustZone also provides the architecture for a trusted platform specifically for mobile devices. The underlying concept is the provision of two virtual processors with hardware-level segregation and access control [10], [11]. This enables the ARM TrustZone to define two execution environments described as Secure world and Normal world. The Secure world executes the security- and privacy-sensitive components of applications and normal execution takes place in the Normal world. The ARM processor manages the switch between the two worlds. The ARM TrustZone is implemented as a security extension to the ARM processors (e.g. ARM1176JZ(F)-S, Cortes-A8, and Cortex-A9 MPCore) [11], which a developer can opt to utilise if required.

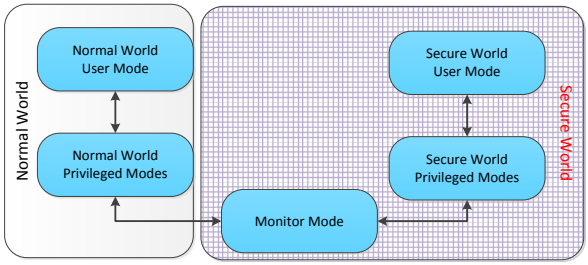

Figure 3. Generic architectural view of ARM TrustZone

The TEE is GlobalPlatform's initiative [12]–[14] for mobile phones, set-top boxes, utility meters, and payphones. GlobalPlatform defines a specification for interoperable secure hardware, which is based on GlobalPlatform's experience in the smart card industry. It does not define any particular hardware, which can be based on either a typical secure element or any of the previously discussed tamper-resistant devices. The rationale for discussing the TEE as one of the candidate devices is to provide a complete picture. The underlying ownership of the TEE device still predominantly resides with the issuing authority,

which is similar to GlobalPlatform's specification for the smart card industry [15].

Encrypted Execution: An application is executed in a manner that all of the application instructions on persistent and non-persistent storage are in encrypted format [16]. The application is executed on processes that decrypt the application n execution cycle before the instruction is going to be executed – n has to be as small as possible to provide efficient performance. Such a solution considers that an adversary has control over the software and hardware of a device except for the internal circuitry of a processor, which is considered to be trusted. This proposal realise on the security and trust on the utmost basic element of computing – a processor. If we consider that an adversary has a compromised processor then it is difficult to hide application execution from it.

Secure and Trusted Supply Chain for Mobile Applications

Provisioning of the application to users mobile device should be closed managed and monitored. The applications that could have the capability to be connected to an aircraft should only be available for the mobile device on a restricted supply chain. Meaning, such an application should not be accessible on general-purpose application distribution channels.

Secure Decommissioning

At the end of the lifecycle of the mobile device or presence of an application on such a device, the application and device should be properly decommissioned. Recycling should be carried out in a manner that all security related parameters are completely removed and the device itself is put on as black list maintained by the airline or maintenance organisation.

Conclusion

In this paper, we looked into the provisioning of connecting mobile devices in different operational capacity with the aircraft systems. It can be argued that mobile devices have the potential to provide benefits; however, in this paper we looked into the security implication of such an operational situation.

In this paper, we described three different mobile device integration models – COPE, BYOD, and CYOD. We have also provided a comparison between these three models based on security control and responsibilities. With these integration models an important aspect how a device can interface with an aircraft, which is either via a wired or wireless interface. In this paper, we have considered three deployed case scenarios and potential threat model is presented. We have divided an adversary into two categories – on-board and off-board adversary. It is apparent that on-board adversary has more capabilities to cause harm then the off-board adversary, but this is by no way means that when designing such an integration, we can ignore the off-board adversary.

We have then briefly evaluated the case scenarios based on the adversary's capabilities. Based on this analysis we have presented a minimum set of guidelines to be followed when mobile devices are considered to be integrated with an aircraft system.

Acknowledgements

The authors acknowledge the support of the UK's innovation agency, InnovateUK, and the contributions of the Secure High-Availability Avionics Wireless Networks (SHAWN) project partners.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the position of SHAWN project or any of organisations associated with this project.

References

[1] J. Freeman, "A warm reception for iPad EFB in Alaska", *Aircraft IT Operations*, vol. v1.6, pp. 16–19, 2012.

[2] M. J. Carrico, "Mobile device integration in the cockpit: Benefits, challenges, and recommendations", in *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*, 2015, 3B3–1–3B3–11. DOI: 10.1109/DASC.2015.7311393.

[3] N. Johnstone. (2013). The electronic flight bag fried or foe? English. Report Nr 104, Air Safety Group.

[4] "Guidelines for the certification, airworthiness, and operational use of electronic flight bags", Federal Aviation Administration, USA, Advisory Circular AC No. 120-76C, 2014.

[5] R. Walters, "Bringing it out of the shadows", *Network Security*, vol. 2013, no. 4, pp. 5–11, 2013.

[6] R. Ballagas, M. Rohs, J. G. Sheridan, and J. Borchers, "Byod: Bring your own device", in *Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp*, vol. 2004, 2004.
[7] A. M. French, C. Guo, and J. Shim, "Current status, issues, and future of bring your own device (byod)", *Communications of the Association for Information Systems*, vol. 35, no. 10, pp. 191–197, 2014.
[8] R. N. Akram, K. Markantonakis, S. Kariyawasam, S. Ayub, A. Seeam, and R. Atkinson, "Challenges of security and trust in avionics wireless networks", in *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*, IEEE, 2015, 4B1–1.
[9] "Trusted platform module main specification", Trusted Computing Group, Tech. Rep., 2011.
[10] F. A. M. T. K. D. A. T. Wilson P., "Implementing embedded security on dual-virtual-cpu systems", in *IEEE Design and Test of Computers*, 2007, pp. 582–591.
[11] , "Arm security technology: building a secure system using trustzone technology", ARM, White Paper PRD29-GENC-009492C, 2009.
[12] , "Globalplatform device: gpd/stip specification overview", GlobalPlatform, Specification Version 2.3, 2007.
[13] *Globalplatform device technology: device application security management - concepts and description document specification*, English, Online, Specification, GlobalPlatform, 2008.
[14] "Globalplatform device technology: tee system architecture", GlobalPlatform, Specification Version 0.4, 2011.
[15] *GlobalPlatform: GlobalPlatform Card Specification, Version 2.2,* GlobalPlatform, 2006.
[16] R. P. Lee, K. Markantonakis, and R. N. Akram, "Binding hardware and software to prevent firmware modification and device counterfeiting", in *Proceedings of the 2nd ACM Workshop on Cyber-Physical System Security, CPSS 2016, Xi'an, China, May 30, 2016*, J. Zhou and J. Lopez, Eds., 2016.

2016 Integrated Communications Navigation and Surveillance (ICNS) Conference
April 19-21, 201