

Imaginary Aircraft Cabin Data Network (Toy Example)



Devices in our Aircraft

CC The Cabin Core Server, a server that controls essential aircraft features, such as air conditioning and the wireless and wired telecommunication of the crew.

C1, C2 Two mobile devices for the crew to help them identifying passenger calls or make announcements.

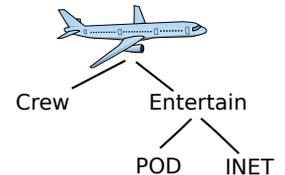
IFEsrv The In-Flight Entertainment server with movies, etc.

IFE1, IFE2 Two In-Flight entertainment displays, mounted at the back of passenger seats. Movies and internet access. Slim devices, everything is streamed from the IFE server.

Wifi A wifi hotspot that allows passengers to access the Internet with their own devices.

Sat A satellite uplink to the Internet.

P1, P2 Two passenger owned devices, e.g. laptops, smartphones.



Security Requirements

Requirement One

In our aircraft, we have 4 different security domains. Higher domains can send to all lower domains, lower domains must not send to higher domains. Different domains on the same level must not send to each other (they are separate).

- **Crew Domain**

A separate domain, very high security level. The mobile crew devices are in this domain. The cabin core server is also in there; however it is a special trusted device that may send to other domains (domain-spanning).

Use cases: Stewards coordinate food distribution; Announcement from the crew is send to In-Flight Entertainment system.

- **Entertain Domain**

A separate domain, same level as Crew Domain. The In-Flight Entertainment displays and the IFE server are in this domain.

The Entertain Domain has several sub-domains of lower security levels:

- **POD Domain**

All passenger owned devices are in this domain. In addition, the wifi access is in this domain. It has (limited) trust, i.e. it is allowed to send into the Entertain Domain but not higher.

Use case: Passenger subscribes a film from the IFE server to her notebook.

- **INET Domain**

The Satellite uplink is the only member of this domain.

Requirement Two

In our aircraft, we have some confidentiality requirements. The complete crew communication, including the cabin core server has the highest confidentiality level. This data must not leak to untrusted places. To protect the passenger's privacy when using the pre-installed devices, the IFE devices also have a confidentiality level, lower than the crew devices. The IFE server has a special role: It can declassify information (i.e. reveal to others).

Use Case: Announcement is send from a crew device and forwarded to the IFE displays via the IFE server.

Requirement Three

In our aircraft, the IFE displays are slim devices and strictly bound to their server.

Example: No peer to peer among the IFE displays; they are not directly reachable from 'the outside'.

Your Task: Design the network

Create a network topology. Put in as many flows as possible, do not violate the security requirements. Use a *directed* graph: Different meanings of 'directed' are allowed per edge. E.g., only send this direction, only establish connections (like a stateful packet filter), ...