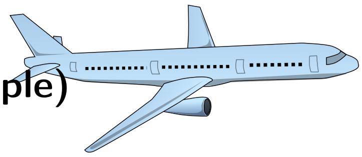
Imaginary Aircraft Cabin Data Network (Toy Example)



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.

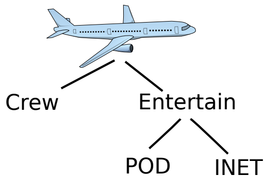
IFEsrv The In-Flight Entertainment server with movies, etc.

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), ...

Name (optional):
Job (optional):

What's your experience?

[ ] Novice some networking course (at university)
[ ] Intermediate have managed large system and network
[ ] Expert many years of experience as network and system administrator

Rate the complexity of the exercise.

[ ] very simple
[ ] simple
[ ] simple, but time consuming
[ ] medium
[ ] medium, but tricky
[ ] hard
[ ] impossible to get right

[Present Tool]

How helpful do you judge our tool?

[ ] counter-productive
[ ] more counter-productive than helpful
[ ] neutral
[ ] helpful
[ ] extremely helpful

How helpful do you consider the overall idea/process of our tool?
// forget about the ugly (no) user interface we have at the moment

[ ] counter-productive
[ ] more counter-productive than helpful
[ ] neutral
[ ] helpful
[ ] extremely helpful

Do you think our idea might help to manage large networks over a long period with lots of responsible persons?

[ ] no
[ ] don't know
[ ] yes

For tasks similar to this test, would you want to use our tool (when it's finished or a competing tool that has the same idea)?

[ ] no
[ ] yes

Author: Cornelius Diekmann

The author would like to thank Michael Schlatt for his advice and help designing this study.

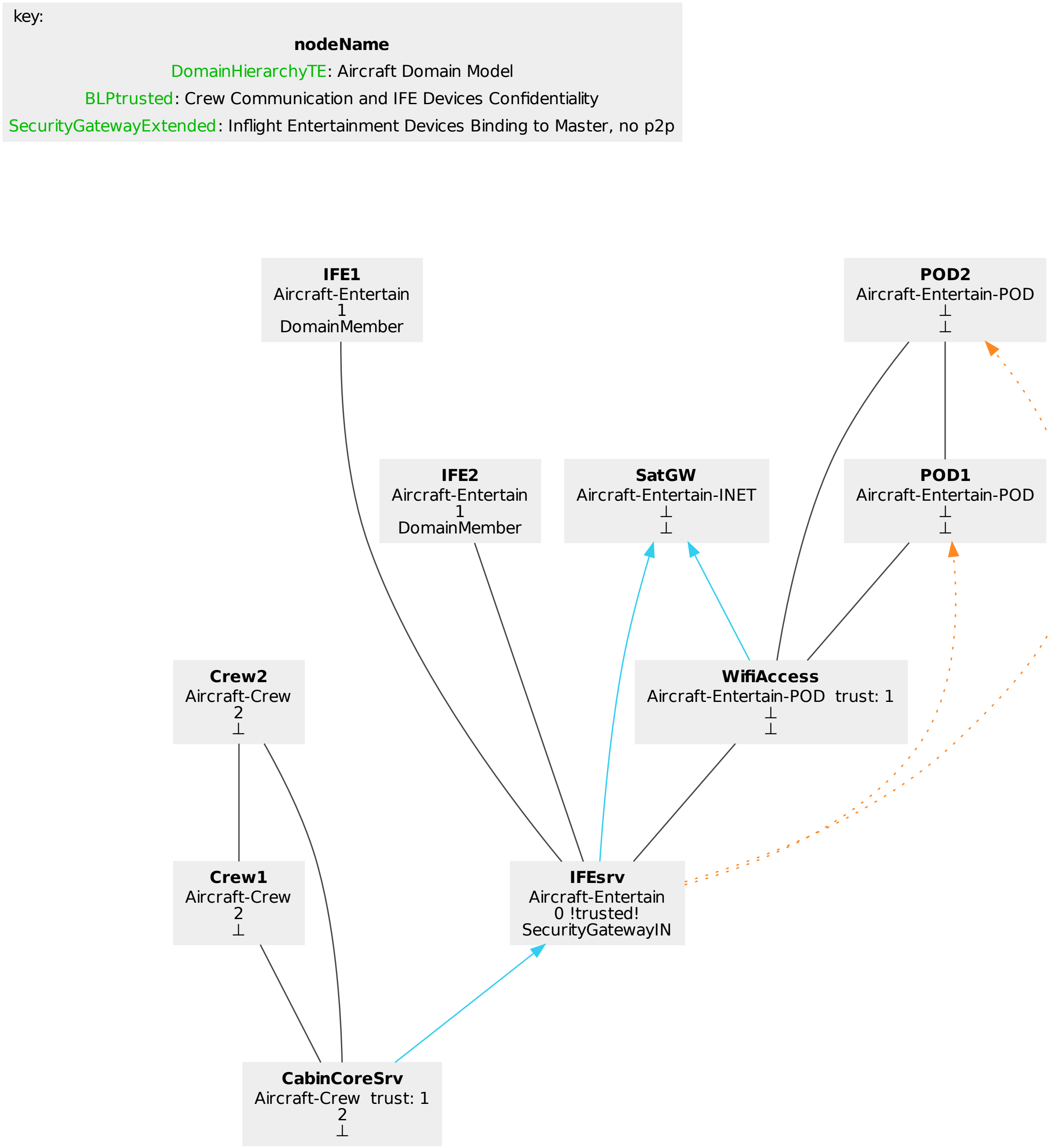


Figure 1: The solution. Unmodified output of our tool.

Results of User Feedback Session

We conducted a user feedback session with 15 IT network professionals. The participants were asked to design the Imaginary Aircraft Cabin Data Network. It was emphasized that no security requirement must be violated but the participants should try to put the maximum number of flows in the network to fulfill as much as possible of use cases. After presenting the participants their results, we presented our tool. The participants were asked to fulfill the questionnaire. The results are summarized in Table 1 and 2.

The network solution, illustrated in Figure 1, consists of 23 valid directed flows, including the two dotted edges. Bidirectional flows (black lines without arrow) count as two. In the participants' solutions, we count the invalid flows, i.e. flows that violate a security requirement; and the missing flows, i.e. flows that were forgotten in the solution. We define the error count as the number of invalid plus the number of missing flows. It is scored such that the dotted flows could be used to gain additional valid flows but never increase the invalid, missing, or error count.

The overall feedback was that our tool is downright helpful (3.0/3.3/0.8). We also introduced the idea

Experience	Participants	Complexity	Valid	Invalid	Missing	Errors
Expert	5	medium but tricky	16.0/15.8/1.7	1.0/3.2/4.4	5.0/5.6/2.1	9.0/8.8/3.8
Intermediate	5	medium	14.0/14.0/1.4	1.0/1.6/1.9	7.0/7.4/1.0	8.0/9.0/2.6
Novice	5	medium	12.0/10.6/5.7	4.0/6.6/4.9	11.0/11.2/6.2	17.0/17.8/9.1
Total	15	medium but tricky	15.0/13.5/4.1	2.0/3.8/4.5	7.0/8.1/4.5	9.0/11.9/7.2

Legend: median/arithmetic mean/std deviation

Table 1: Results of user field study with IT network professionals.

Experience	utility tool	utility idea	acceptance idea	acceptance tool
Expert	3.0/3.4/0.5	3.0/3.2/0.7	100%	100%
Intermediate	3.0/3.2/0.4	4.0/4.0/0.0	100%	100%
Novice	4.0/3.2/1.2	4.0/3.2/1.2	80%	100%
Total	3.0/3.3/0.8	4.0/3.5/0.9	93%	100%

Utility measure: 0) counter-productive, 1) more counter-productive than helpful, 2) neutral, 3) helpful, 4) extremely helpful

Table 2: Results of user field study with IT network professionals.

behind our tool and admitted, that the user interface of our prototype can be vastly increased. We asked the participants to judge the idea behind our tool. An experienced participant raised concern that special training for novice administrators is necessary. However, the overall judgment about the idea was very positive and it was considered remarkably helpful (4.0/3.5/0.9). In addition, 93% of the participants consider that our idea might help to manage large networks over a long period with many responsible persons. The positive feedback and recurring question we received during the user field study about where, when, and how expensive to obtain our tool was very motivating. Our tool's graphical feedback was also very appreciated. Finally, 100% of the participants would want to use our tool[1] for similar tasks.

The raw evaluation data of the study is listed below. Generated on 2013-08-13.

```
evaluating study for experience level [All]
number of entries: 15
What's your experience?
  median: 1.0 (Intermediate)
  arith mean: 1.0, stddev: 0.816496580928
   Mean: Intermediate -- stddev: from 'Novice' to 'Expert'
Rate the complexity of the exercise
  median: 4.0 (medium but tricky)
  arith mean: 3.33333333333, stddev: 1.490711985
   Mean: medium -- stddev: from 'simple but time consuming' to 'hard'
How helpful do you judge our tool?
  median: 3.0 (helpful)
  arith mean: 3.26666666667, stddev: 0.771722460186
   Mean: helpful -- stddev: from 'neutral' to 'extremely helpful'
How helpful do you consider the overall idea/process of our tool?
  median: 4.0 (extremely helpful)
  arith mean: 3.46666666667, stddev: 0.884433277428
   Mean: helpful -- stddev: from 'helpful' to 'extremely helpful'
Do you think our idea might help to manage large networks over a long period with lots of responsible p
  Yes: 93.333333%
  Don't know: 6.666667%
  No: 0.000000%
For tasks similar to this test, would you want to use our tool?
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
the network design task:
  valid: median: 15.0
```

[1] or a competing product, we asked to assume that an intuitive user interface is available

```
    arith mean: 13.4666666667, stddev: 4.12903001792
  invalid: median: 2.0
    arith mean: 3.8, stddev: 4.48998886413
  missing: median: 7.0
    arith mean: 8.06666666667, stddev: 4.46417841141
  errors: median: 9.0
    arith mean: 11.8666666667, stddev: 7.22833928983
----------------------------------------------------------------
evaluating study for experience level Novice
number of entries: 5
What's your experience?
  median: 0.0 (Novice)
  arith mean: 0.0, stddev: 0.0
   Mean: Novice -- stddev: from 'Novice' to 'Novice'
Rate the complexity of the exercise
  median: 1.0 (simple)
  arith mean: 2.6, stddev: 2.0591260282
   Mean: medium -- stddev: from 'simple' to 'hard'
How helpful do you judge our tool?
  median: 4.0 (extremely helpful)
  arith mean: 3.2, stddev: 1.16619037897
   Mean: helpful -- stddev: from 'neutral' to 'extremely helpful'
How helpful do you consider the overall idea/process of our tool?
  median: 4.0 (extremely helpful)
  arith mean: 3.2, stddev: 1.16619037897
   Mean: helpful -- stddev: from 'neutral' to 'extremely helpful'
Do you think our idea might help to manage large networks over a long period with lots of responsible pe
  Yes: 80.000000%
  Don't know: 20.000000%
  No: 0.000000%
For tasks similar to this test, would you want to use our tool?
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
the network design task:
  valid: median: 12.0
    arith mean: 10.6, stddev: 5.67802782663
  invalid: median: 4.0
    arith mean: 6.6, stddev: 4.92341345004
  missing: median: 11.0
    arith mean: 11.2, stddev: 6.17737808459
  errors: median: 17.0
    arith mean: 17.8, stddev: 9.10823802939
----------------------------------------------------------------
evaluating study for experience level Intermediate
number of entries: 5
What's your experience?
  median: 1.0 (Intermediate)
  arith mean: 1.0, stddev: 0.0
   Mean: Intermediate -- stddev: from 'Intermediate' to 'Intermediate'
Rate the complexity of the exercise
  median: 3.0 (medium)
  arith mean: 3.4, stddev: 0.489897948557
   Mean: medium -- stddev: from 'medium' to 'medium but tricky'
How helpful do you judge our tool?
  median: 3.0 (helpful)
  arith mean: 3.2, stddev: 0.4
   Mean: helpful -- stddev: from 'helpful' to 'extremely helpful'
How helpful do you consider the overall idea/process of our tool?
  median: 4.0 (extremely helpful)
  arith mean: 4.0, stddev: 0.0
```

```
   Mean: extremely helpful -- stddev: from 'extremely helpful' to 'extremely helpful'
Do you think our idea might help to manage large networks over a long period with lots of responsible pe
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
For tasks similar to this test, would you want to use our tool?
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
the network design task:
  valid: median: 14.0
    arith mean: 14.0, stddev: 1.41421356237
  invalid: median: 1.0
    arith mean: 1.6, stddev: 1.8547236991
  missing: median: 7.0
    arith mean: 7.4, stddev: 1.01980390272
  errors: median: 8.0
    arith mean: 9.0, stddev: 2.60768096208
----------------------------------------------------------------
evaluating study for experience level Expert
number of entries: 5
What's your experience?
  median: 2.0 (Expert)
  arith mean: 2.0, stddev: 0.0
   Mean: Expert -- stddev: from 'Expert' to 'Expert'
Rate the complexity of the exercise
  median: 4.0 (medium but tricky)
  arith mean: 4.0, stddev: 1.09544511501
   Mean: medium but tricky -- stddev: from 'medium' to 'hard'
How helpful do you judge our tool?
  median: 3.0 (helpful)
  arith mean: 3.4, stddev: 0.489897948557
   Mean: helpful -- stddev: from 'helpful' to 'extremely helpful'
How helpful do you consider the overall idea/process of our tool?
  median: 3.0 (helpful)
  arith mean: 3.2, stddev: 0.748331477355
   Mean: helpful -- stddev: from 'neutral' to 'extremely helpful'
Do you think our idea might help to manage large networks over a long period with lots of responsible pe
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
For tasks similar to this test, would you want to use our tool?
  Yes: 100.000000%
  Don't know: 0.000000%
  No: 0.000000%
the network design task:
  valid: median: 16.0
    arith mean: 15.8, stddev: 1.72046505341
  invalid: median: 1.0
    arith mean: 3.2, stddev: 4.44522215418
  missing: median: 5.0
    arith mean: 5.6, stddev: 2.0591260282
  errors: median: 9.0
    arith mean: 8.8, stddev: 3.76297754445
```

Configuration for Our Tool

Figure 1 was generated by our tool. The following input was provided.

Listing 1: Host property mapping for security requirement 1

```
{"model_type": "DomainHierarchyTE",
 "model_description": "Aircraft Domain Model",
 "model_breach_severity": 20,
 "model_params":{
   "node_properties": [
     {"node":"CabinCoreSrv", "position":["Aircraft", "Crew"], "trust":1},
     {"node":"Crew1", "position":["Aircraft", "Crew"]},
     {"node":"Crew2", "position":["Aircraft", "Crew"]},
     {"node":"IFEsrv", "position":["Aircraft", "Entertain"]},
     {"node":"IFE1", "position":["Aircraft", "Entertain"]},
     {"node":"IFE2", "position":["Aircraft", "Entertain"]},
     {"node":"SatGW", "position":["Aircraft", "Entertain", "INET"]},
     {"node":"WifiAccess", "position": ["Aircraft", "Entertain", "POD"], "trust":1},
     {"node":"POD1", "position": ["Aircraft", "Entertain", "POD"]},
     {"node":"POD2", "position": ["Aircraft", "Entertain", "POD"]}
     ],
   "global_properties":
              {"division": "Aircraft", "sub_divisions":[
                {"division": "Crew", "sub_divisions":[]},
                {"division": "Entertain", "sub_divisions":[
                  {"division": "POD", "sub_divisions":[]},
                  {"division": "INET", "sub_divisions":[]}
                ]}
               ]}

  }
}
```

Listing 2: Host property mapping for security requirement 3

```
{"model_type": "SecurityGatewayExtended",
 "model_description": "Inflight Entertainment Devices Binding to Master, no p2p",
 "model_breach_severity": 10,
 "model_params":{
    "node_properties": [
          {"node":"IFEsrv", "member_type":"SecurityGatewayIN"},
          {"node":"IFE1", "member_type":"DomainMember"},
          {"node":"IFE2", "member_type":"DomainMember"}
          ],
    "global_properties":null
    }
}
```

Listing 3: Host property mapping for security requirement 2

```
{"model_type": "BLPtrusted",
 "model_description": "Crew Communication and IFE Devices Confidentiality",
 "model_breach_severity": 5,
 "model_params":{
    "node_properties": [
        {"node":"CabinCoreSrv", "privacy":2},
        {"node":"Crew1", "privacy":2},
        {"node":"Crew2", "privacy":2},

        {"node":"IFE1", "privacy":1},
        {"node":"IFE2", "privacy":1},

        {"node":"IFEsrv", "privacy":0, "trusted": true},

          ],
    "global_properties":null
    }
}
```

Listing 4: The graph to be verified and analyzed

```
{
"nodes": [
 "CabinCoreSrv",
 "Crew1",
 "Crew2",
 "IFEsrv",
 "IFE1",
 "IFE2",
 "WifiAccess",
 "SatGW",
 "POD1",
 "POD2"],
"edges": [
   {"e1":"CabinCoreSrv", "e2":"Crew1"},
   {"e1":"CabinCoreSrv", "e2":"Crew2"},
   {"e1":"CabinCoreSrv", "e2":"IFEsrv"},
   {"e1":"Crew1", "e2":"CabinCoreSrv"},
   {"e1":"Crew1", "e2":"Crew2"},
   {"e1":"Crew2", "e2":"CabinCoreSrv"},
   {"e1":"Crew2", "e2":"Crew1"},
   {"e1":"IFEsrv", "e2":"IFE1"},
   {"e1":"IFEsrv", "e2":"IFE2"},
   {"e1":"IFEsrv", "e2":"WifiAccess"},
   {"e1":"IFEsrv", "e2":"SatGW"},
   {"e1":"IFE1", "e2":"IFEsrv"},
   {"e1":"IFE2", "e2":"IFEsrv"},
   {"e1":"WifiAccess", "e2":"IFEsrv"},
   {"e1":"WifiAccess", "e2":"SatGW"},
   {"e1":"WifiAccess", "e2":"POD1"},
   {"e1":"WifiAccess", "e2":"POD2"},
   {"e1":"POD1", "e2":"WifiAccess"},
   {"e1":"POD1", "e2":"POD2"},
   {"e1":"POD2", "e2":"WifiAccess"},
   {"e1":"POD2", "e2":"POD1"}

]

}
```