How to hack airplanes

…and get away with it.

elttam

whoami

0xloltan

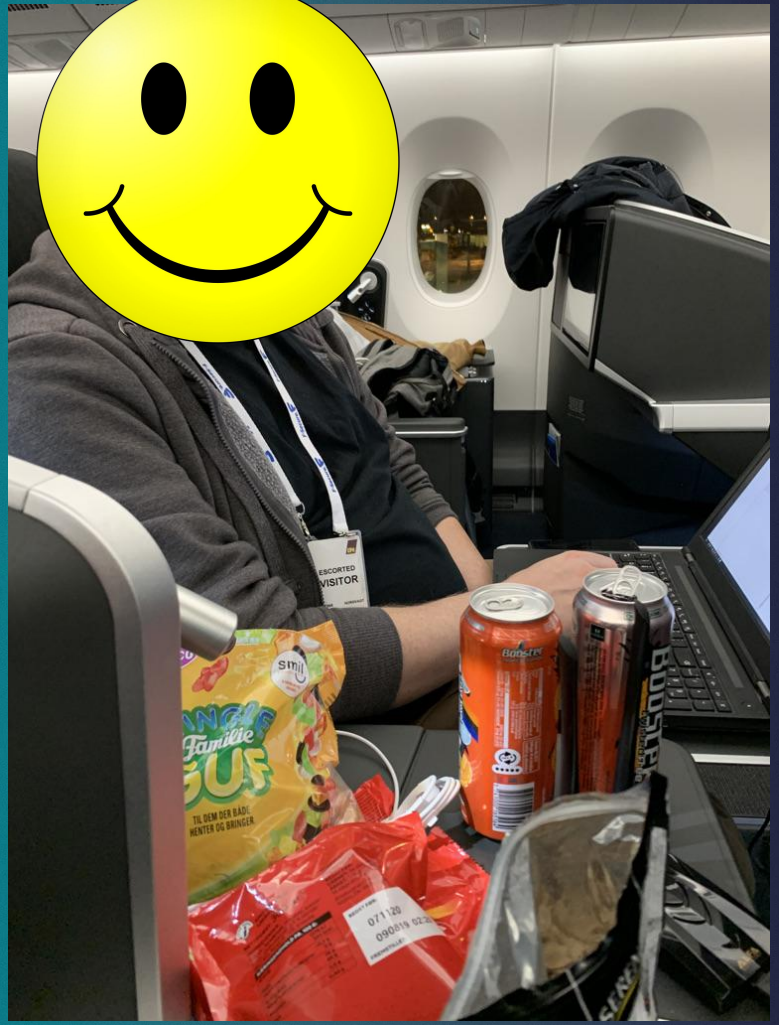
Zoltan Madarassy

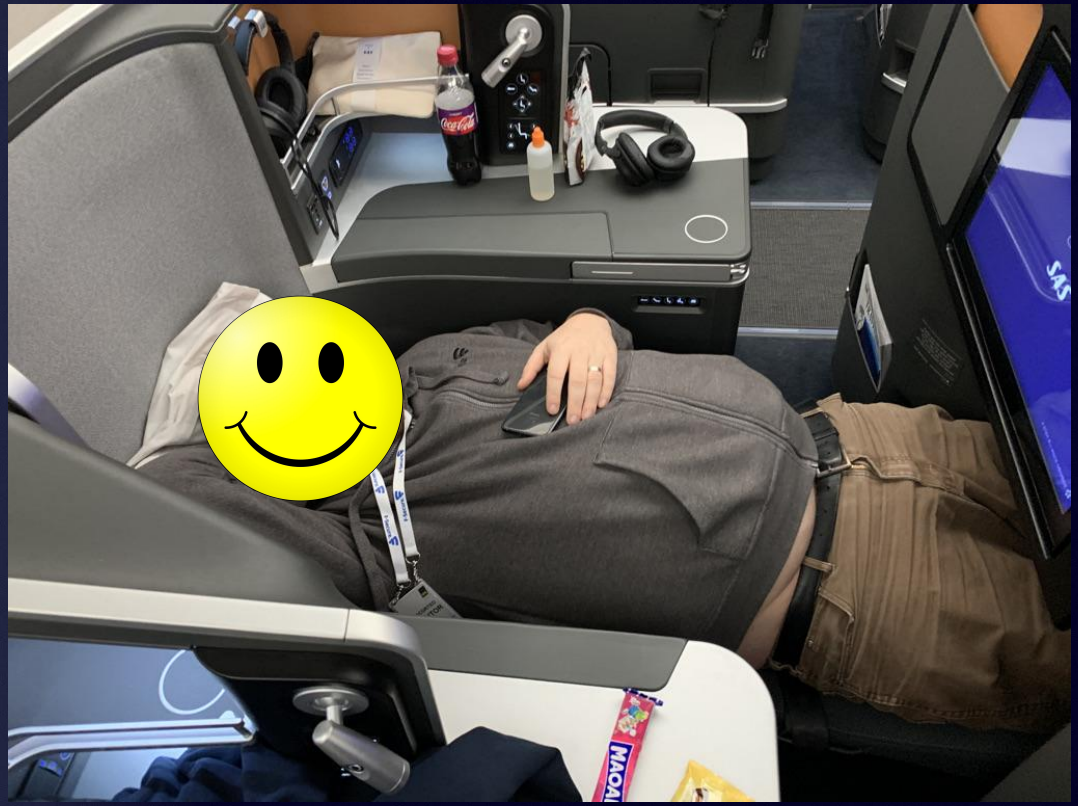
Principal Security Consultant at elttam

Relentless expat
🌍 🇭🇺🇳🇴🇸🇪🇦🇺 🌍

I like computers that fly

elttam

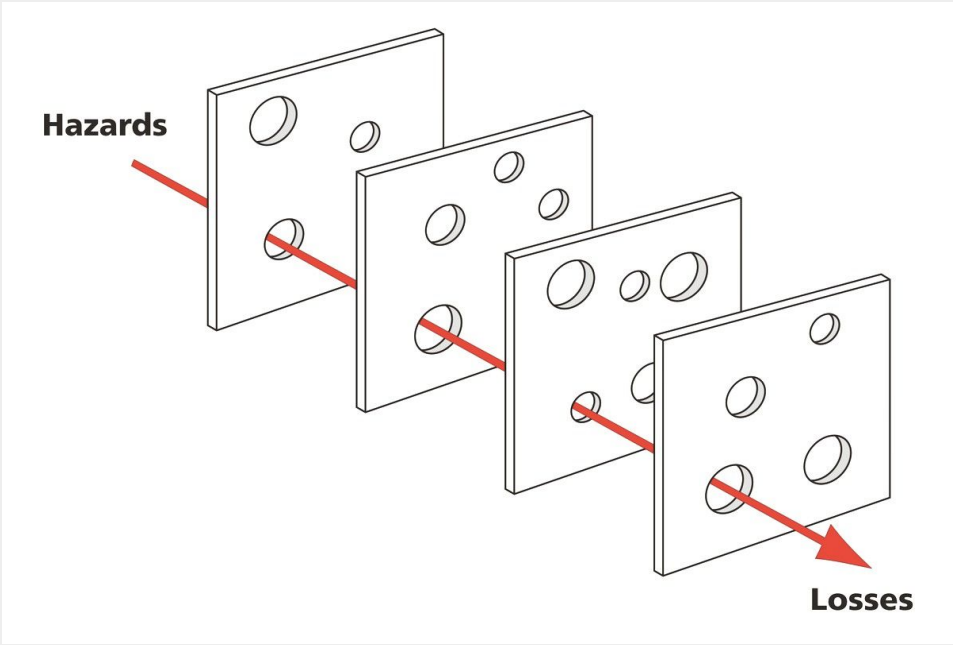

ESCORTED
VISITOR
Familie
TIL DEM DER BADE,
HENTER OG BRINGER
Booster
BOOSTER

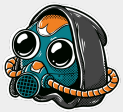

Coca-Cola

elttam

Aviation primer

- Security boundaries
- History in safety
- (Information) security is still kind of new
- Certification requirements
  - Now with a 100% more cyber!
- Swiss cheese model



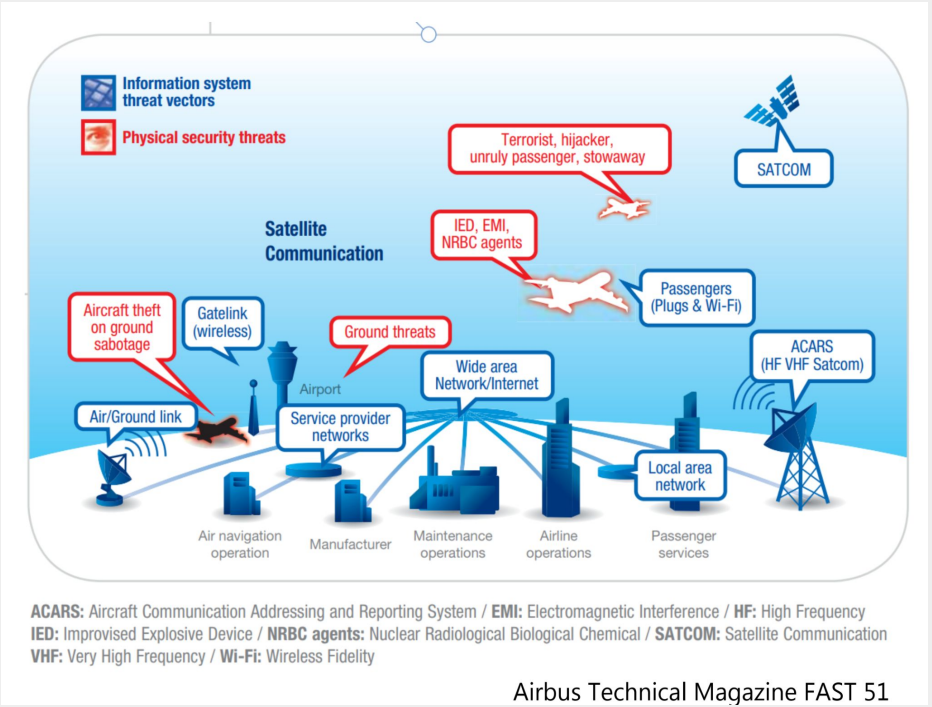


Glossary

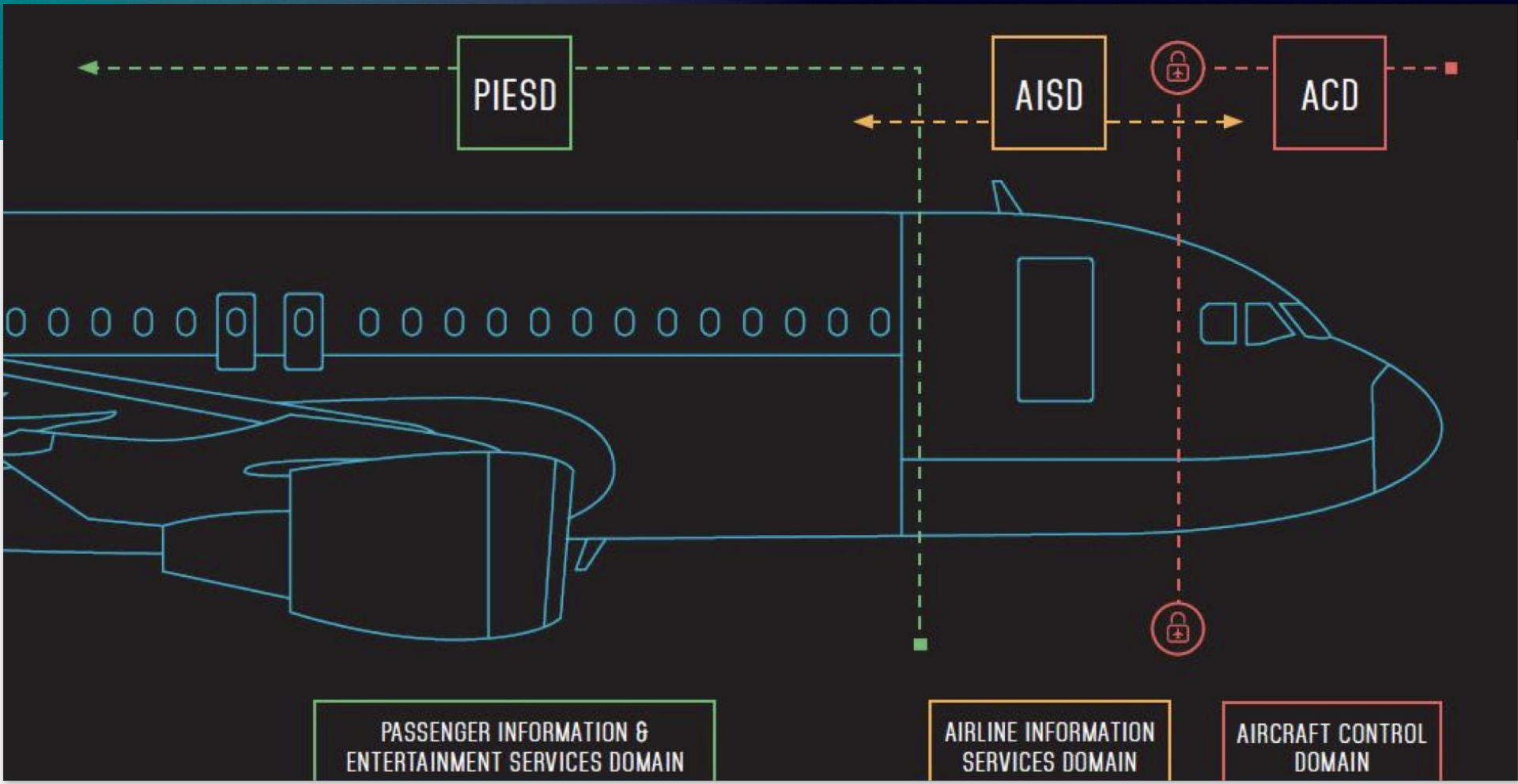
- ARINC-615(A)
  - Dataloading interfaces over ARINC-429 or ARINC-664
- ARINC-665
  - Loadable Software [Airplane] Parts (LS[A]P)
  - Media Set Parts (MSP)
- ARINC-827
  - Software crate
- ARINC-835
  - Encryption guidance for LSPs and MSPs
- ARINC-429/AFDX(ARINC-664)
  - Main network buses on an aircraft
- LRU
  - Line Replaceable Unit
- LSAP
  - Loadable Software Airplane Parts
- MRO
  - Maintenance, Repair and Operations
- ACD
- AISD
- PIESD

Aviation entanglement

- Aircraft manufacturers
- OEMs
- Operators and maintenance
- Airports and ANSPs
- Regulatory bodies



Airbus Technical Magazine FAST 51


PIESD
AISD
ACD
PASSENGER INFORMATION & ENTERTAINMENT SERVICES DOMAIN
AIRLINE INFORMATION SERVICES DOMAIN
AIRCRAFT CONTROL DOMAIN

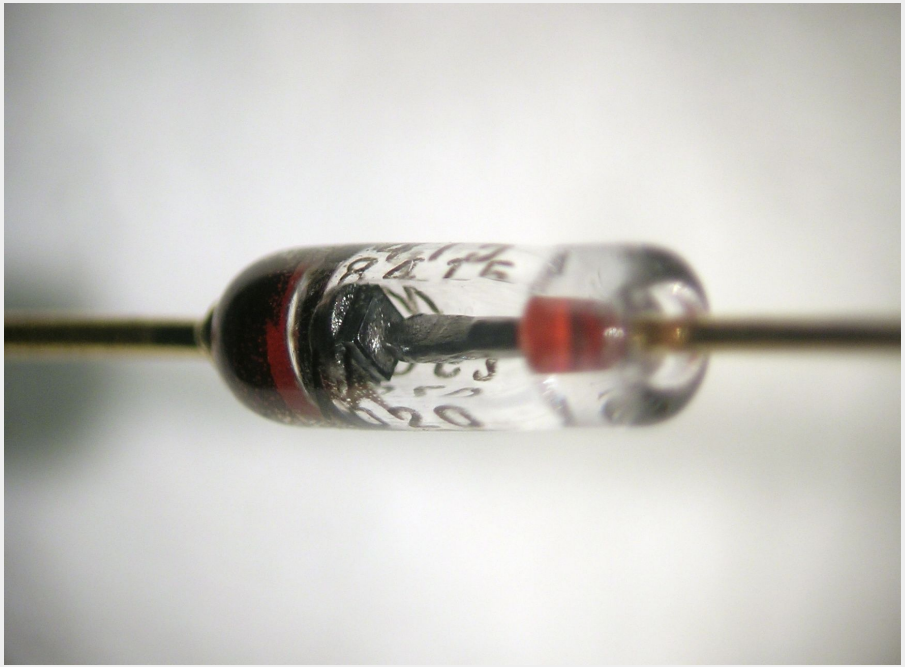
Feds Say That Banned Researcher Commandeered a Plane

A security researcher who was kicked off a United Airlines flight last month after tweeting a reference to its security vulnerabilities had previously taken control of an airplane mid-flight.

GETTY IMAGES

Domain separation

- Example: Data diodes
  - Ideal separation between domains
- Interconnection cutoffs MAC <> PHY



Attack surface example 1 - ACD

CAN bus

- CAN is rarely used on airplanes
- Except for example lavatory doors
- Inaccessible in bulkheads

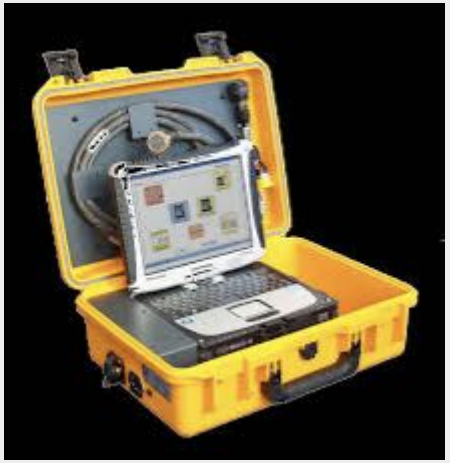
Honorable mention:

- B737 MAX MCAS

Attack surface example 2 - AISD

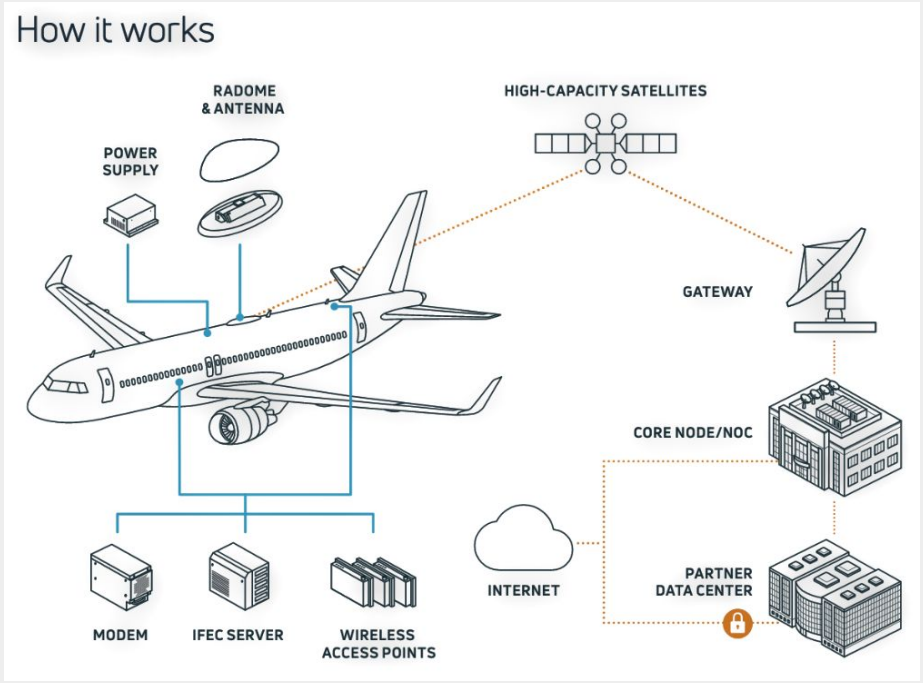
Data loading

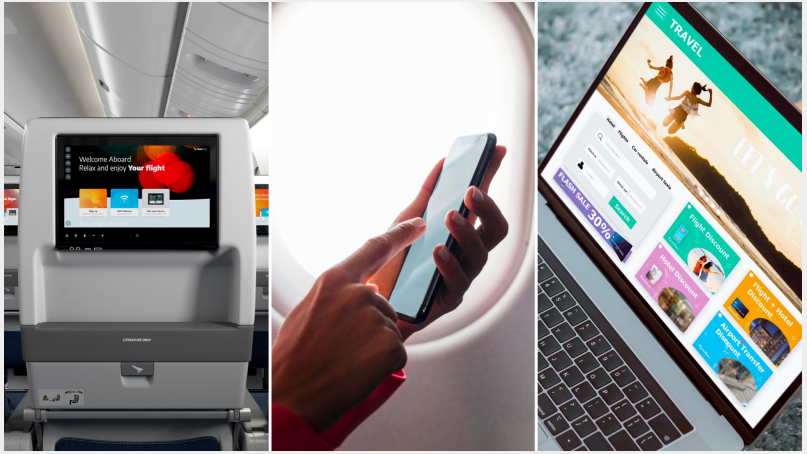
- Media
  - Floppies
  - USB drives
  - Maintenance laptops
  - Portable data loaders
  - Integrated data loaders
  - Gatelink (wifi/cellular)
- Update types
- Bus
- Signatures and verification



Attack surface example 3 - PIESD

IFEC

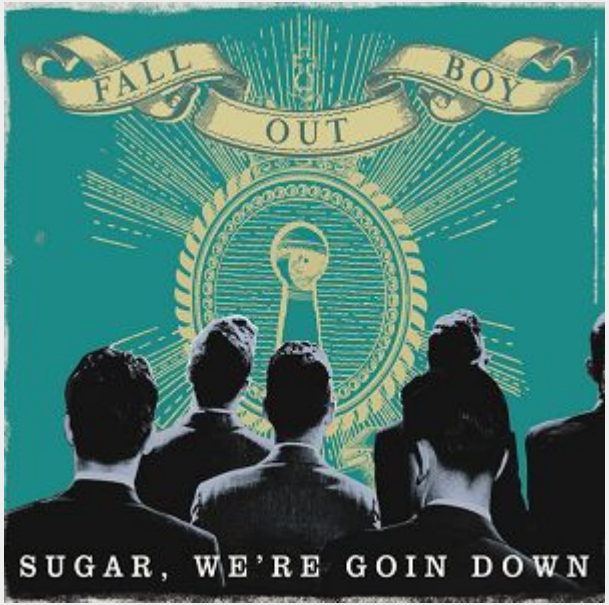




Attack surface example 3 - PIESD

IFEC

- Maintenance panels
  - Touchscreen
  - RJ-45
- IFE APIs
  - IDOR
  - Auth bypass
- IFC
  - Network separation
  - Client isolation
- PRAMs



Case study - Portable data loader

Data loading process

1. New update available (LSAP)
2. LSAP -> Librarian
3. Librarian -> Data loader / LRU
4. Verification and installation

Case study - Portable data loader

Attack surface

- GUI
- USB (airside and groundside)
- Wifi
- Ethernet
- Backend APIs
- ARINC-615(A)
- Secure boot
- Debugging interfaces

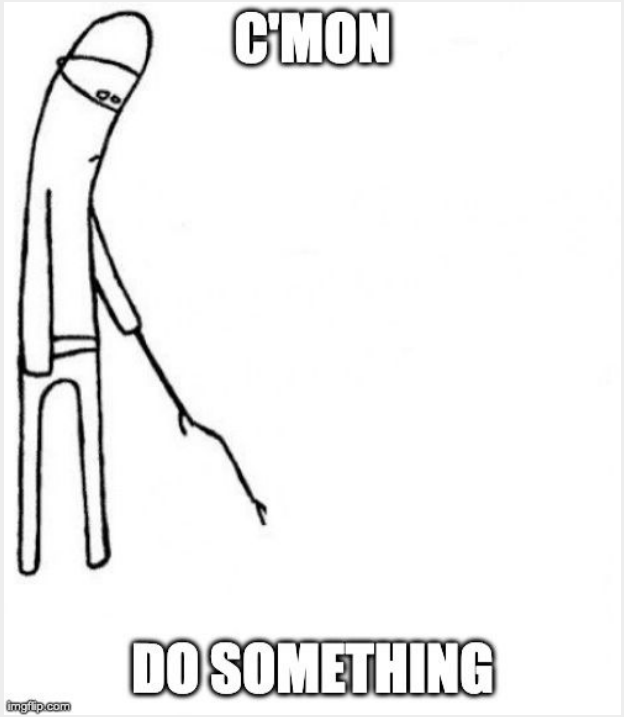
Case study - Portable data loader

Threat scenarios

- Isolation bypass
- Physical tampering
- Malicious data

Case study - Portable data loader

Approach

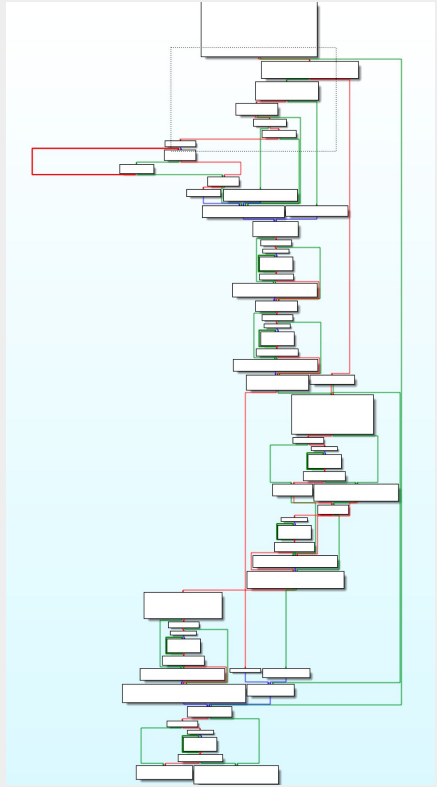


- Scope:
  - USB
  - Ethernet
  - Wifi
- Network exposure and comms review
- IP stack fuzzing
- USB stack fuzzing
  - Mass storage
- File system and file name manipulation
  - Manually

Case study - Portable data loader

Threat scenario - Importing root CAs from USB

- Idea: RCE via cert attribute
- Reverse all the things!
- Spoiler alert: no luck ☹
- Reversing QT binaries is terrible



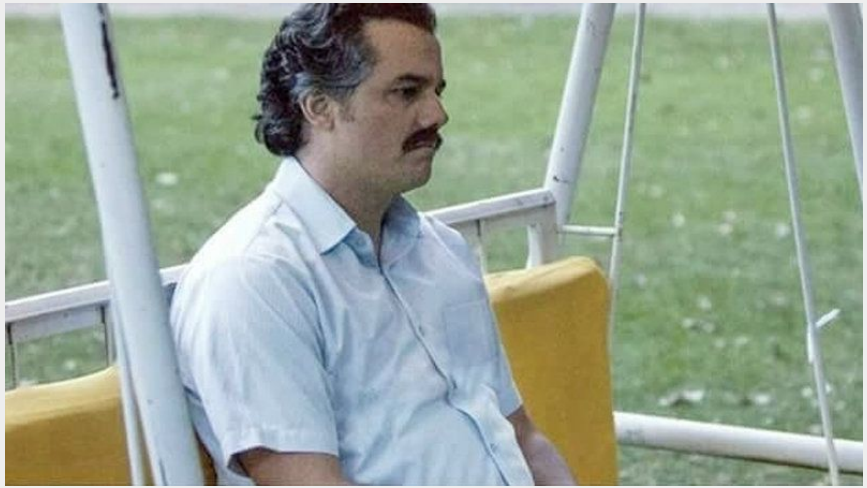
rfc-editor.org/rfc/rfc2631

Note that these ASN.1 definitions use EXPLICIT tagging. (In ASN.1, EXPLICIT tagging is implicit unless IMPLICIT is explicitly specified.)

Case study - Portable data loader

Expectation

Reality



Case study - Portable data loader

- Internal requirement
- Choice: ClamAV
  - Because it’s free
- Increased attack surface
- AV in aviation 😲
- But it doesn't actually do anything ¯_(ツ)_/¯

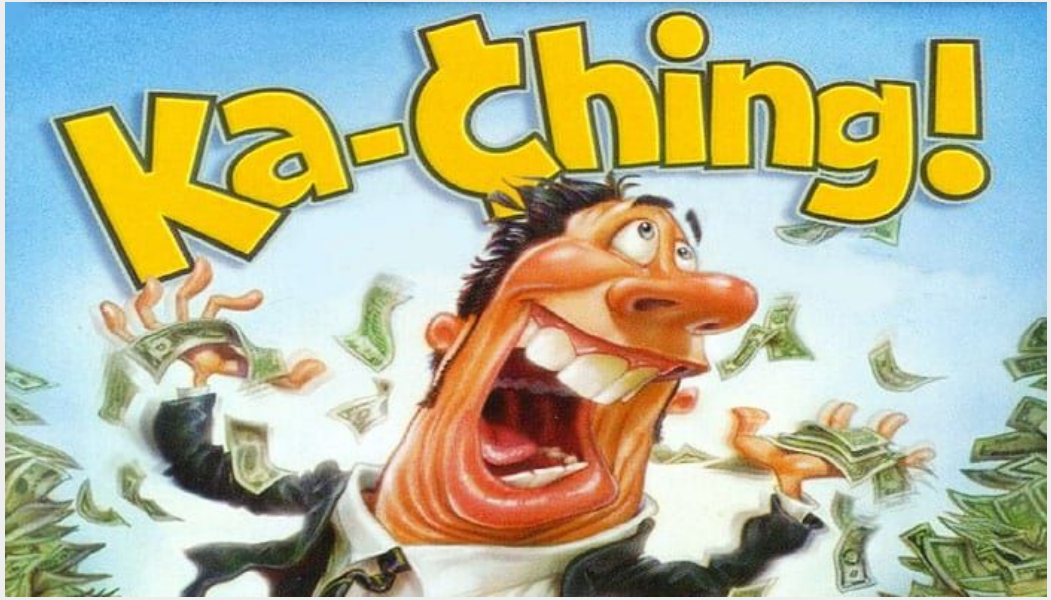
Case study - Portable data loader

```
configurations {
  default = "conf@1";
  conf@1 {
    description = "blah";
    kernel = "kernel@1";
    fdt = "fdt@1";
    signature@1 {
      hashed-strings = [00 00 00 00 00 00 00 a1];
      hashed-nodes = "/", "/configurations/conf@1", "/images/fdt@1", "/images/fdt@1/hash@1",
      timestamp = [5e 28 42 b3];
      signer-version = "2018.03";
      signer-name = "mkimage";
      value = [54 82 6e b0 7b 80 df ef f1 9a e4 73 89 14 1e 92 6b 7a 29 59 2b 40 90 f9 da a4
      algo = "sha256,rsa2048";
      key-name-hint = "dev";
      sign-images = "fdt", "kernel";
    };
  };
};
```

Case study - Portable data loader

```
## Loading kernel from FIT Image at 12000000 ...
   Using 'conf@2' configuration
   Verifying Hash Integrity ... sha256,rsa4096:PMATXS_OPSA+ OK
   Trying 'kernel@2' kernel subimage
     Description:  Super 1337 kernel
     Type:         Kernel Image
     Compression:  uncompressed
     Data Start:   0x22524244
     Data Size:    6761824 Bytes = 6.4 MiB
     Architecture: ARM
     OS:           Linux
     Load Address: 0x11000000
     Entry Point:  0x11000000
   Verifying Hash Integrity ... OK
## Loading ramdisk from FIT Image at 12000000 ...
## Loading fdt from FIT Image at 12000000 ...
   Using 'conf@2' configuration
   Trying 'fdt@1' fdt subimage
     Description:  ADK MSC SM2 i.MX6 LVDS Device Tree
     Type:         Flat Device Tree
     Compression:  uncompressed
     Data Start:   0x12672f68
     Data Size:    50225 Bytes = 49 KiB
     Architecture: ARM
     Load Address: 0x11800000
     Hash algo:    sha256
     Hash value:   d084787a3498ab51fabc86e11bd41ade9c077a01f1def1f7b767fb
66a
   Verifying Hash Integrity ... sha256+ OK
   Loading fdt from 0x12672f68 to 0x11800000
   Booting using the fdt blob at 0x11800000
   Loading Kernel Image ... OK
   Using Device Tree in place at 11800000, end 1180f430

Starting kernel ...
```



Thank You!

Questions?

elttam