digital security | econocom

IoT Devices Vulnerabilities - aeronautics and aerospace security

Renaud Lifchitz – Space's Industrial Control Systems Security – 28/10/2018

digital.security IoT CERT and its activities

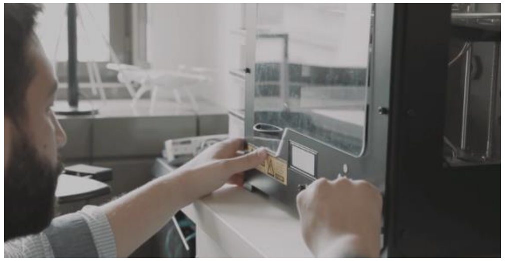
digital security

Our CERT

- CERT UBIK:
  the very first CERT in Europe dedicated to IoT security
- 40 experts
- Security watch, incident response, security audits, reverse engineering, …
- We have our own dedicated lab in Paris

Digital Security portfolio

- **Security level evaluation of the IoT chain**
  - Integrating security into projects
  - Software and hardware reverse engineering
  - Code review
  - Penetration tests



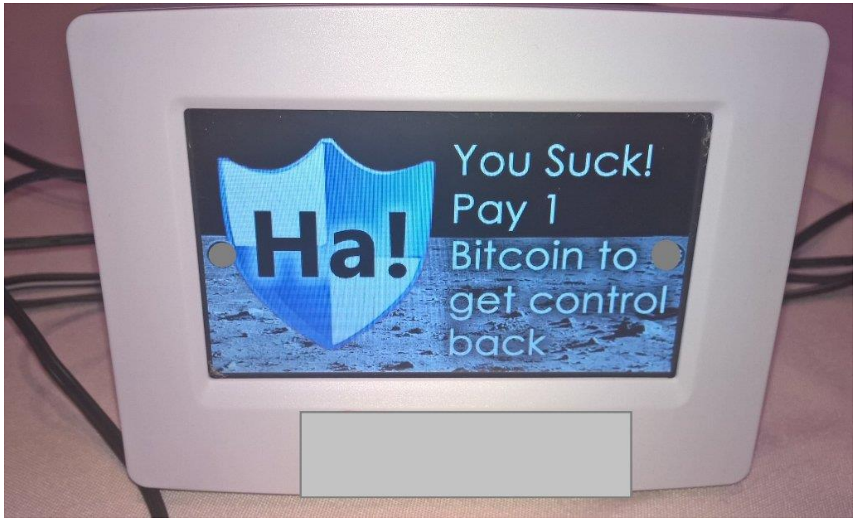
Equipment and appropriate skills for the IoT security specificities

Top 5 IoT vulnerabilities after 100 IoT audits

digital security

#1 : Non-secure updates

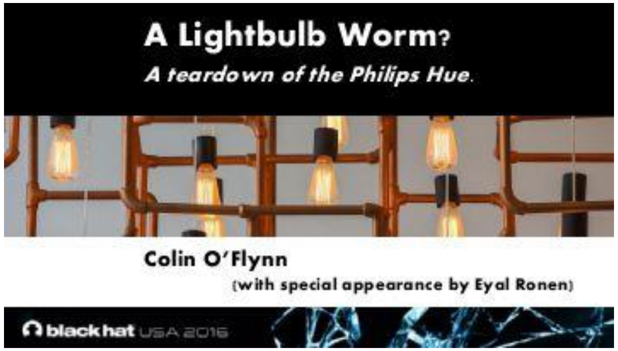
- Lack of encryption: **secrets leak**
- Lack of authenticated signatures: **possible alteration of software**



Connected thermostat compromised by a ransomware

#2 : Secret keys by default

- **ZigBee**
  - Key **ZigbeeAlliance09** still often used
  - Non-compliance with security best practices about key management (PKI)



A Lightbulb Worm?

A teardown of the Philips Hue.

Colin O'Flynn

(with special appearance by Eyal Ronen)

black hat USA 2016

- **Bluetooth Smart**
  - PIN code easy to guess (**0000**, **1234**, ...)

ZigBee default key implemented on existing Lightify Osram lightbulbs

#3 : Lack of encrypted communications

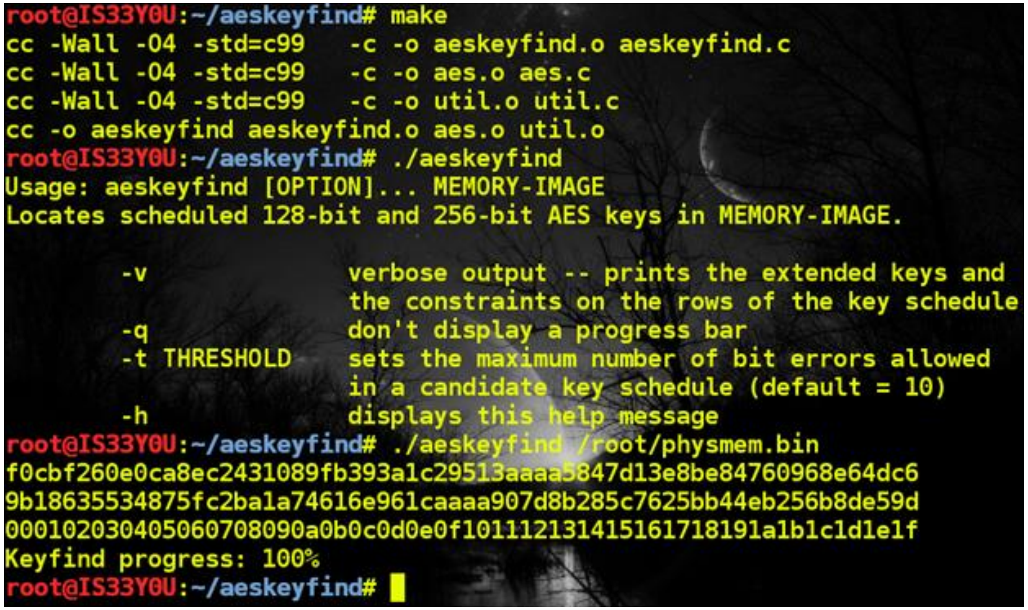
- **Sigfox**
  - No encryption by default
  - Data size : 12 bytes maximum (AES not possible)

Préambule 1	Préambule 2	Compteur	Numéro de série	Contenu applicatif	MAC	FCS
aaaa	a94c	000c	61870000	aaaaaaaaaaaaaaaaaaaaaaaa	c913	8fef
aaaa	a94c	002a	61870000	ffffffff7ffffffffffffff	f008	de0a
aaaa	a94c	002d	61870000	ffffffff7ffffffffffffff	558e	f7d0

- **LoRa**
  - No encryption by default (unlike **LoRaWAN**)

#4 : Non-secure data storage

- Configuration datas
- Personal data linked to a user
- Encryption or authentication keys

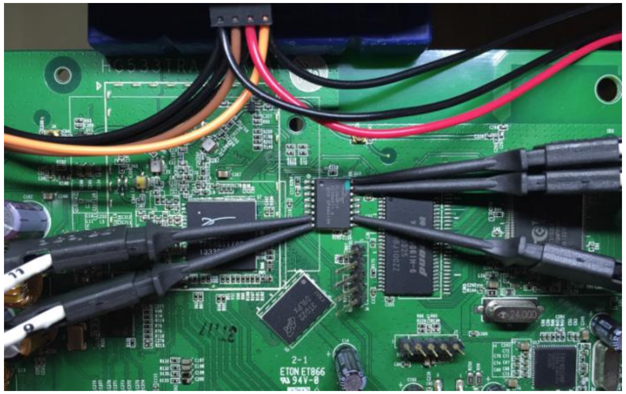


```
root@IS33Y0U:~/aeskeyfind# make
cc -Wall -O4 -std=c99   -c -o aeskeyfind.o aeskeyfind.c
cc -Wall -O4 -std=c99   -c -o aes.o aes.c
cc -Wall -O4 -std=c99   -c -o util.o util.c
cc -o aeskeyfind aeskeyfind.o aes.o util.o
root@IS33Y0U:~/aeskeyfind# ./aeskeyfind
Usage: aeskeyfind [OPTION]... MEMORY-IMAGE
Locates scheduled 128-bit and 256-bit AES keys in MEMORY-IMAGE.

        -v              verbose output -- prints the extended keys and
                        the constraints on the rows of the key schedule
        -q              don't display a progress bar
        -t THRESHOLD    sets the maximum number of bit errors allowed
                        in a candidate key schedule (default = 10)
        -h              displays this help message
root@IS33Y0U:~/aeskeyfind# ./aeskeyfind /root/physmem.bin
f0cbf260e0ca8ec2431089fb393a1c29513aaaa5847d13e8be84760968e64dc6
9b18635534875fc2ba1a74616e961caaaa907d8b285c7625bb44eb256b8de59d
000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
Keyfind progress: 100%
root@IS33Y0U:~/aeskeyfind# 
```

#5 : Debug interface

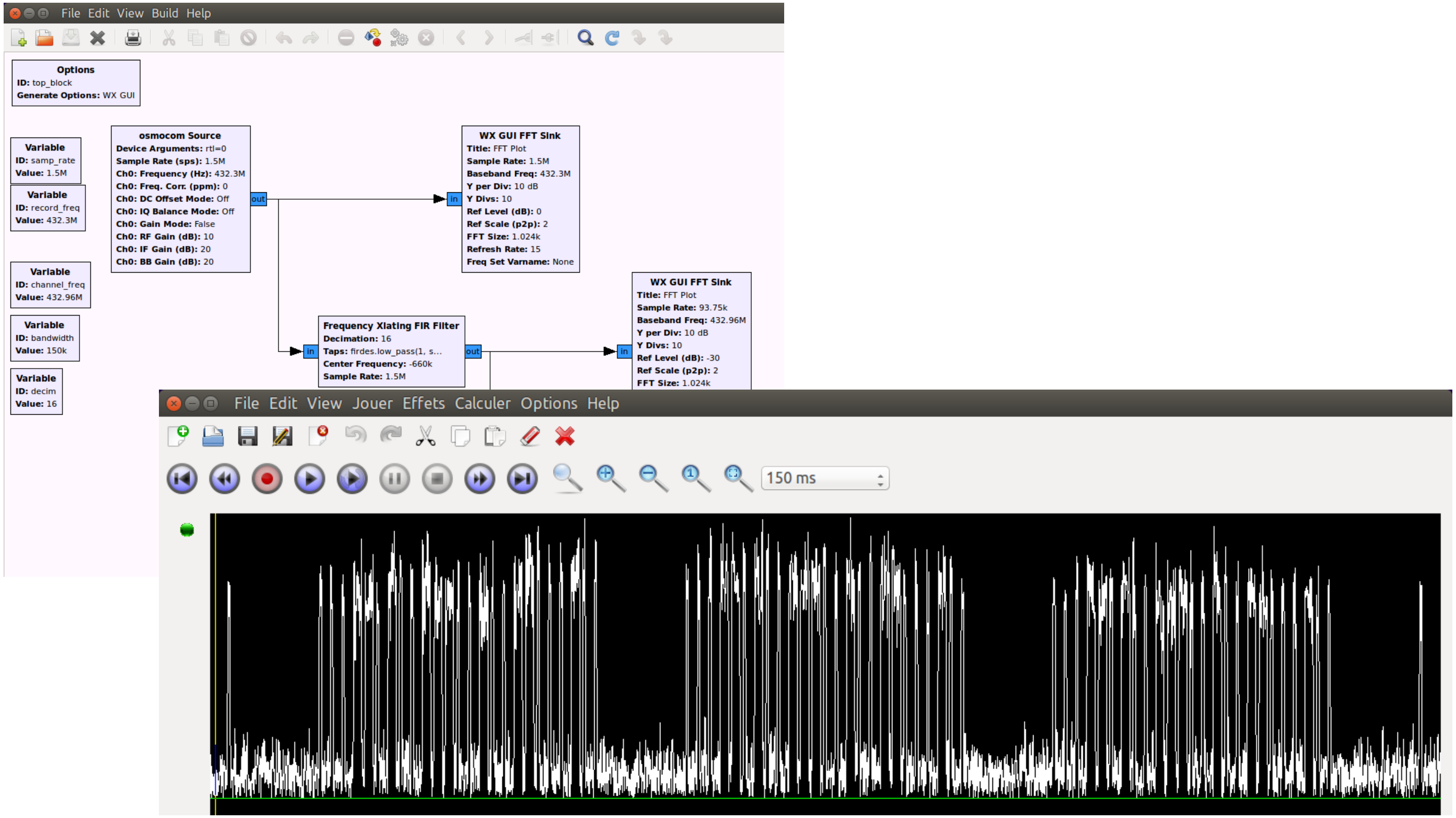
- Ability to bypass the read only protection
  - Reuse of protected code...
  - ... that accesses memory informations !
- Content extraction with the microprocessor registry



- Extraction of secrets from RAM, of firmware from Flash

IoT devices vulnerabilities &
aeronautics and aerospace security

SDR is spreading


File Edit View Build Help
File Edit View Jouer Effets Calculer Options Help
150 ms
out
in
out
in

Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 1.5M

Variable
ID: record_freq
Value: 432.3M

Variable
ID: channel_freq
Value: 432.96M

Variable
ID: bandwidth
Value: 150k

Variable
ID: decim
Value: 16

osmocom Source
Device Arguments: rtl=0
Sample Rate (sps): 1.5M
Ch0: Frequency (Hz): 432.3M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20

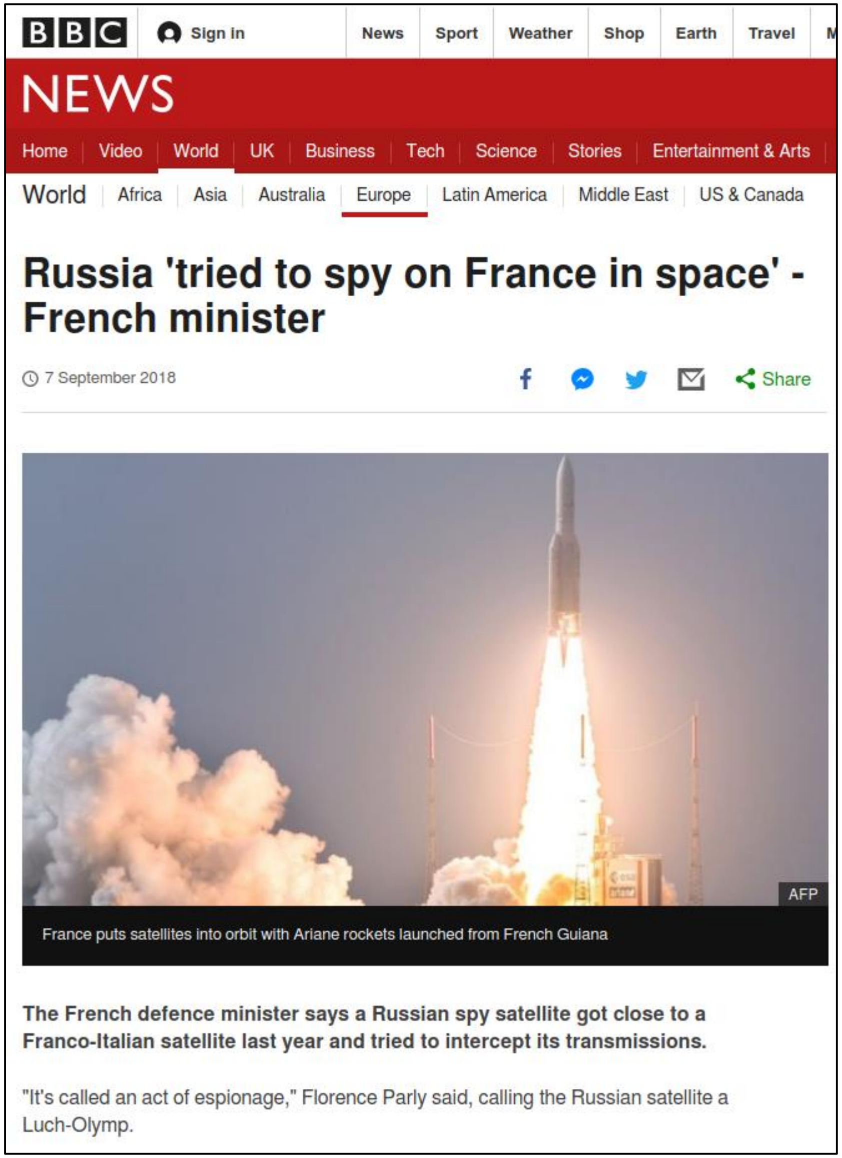
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 1.5M
Baseband Freq: 432.3M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

Frequency Xlating FIR Filter
Decimation: 16
Taps: firdes.low_pass(1, s...
Center Frequency: -660k
Sample Rate: 1.5M

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 93.75k
Baseband Freq: 432.96M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -30
Ref Scale (p2p): 2
FFT Size: 1.024k

- Software Defined Radio allows analysis of any RF communication
- Cheap devices (10€-400€)
- Open Source software, freely available

SDR allows easy RF sniffing



Russia 'tried to spy on France in space' - French minister

7 September 2018

France puts satellites into orbit with Ariane rockets launched from French Guiana

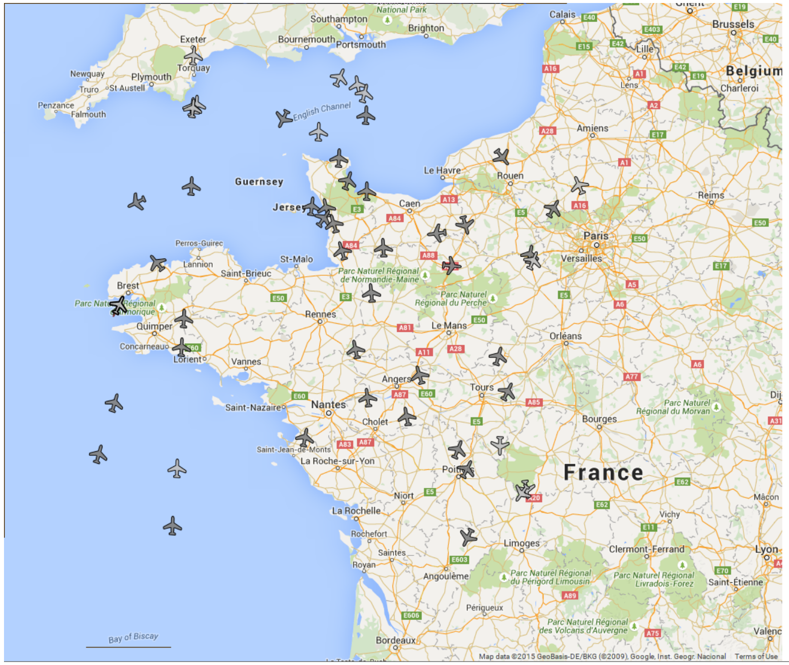
The French defence minister says a Russian spy satellite got close to a Franco-Italian satellite last year and tried to intercept its transmissions.

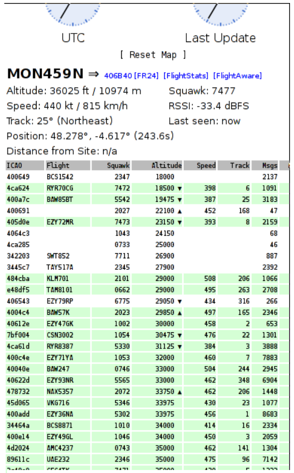
"It's called an act of espionage," Florence Parly said, calling the Russian satellite a Luch-Olymp.

<u>September 2018</u>:

Russian satellite Luch-Olymp tried to sniff French&Italian satellite Athena-Fidus communications

Real-time aircraft identification & geolocation

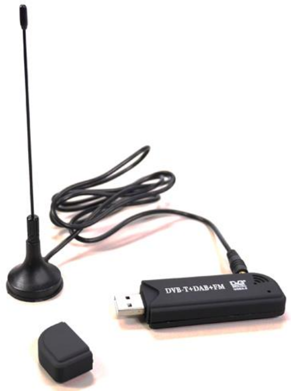




MON459N ⇒ 406B40 [FR24] [FlightStats] [FlightAware]

Altitude: 36025 ft / 10974 m Squawk: 7477
Speed: 440 kt / 815 km/h RSSI: -33.4 dBFS
Track: 25° (Northeast) Last seen: now
Position: 48.278°, -4.617° (243.6s)
Distance from Site: n/a

ICAO	Flight	Squawk	Altitude	Speed	Track	Msgs
400649	BCS1542	2347	18000			2137
4ca624	RYR70CG	7472	18500 ▼	398	6	1091
400a7c	BAW85BT	5542	19475 ▼	387	25	3183
400691		2027	22100 ▲	452	168	47
405d0e	EZY72MR	7473	23150 ▼	393	8	2159
4064c3		1043	24150			68
4ca285		0733	25000			46
342203	SWT852	7711	26900			887
3445c7	TAY517A	2345	27900			2392
484cba	KLM701	2101	29000	508	206	1066
e48df5	TAM8101	0662	29000	495	263	2708
406543	EZY79RP	6775	29050 ▼	434	316	266
4004c4	BAW57K	2023	29850 ▲	497	165	2346
40612e	EZY47GK	1002	30000	458	2	653
7bf004	CSN3002	1054	30475 ▼	476	22	1301
4ca61d	RYR8387	5330	31125 ▼	384	3	3888
400c4e	EZY71YA	1053	32000	460	7	7883
40040e	BAW247	0746	33000	504	244	2945
40622d	EZY93NR	5565	33000	462	348	6904
478732	NAX5357	2072	33750 ▲	462	206	1448
45d065	VKG716	5346	33975	430	23	1077
400add	EZY36NA	5302	33975	456	1	8683
34464a	BCS8871	1010	34000	414	16	2334
400e14	EZY49GL	1046	34000	450	3	2059
4d2024	AMC4237	0743	35000	462	141	1304
89611c	UAE232	2346	35000	475	96	7142



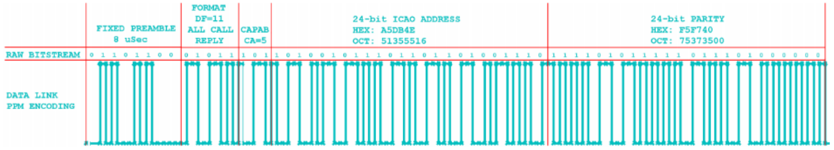
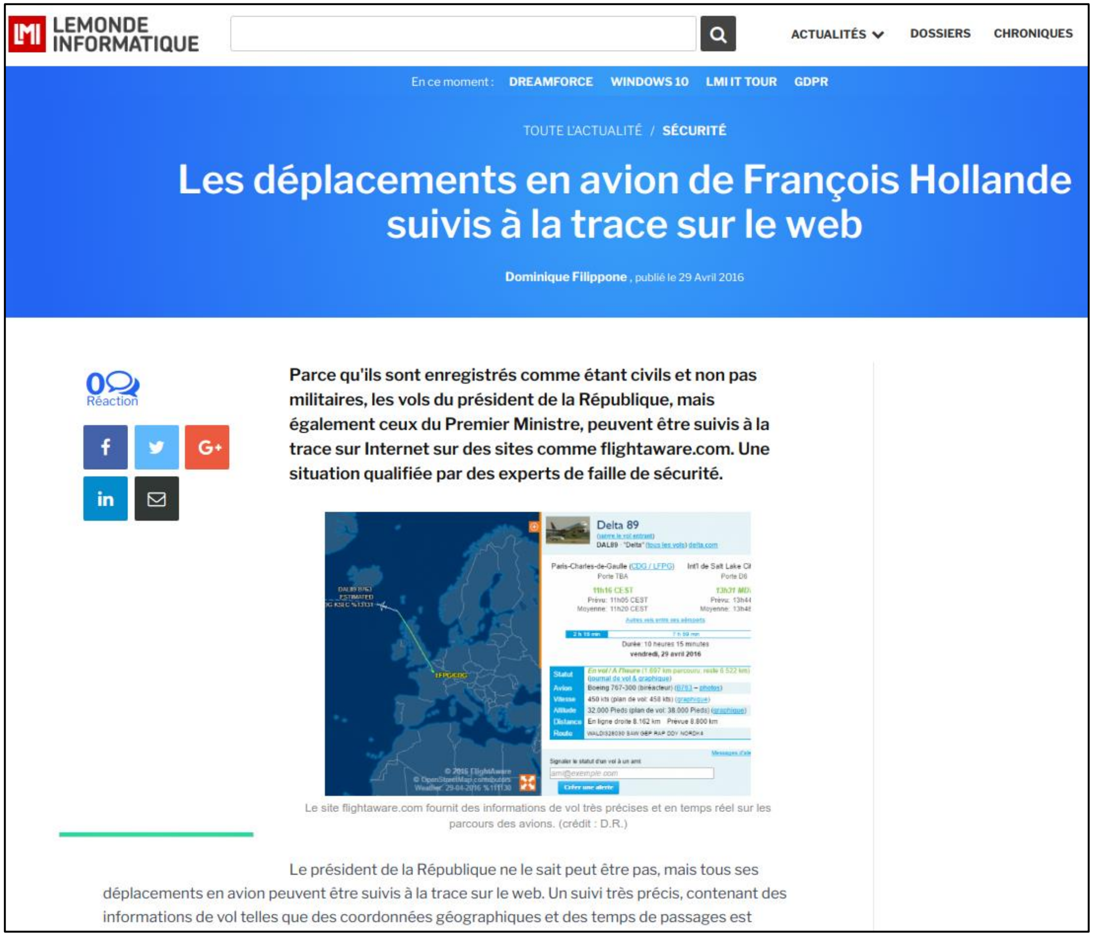


Figure 2. PPM-encoded ADS-B 56 bit sample frame.

- Listening to ADS-B frames (1090 MHz) sent in clear (flight number, position, altitude, speed...)
- Same issues with cockpit conversations (120-130 MHz) and ACARS damage reporting protocol (131-137 MHz)
- 10€ device and typical range of 100 km!

Real-time aircraft identification & geolocation



LEMONDE INFORMATIQUE

ACTUALITÉS DOSSIERS CHRONIQUES

En ce moment : DREAMFORCE WINDOWS 10 LMI IT TOUR GDPR

TOUTE L'ACTUALITÉ / SÉCURITÉ

Les déplacements en avion de François Hollande suivis à la trace sur le web

Dominique Filippone , publié le 29 Avril 2016

0 Réaction

Parce qu'ils sont enregistrés comme étant civils et non pas militaires, les vols du président de la République, mais également ceux du Premier Ministre, peuvent être suivis à la trace sur Internet sur des sites comme flightaware.com. Une situation qualifiée par des experts de faille de sécurité.

Delta 89
(suivre le vol entrant)
DAL89 · "Delta" (tous les vols) delta.com

Paris-Charles-de-Gaulle (CDG / LFPG) Porte TBA
11h16 CEST
Prévu: 11h05 CEST
Moyenne: 11h20 CEST

Int'l de Salt Lake Ci Porte D6
13h31 MD
Prévu: 13h44
Moyenne: 13h48

Autres vols entre ces aéroports

2 h 15 min 7 h 59 min
Durée: 10 heures 15 minutes
vendredi, 29 avril 2016

Statut	En vol / A l'heure (1.697 km parcouru, reste 6.522 km) (journal de vol & graphique)
Avion	Boeing 767-300 (biréacteur) (B763 – photos)
Vitesse	450 kts (plan de vol: 458 kts) (graphique)
Altitude	32.000 Pieds (plan de vol: 38.000 Pieds) (graphique)
Distance	En ligne droite 8.162 km Prévue 8.800 km
Route	WALDI328030 SAW GEP RAP DDY NORDK4

Messages d'ale
Signaler le statut d'un vol à un ami
ami@exemple.com
Créer une alerte

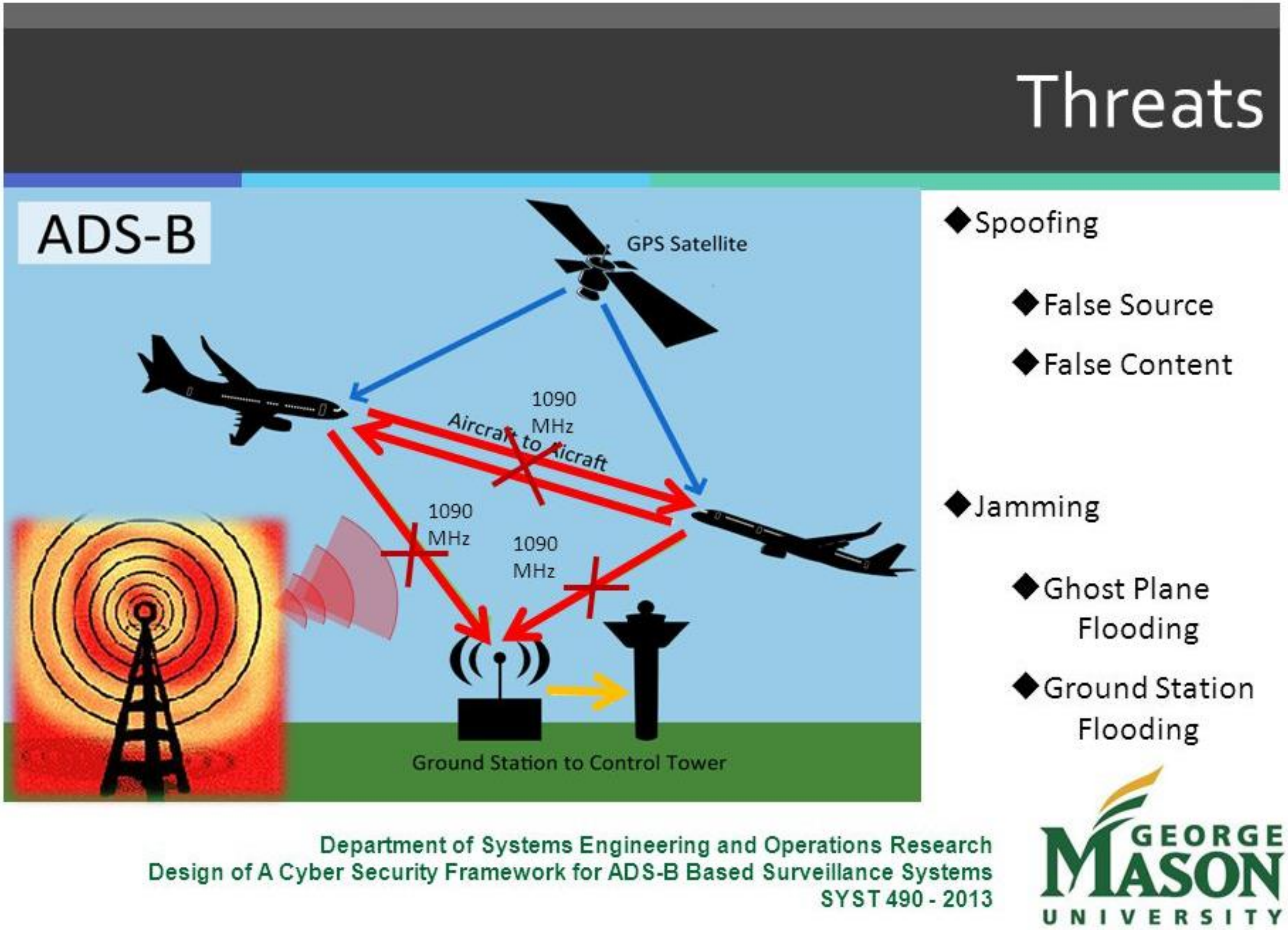
Le site flightaware.com fournit des informations de vol très précises et en temps réel sur les parcours des avions. (crédit : D.R.)

Le président de la République ne le sait peut être pas, mais tous ses déplacements en avion peuvent être suivis à la trace sur le web. Un suivi très précis, contenant des informations de vol telles que des coordonnées géographiques et des temps de passages est

April 2016:

French president and prime minister flights were easily trackable in realtime

Aircraft spoofing & jamming



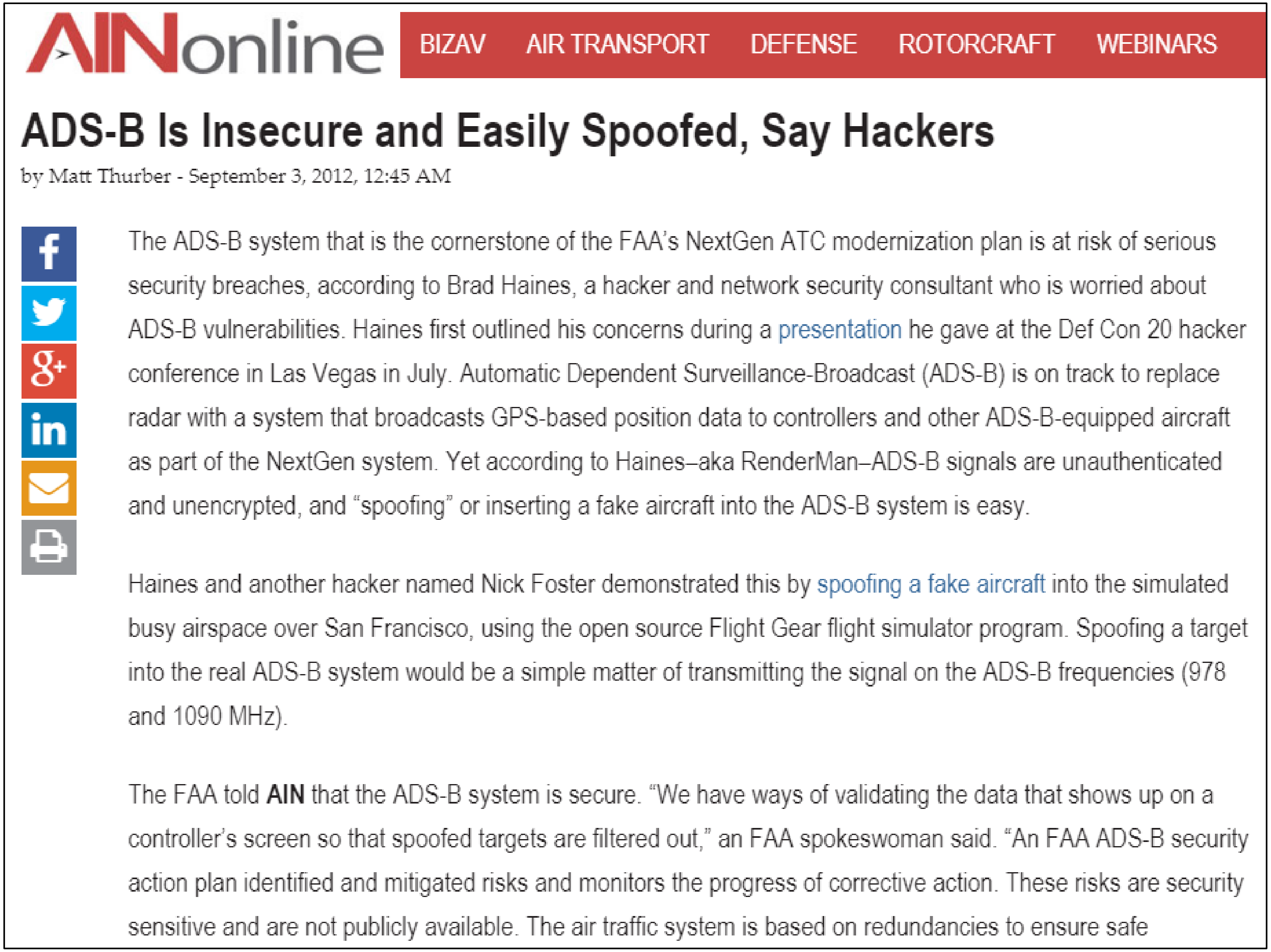
Threats

- ◆Spoofing
  - ◆False Source
  - ◆False Content
- ◆Jamming
  - ◆Ghost Plane Flooding
  - ◆Ground Station Flooding

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 490 - 2013

GEORGE MASON UNIVERSITY

Aircraft spoofing & jamming



ADS-B Is Insecure and Easily Spoofed, Say Hackers

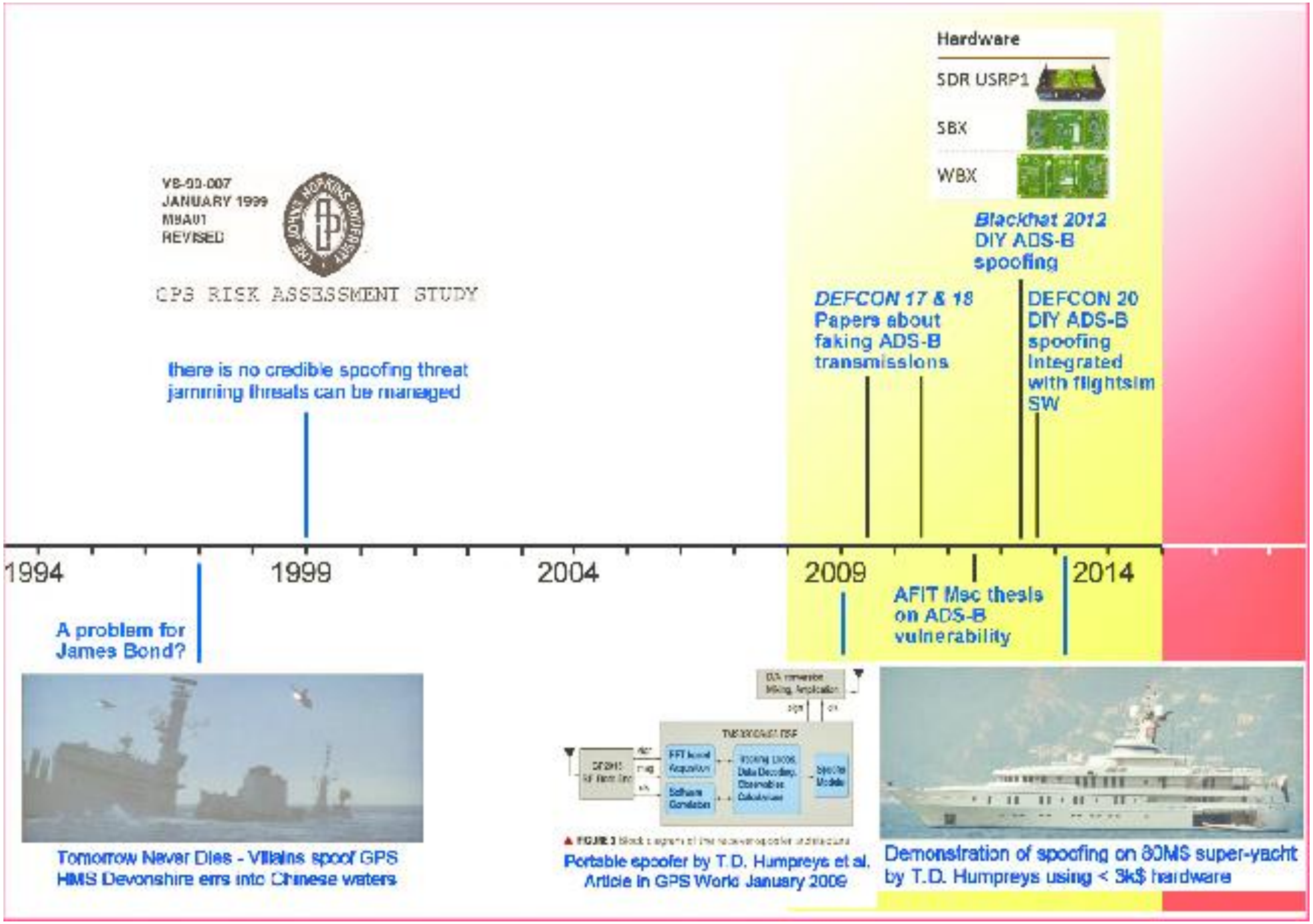
by Matt Thurber - September 3, 2012, 12:45 AM

The ADS-B system that is the cornerstone of the FAA's NextGen ATC modernization plan is at risk of serious security breaches, according to Brad Haines, a hacker and network security consultant who is worried about ADS-B vulnerabilities. Haines first outlined his concerns during a presentation he gave at the Def Con 20 hacker conference in Las Vegas in July. Automatic Dependent Surveillance-Broadcast (ADS-B) is on track to replace radar with a system that broadcasts GPS-based position data to controllers and other ADS-B-equipped aircraft as part of the NextGen system. Yet according to Haines–aka RenderMan–ADS-B signals are unauthenticated and unencrypted, and "spoofing" or inserting a fake aircraft into the ADS-B system is easy.

Haines and another hacker named Nick Foster demonstrated this by spoofing a fake aircraft into the simulated busy airspace over San Francisco, using the open source Flight Gear flight simulator program. Spoofing a target into the real ADS-B system would be a simple matter of transmitting the signal on the ADS-B frequencies (978 and 1090 MHz).

The FAA told **AIN** that the ADS-B system is secure. "We have ways of validating the data that shows up on a controller's screen so that spoofed targets are filtered out," an FAA spokeswoman said. "An FAA ADS-B security action plan identified and mitigated risks and monitors the progress of corrective action. These risks are security sensitive and are not publicly available. The air traffic system is based on redundancies to ensure safe

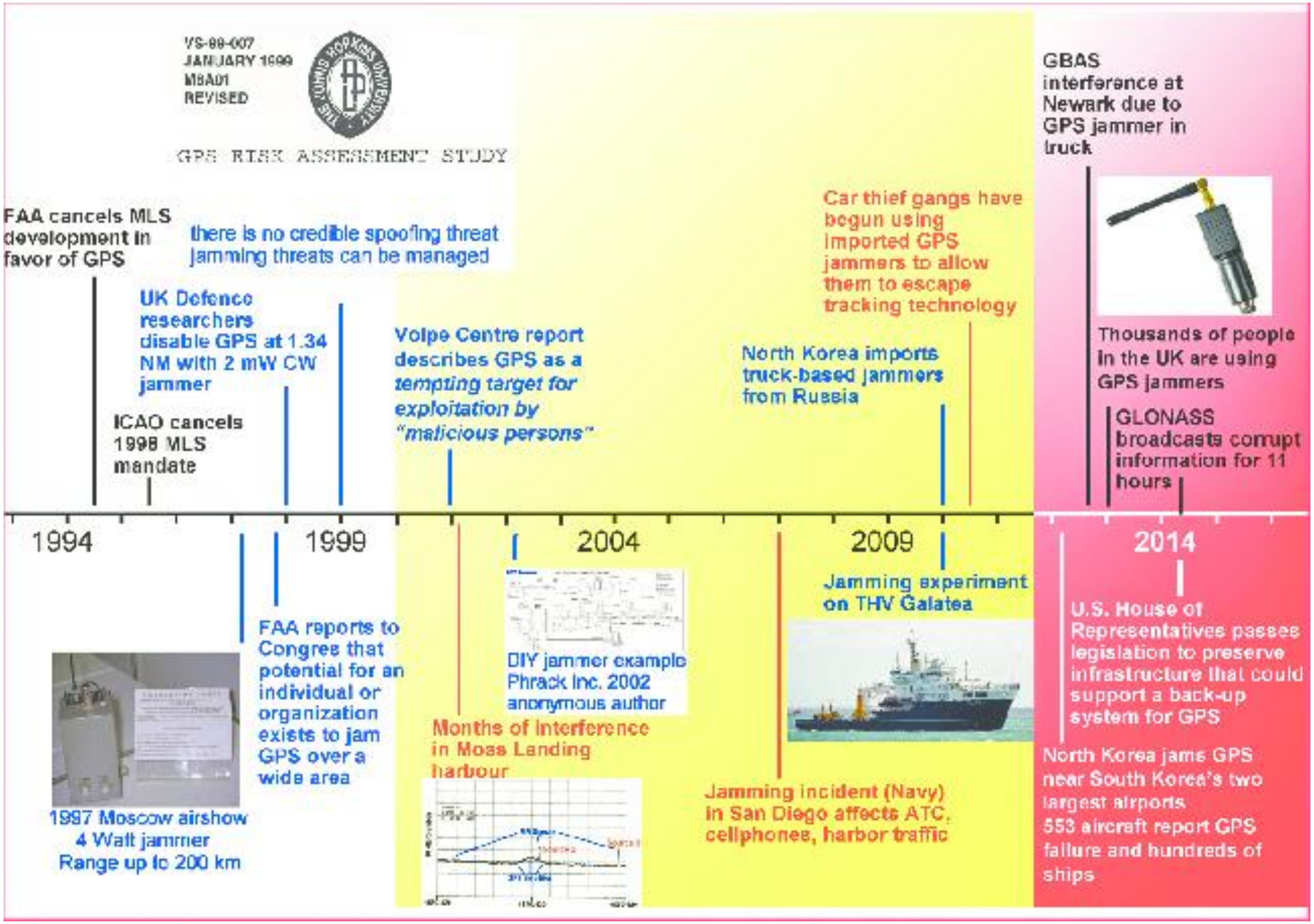
Aircraft spoofing & jamming


VS-99-007
JANUARY 1999
M9A01
REVISED
GPS RISK ASSESSMENT STUDY
there is no credible spoofing threat
jamming threats can be managed
Hardware
SDR USRP1
SBX
WBX
Blackhat 2012
DIY ADS-B
spoofing
DEFCON 17 & 18
Papers about
faking ADS-B
transmissions
DEFCON 20
DIY ADS-B
spoofing
Integrated
with flightsim
SW
1994
1999
2004
2009
2014
A problem for
James Bond?
AFIT Msc thesis
on ADS-B
vulnerability
Tomorrow Never Dies - Villains spoof GPS
HMS Devonshire errs into Chinese waters
Portable spoofer by T.D. Humpreys et al.
Article in GPS World January 2009
Demonstration of spoofing on 80MS super-yacht
by T.D. Humpreys using < 3k$ hardware

ADS-B security from 1994 to 2014

"So you think you are safe", Eric Theunissen, Ministry of Defense - Netherlands, 2014

GPS spoofing & jamming



VS-99-007
JANUARY 1999
MBA01
REVISED

GPS RISK ASSESSMENT STUDY

there is no credible spoofing threat
jamming threats can be managed

FAA cancels MLS development in favor of GPS

ICAO cancels 1998 MLS mandate

UK Defence researchers disable GPS at 1.34 NM with 2 mW CW jammer

1997 Moscow airshow
4 Watt jammer
Range up to 200 km

FAA reports to Congres that potential for an individual or organization exists to jam GPS over a wide area

Volpe Centre report describes GPS as a *tempting target for exploitation by "malicious persons"*

Months of interference in Moss Landing harbour

DIY jammer example
Phrack Inc. 2002
anonymous author

Jamming incident (Navy) in San Diego affects ATC, cellphones, harbor traffic

North Korea imports truck-based jammers from Russia

Car thief gangs have begun using imported GPS jammers to allow them to escape tracking technology

Jamming experiment on THV Galatea

GBAS interference at Newark due to GPS jammer in truck

Thousands of people in the UK are using GPS jammers

GLONASS broadcasts corrupt information for 11 hours

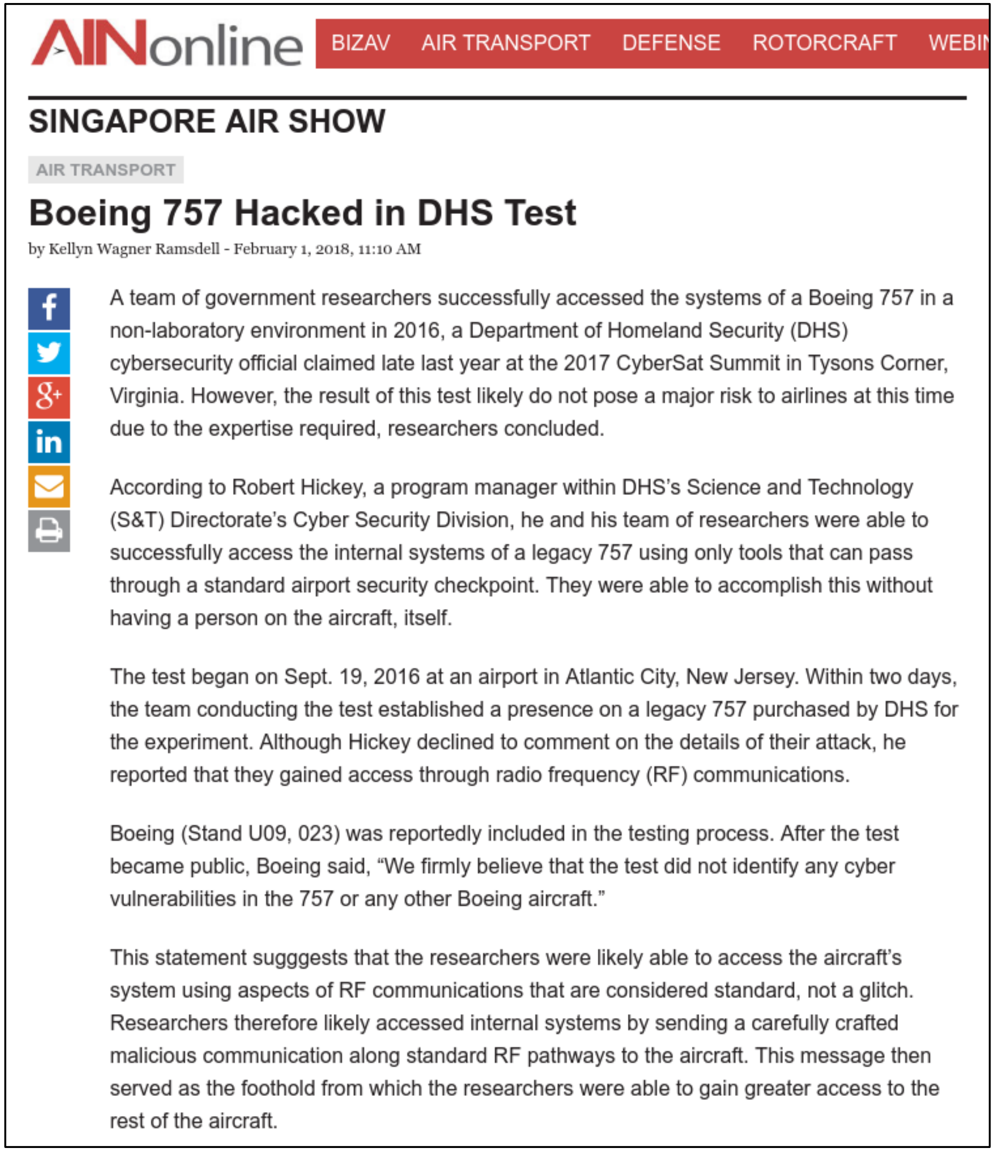
U.S. House of Representatives passes legislation to preserve infrastructure that could support a back-up system for GPS

North Korea jams GPS near South Korea's two largest airports
553 aircraft report GPS failure and hundreds of ships

GPS security from 1994 to 2014

"So you think you are safe", Eric Theunissen, Ministry of Defense - Netherlands, 2014

Most RF protocols aren’t designed for security



SINGAPORE AIR SHOW

AIR TRANSPORT

Boeing 757 Hacked in DHS Test

by Kellyn Wagner Ramsdell - February 1, 2018, 11:10 AM

A team of government researchers successfully accessed the systems of a Boeing 757 in a non-laboratory environment in 2016, a Department of Homeland Security (DHS) cybersecurity official claimed late last year at the 2017 CyberSat Summit in Tysons Corner, Virginia. However, the result of this test likely do not pose a major risk to airlines at this time due to the expertise required, researchers concluded.

According to Robert Hickey, a program manager within DHS’s Science and Technology (S&T) Directorate’s Cyber Security Division, he and his team of researchers were able to successfully access the internal systems of a legacy 757 using only tools that can pass through a standard airport security checkpoint. They were able to accomplish this without having a person on the aircraft, itself.

The test began on Sept. 19, 2016 at an airport in Atlantic City, New Jersey. Within two days, the team conducting the test established a presence on a legacy 757 purchased by DHS for the experiment. Although Hickey declined to comment on the details of their attack, he reported that they gained access through radio frequency (RF) communications.

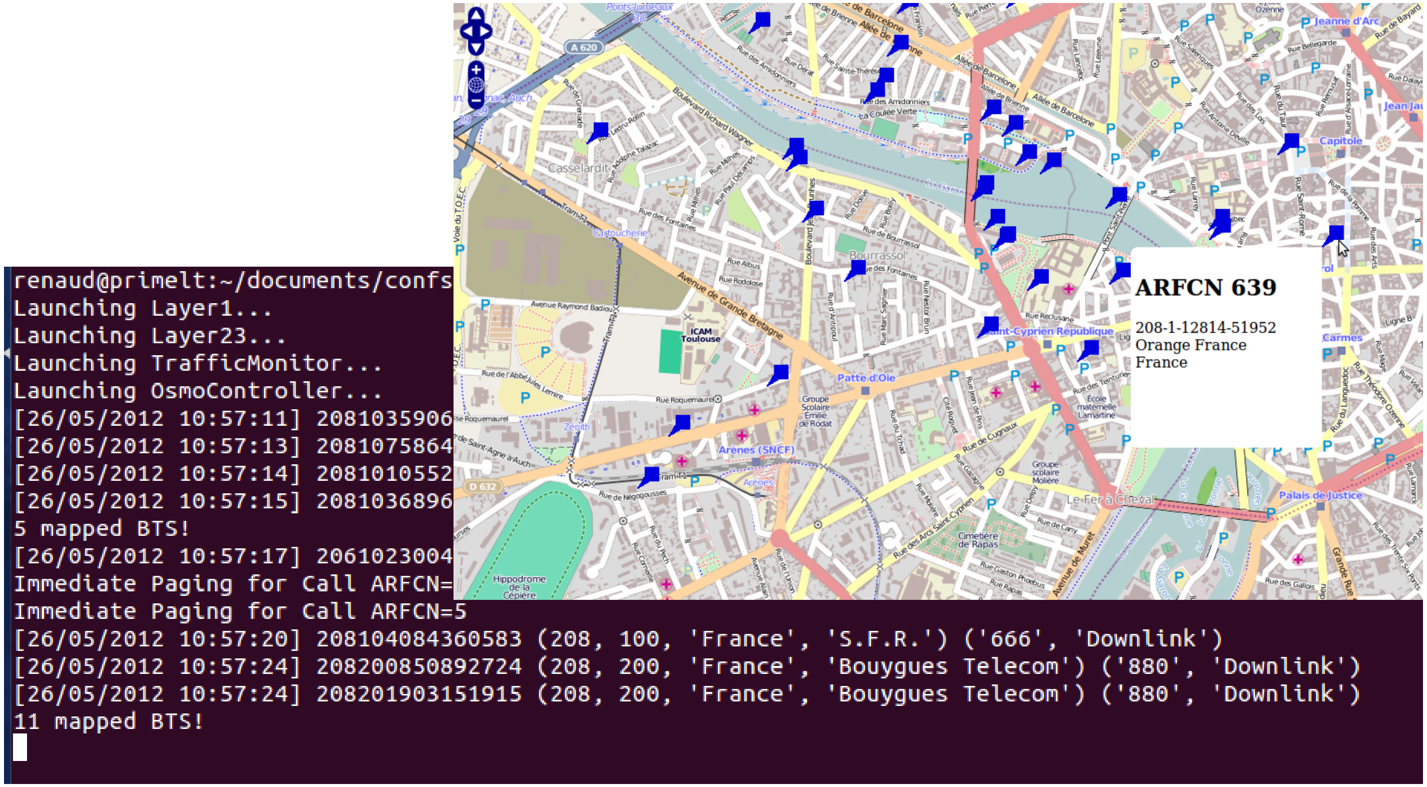
Boeing (Stand U09, 023) was reportedly included in the testing process. After the test became public, Boeing said, “We firmly believe that the test did not identify any cyber vulnerabilities in the 757 or any other Boeing aircraft.”

This statement suggests that the researchers were likely able to access the aircraft’s system using aspects of RF communications that are considered standard, not a glitch. Researchers therefore likely accessed internal systems by sending a carefully crafted malicious communication along standard RF pathways to the aircraft. This message then served as the foothold from which the researchers were able to gain greater access to the rest of the aircraft.

September 2016:

A Boeing 757 was hacked remotely in its runway using RF protocols

GSM antenna mapping and mobile devices geolocation



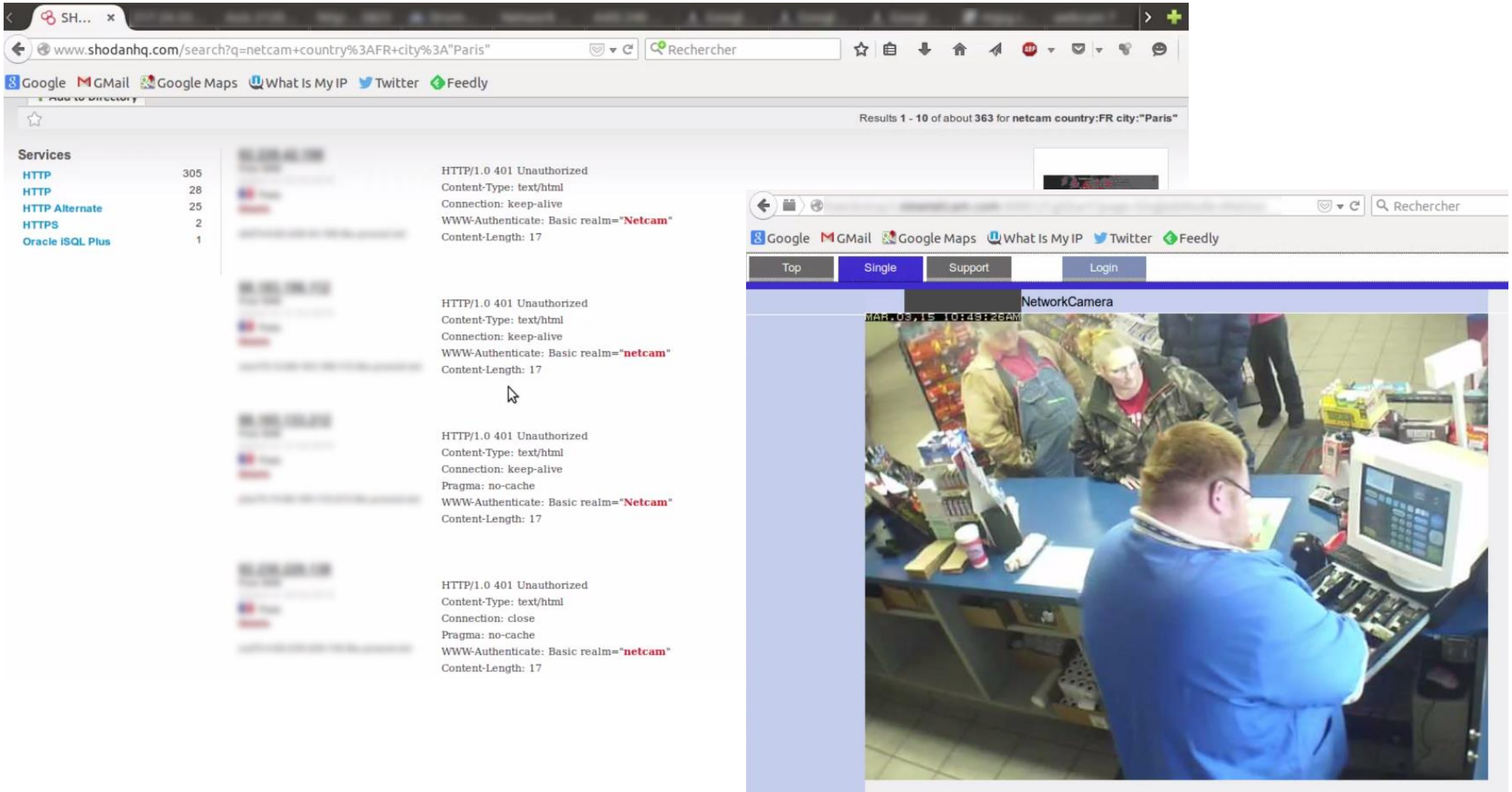
```
renaud@primelt:~/documents/confs
Launching Layer1...
Launching Layer23...
Launching TrafficMonitor...
Launching OsmoController...
[26/05/2012 10:57:11] 2081035906
[26/05/2012 10:57:13] 2081075864
[26/05/2012 10:57:14] 2081010552
[26/05/2012 10:57:15] 2081036896
5 mapped BTS!
[26/05/2012 10:57:17] 2061023004
Immediate Paging for Call ARFCN=
Immediate Paging for Call ARFCN=5
[26/05/2012 10:57:20] 208104084360583 (208, 100, 'France', 'S.F.R.') ('666', 'Downlink')
[26/05/2012 10:57:24] 208200850892724 (208, 200, 'France', 'Bouygues Telecom') ('880', 'Downlink')
[26/05/2012 10:57:24] 208201903151915 (208, 200, 'France', 'Bouygues Telecom') ('880', 'Downlink')
11 mapped BTS!
█
```

ARFCN 639

208-1-12814-51952
Orange France
France

The GSM signalling protocol is plaintext, so it’s easy to map the base stations antennas and then geolocate a device....

Spying and control of IP cameras



Results 1 - 10 of about 363 for netcam country:FR city:"Paris"

Services

HTTP	305
HTTP	28
HTTP Alternate	25
HTTPS	2
Oracle iSQL Plus	1

[redacted]

```
HTTP/1.0 401 Unauthorized
Content-Type: text/html
Connection: keep-alive
WWW-Authenticate: Basic realm="Netcam"
Content-Length: 17
```

[redacted]

```
HTTP/1.0 401 Unauthorized
Content-Type: text/html
Connection: keep-alive
WWW-Authenticate: Basic realm="netcam"
Content-Length: 17
```

[redacted]

```
HTTP/1.0 401 Unauthorized
Content-Type: text/html
Connection: keep-alive
Pragma: no-cache
WWW-Authenticate: Basic realm="Netcam"
Content-Length: 17
```

[redacted]

```
HTTP/1.0 401 Unauthorized
Content-Type: text/html
Connection: close
Pragma: no-cache
WWW-Authenticate: Basic realm="netcam"
Content-Length: 17
```

Many IP cameras are accessible from the Internet due to a lack of security: sensitive areas are made more vulnerable

« IoT Qualified Security » label

digital security

What is the difference between these two connected locks?

One protects your home, the other opens the door to intruders!

IoT Standards and safety guides

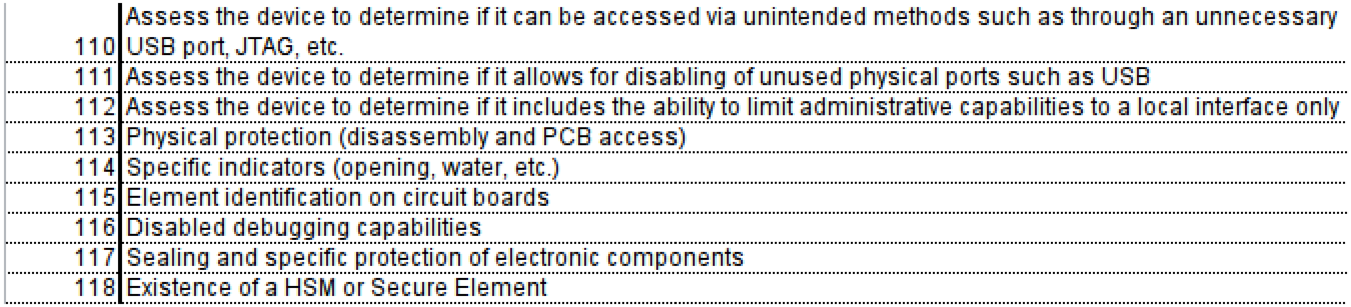
- Several initiatives :
  - Sectorial guidance on IoT security by the ENISA
  - U.S. Dept of Homeland Security Strategic Principles for securing IoT
  - NIST Special Publication 800-160
  - Projet OWASP for the IoT
  - NESCOR Standard
  - UL 2900 Standard

IoT security is on the way, but connected solutions are already largely widespread

IoT Qualified Security

IQS enables future buyers, companies or individuals to identify the security level of a connected solution according to a reliable, neutral and independent indicator.

IoT Qualified Security

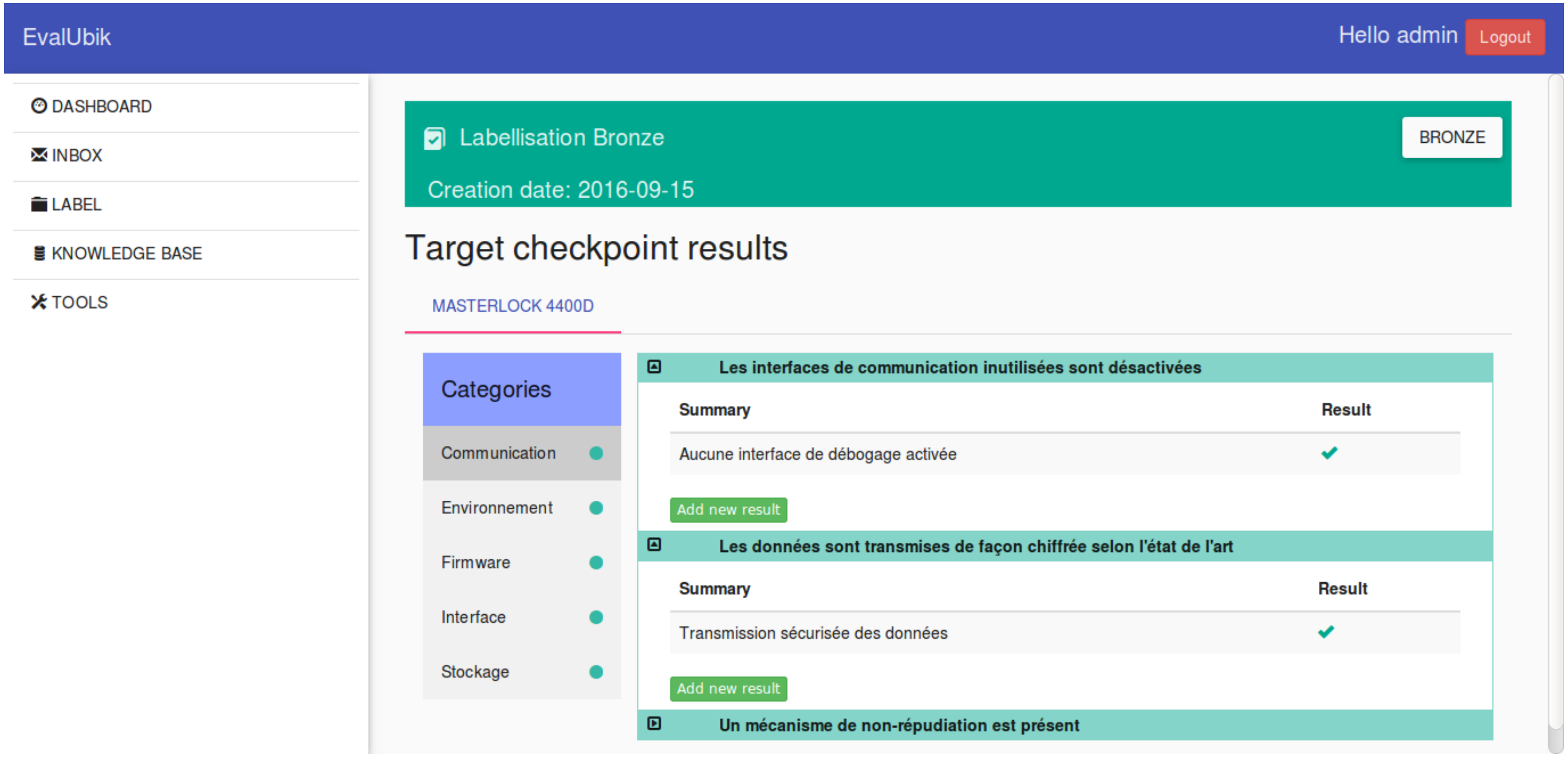


110	Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port, JTAG, etc.
111	Assess the device to determine if it allows for disabling of unused physical ports such as USB
112	Assess the device to determine if it includes the ability to limit administrative capabilities to a local interface only
113	Physical protection (disassembly and PCB access)
114	Specific indicators (opening, water, etc.)
115	Element identification on circuit boards
116	Disabled debugging capabilities
117	Sealing and specific protection of electronic components
118	Existence of a HSM or Secure Element

A repository based on SSI standards (OWASP IoT, RGS), best practices and on our feedback on the safety assessment of more than 100 IoT solutions

IoT Qualified Security

- EvalUbik, platform for evaluating the security of connected objects



Labellisation Bronze

Creation date: 2016-09-15

Target checkpoint results

MASTERLOCK 4400D

Les interfaces de communication inutilisées sont désactivées

Summary	Result
Aucune interface de débogage activée	✓

Les données sont transmises de façon chiffrée selon l'état de l'art

Summary	Result
Transmission sécurisée des données	✓

Un mécanisme de non-répudiation est présent

IoT Qualified Security

- IQS features:
  - Applicable to all sectors of the IoT
  - Repository integrating requirements of security standards, IS best practices and feedback from Digital Security
  - Two levels of labelling:
    - Standard
    - Advanced
  - Independent labelling committee provides the label for 2 years
  - Promotion of the label to companies and to the general public (2018)

Contact

digital security

Internet of Things security

info@digital.security