Cyber Security and STCs

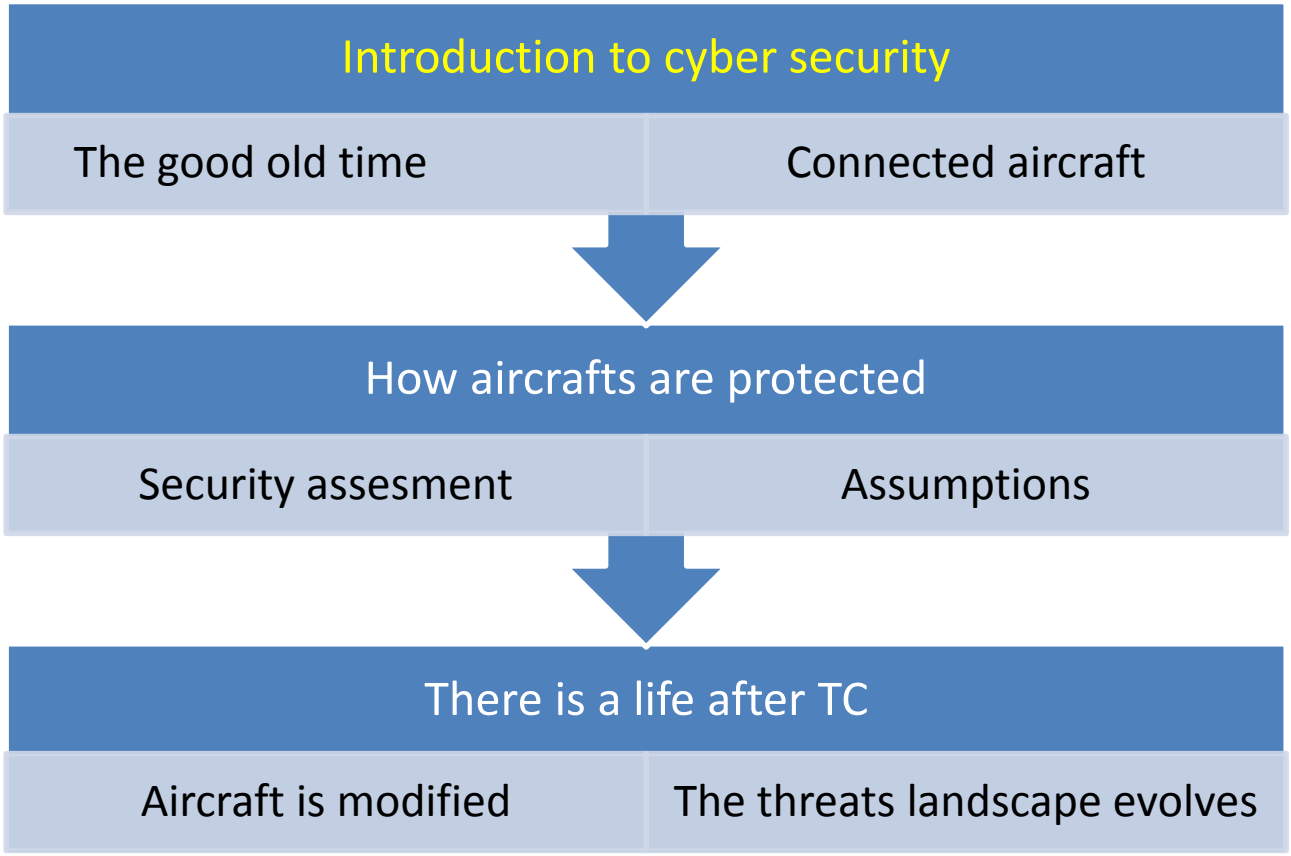
Cyrille Rosay
Senior Expert Cyber Security
Certification Directorate
EASA

STC workshop, Cologne May 2016

Your safety is our mission.

An agency of the European Union

Presentation Overview

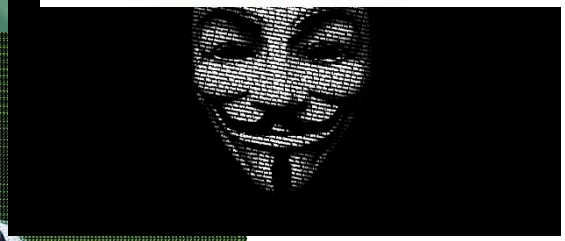


Introduction to Cyber Security

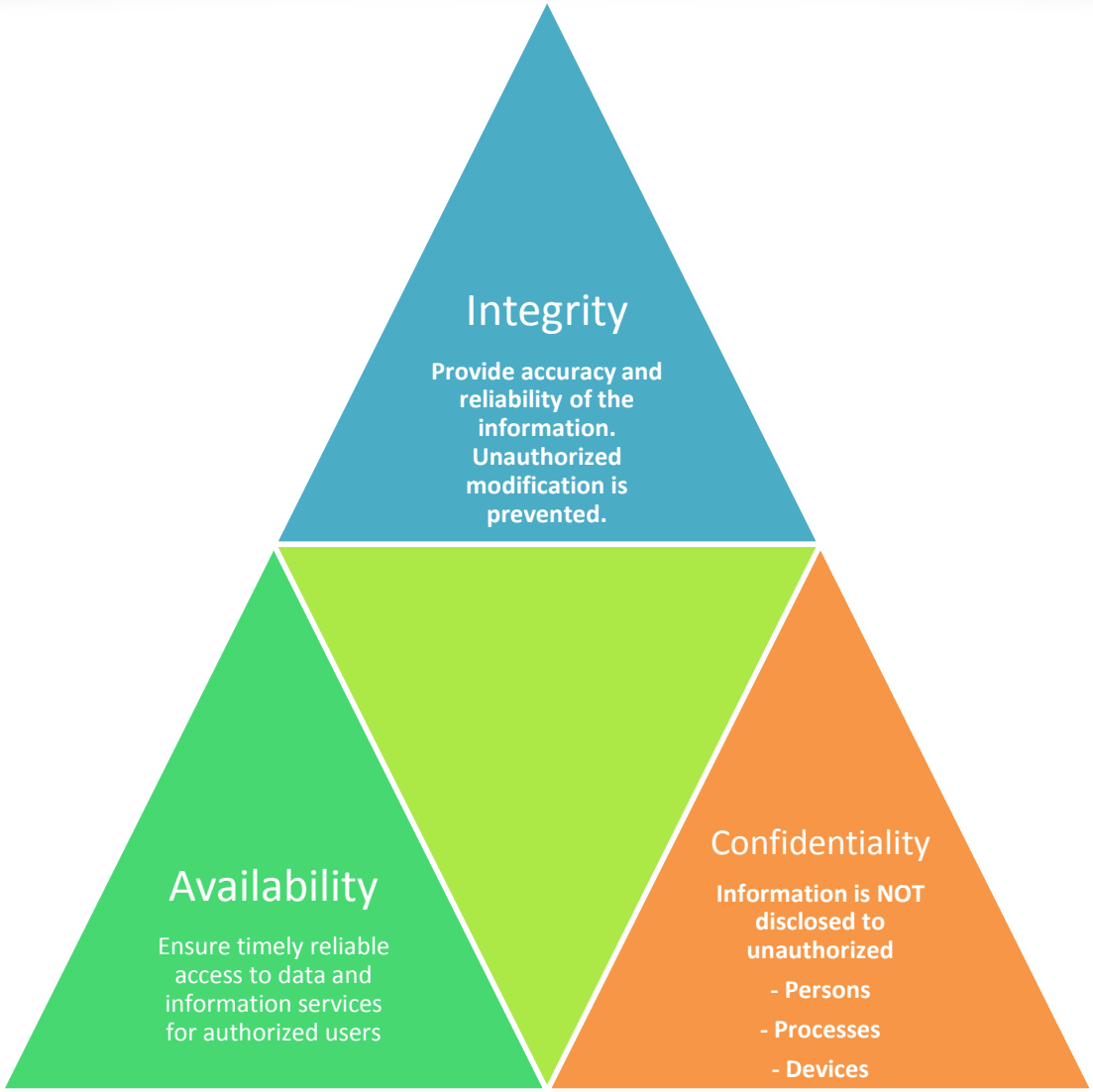
Cyber security

The ability to protect or defend the use of cyberspace from cyber attacks

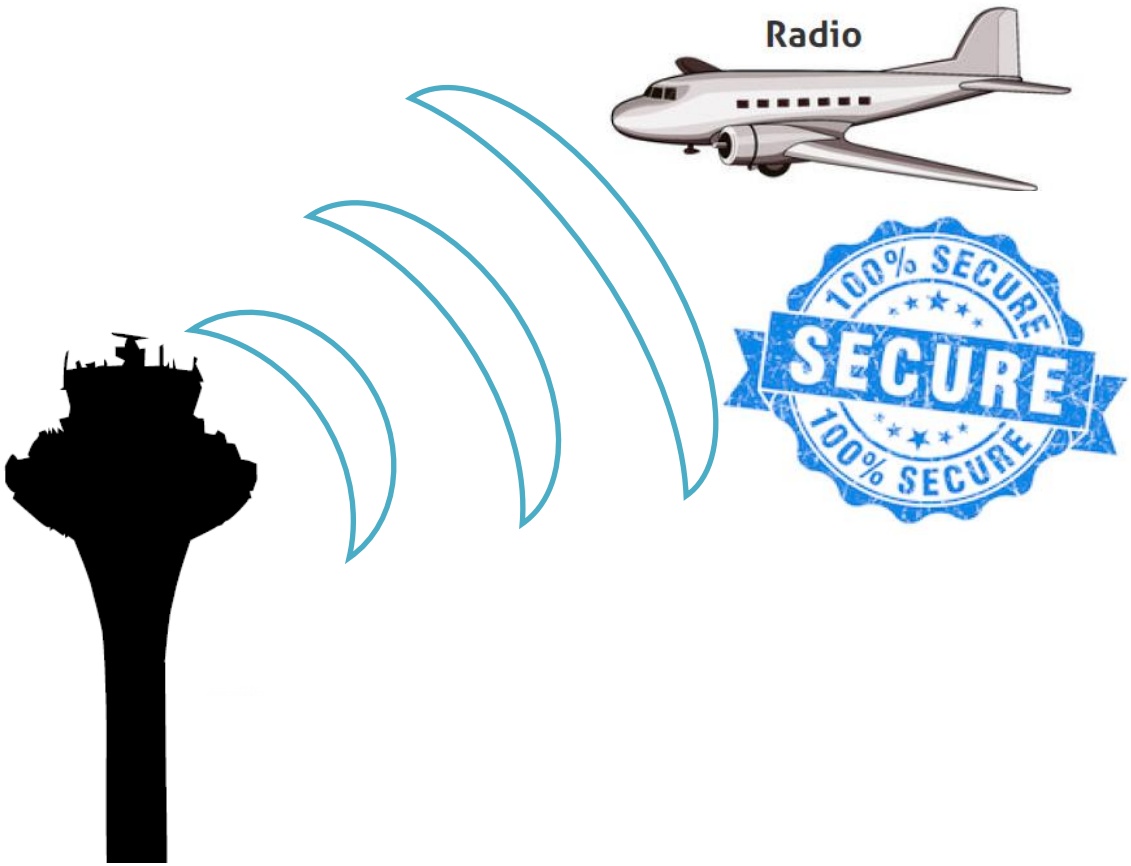
A **global domain** within the **information environment** consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.



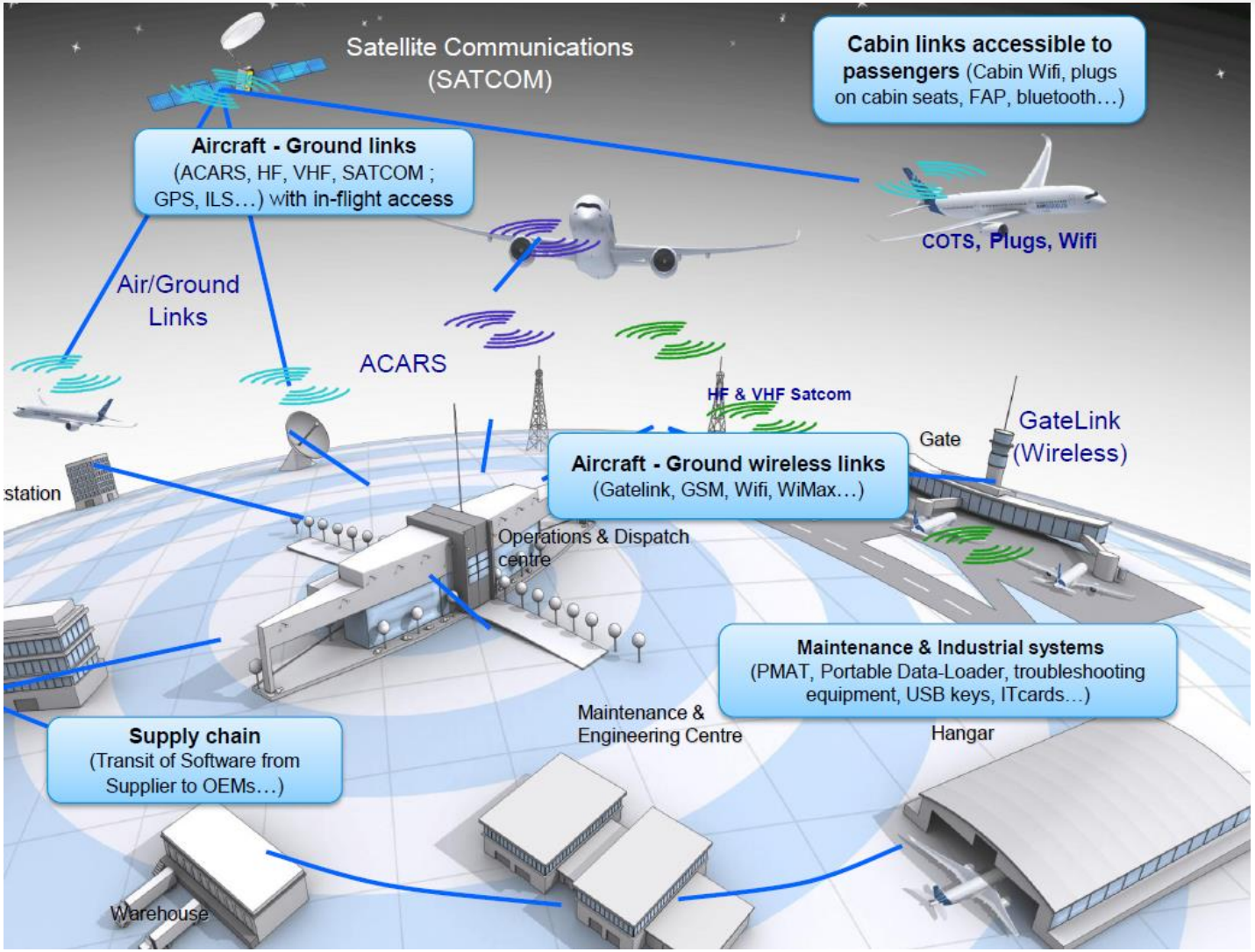
Introduction to cyber security



The good old days



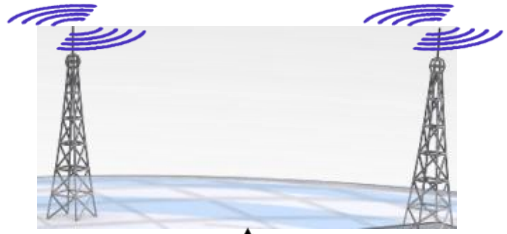
Today

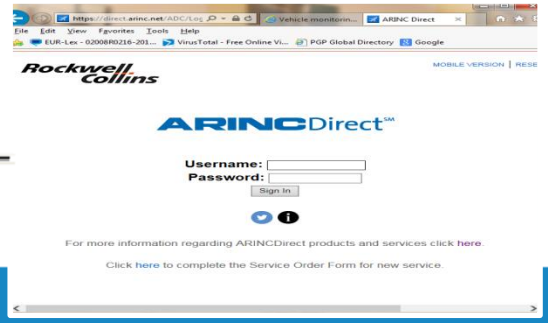


courtesy Airbus

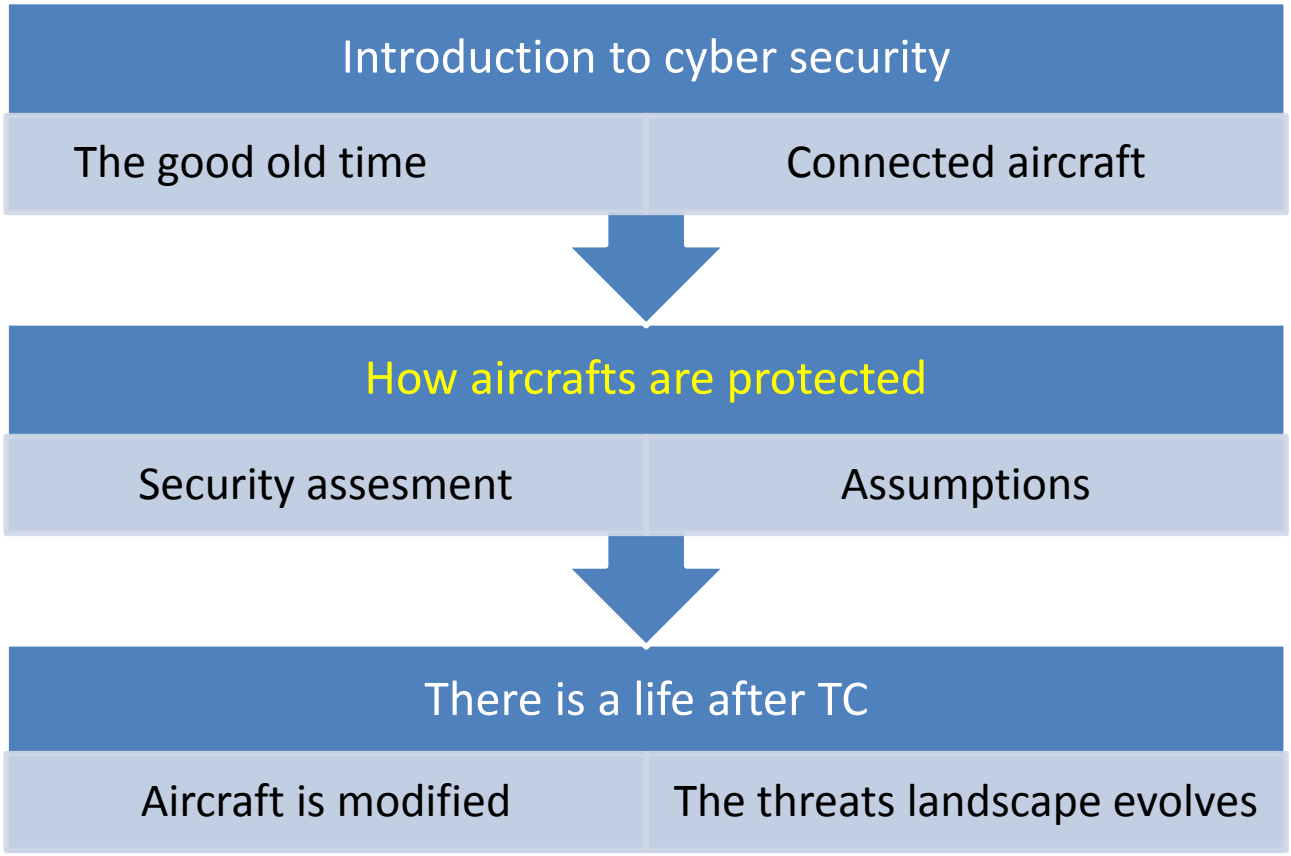
(bad) Example

- It can take 5 min for a hacker to steal operator password (X-script on portal)
- Social engineering also possible
- With it he get access to the whole airline fleet anywhere in the world, on the ground or airborne.
- He can send data directly to the plane (AOC)
- Just be imaginative…





Presentation Overview



Initial Airworthiness

Large A/C	Today, Special condition	Requires the manufacturer to define and **assess the cyber risk** on the A/C design, when needed, to mitigate and to maintain the risk to an acceptable level during operation.
	Tomorrow in CS-25	Rulemaking task 0648 started. ToR published (17/05/2016)
	Standards and AMCs	Objective is to recognize and reference the industry standards (EUROCAE). Issue to be solve by the industry on difference between RTCA and EUROCAE
General Aviation	Low end: nothing asked. Industry voluntary basis	GAMA GA initiative to address cyber security in GA is well perceived by EASA. Candidate for an ASTM standard in F44?
	PAX > 19	Today case by case basis.Asking usually via a CAI (Certiciation Action Item) to review the design with the cyber security scope. Sometime followed by a SC.

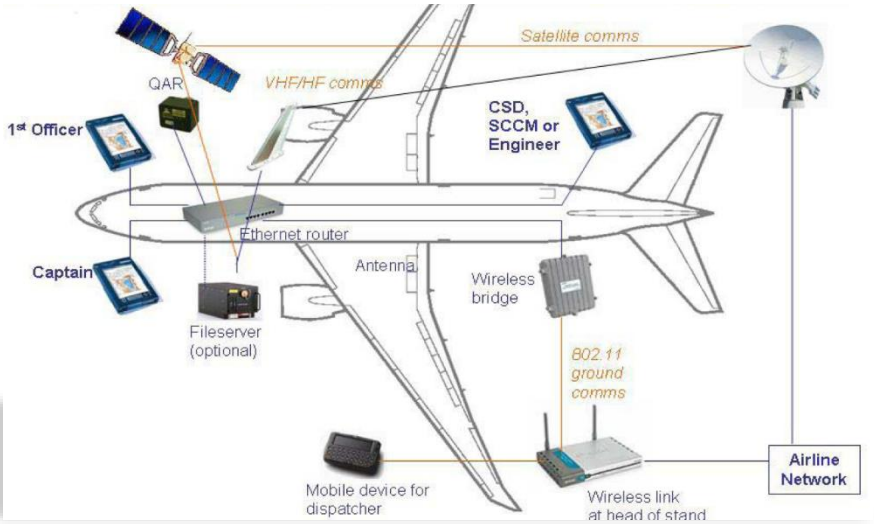
Cyber Security Risk Assessment

Purpose is to evaluate the security risk of an aircraft or system subject to unauthorized interference with its systems

Risk is defined by

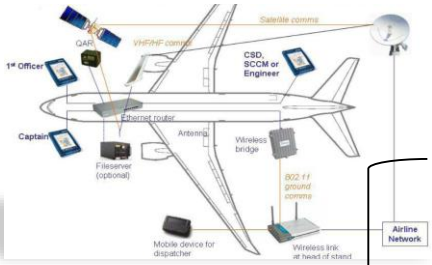
1. **Severity of the effect of the Threat Condition**
2. **Difficulty to attack**

Risk = Severity /Difficulty



Src ED 202A

Case study: Air Mgt. Syst. (src ED 203)



Functions

- Provide Cabin Pressurization
- Provide Aircraft Structural Integrity
- Provide Aircraft status
- Troubleshooting Support

Assets

- Press. Contr. Field Loadable S/W
- Press. Contr. Configuration files

Interfaces

- Physical I/F to Maintenance GSE
- Logical I/F to Bleed System

Security scope

Failure conditions

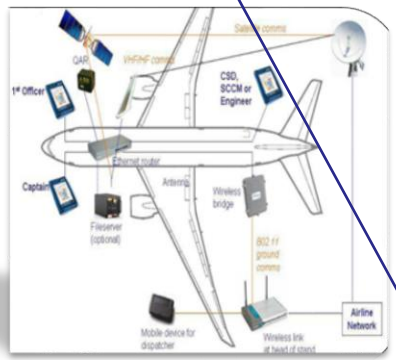
	Failures	Attribute	Flight Phase	Hazzard Classification
F1	Loss of Pressurization	Availability	Airborne	Catastrophic
F2	Loss of Structural Integrity	Availability	Airborne	Catastrophic
F3	Loss of Aircraft status	Availability	Airborne	Major
F4	Loss of Troubleshooting Support	Availability	On Ground	No safety effect

Threat conditions

	Threat Condition	Attribute	Flight Phase	Failure	Hazzard Classification
TC1	Communication interrupted due to malware infection	Availability	Airborne	F1	Catastrophic
TC2	Communication interrupted due to malware infection	Availability	On Ground	F1	No safety effect
TC3	Counterfeit LRU installation	Integrity	Airborne	F1	Catastrophic
TC4	Misleading commands to bleed due to S/W corruption	Integrity	Airborne	F1	Catastrophic

General process (ED 202)

Planning
(Certification plan)



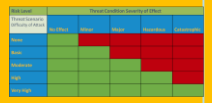
concept

Integral processes

Safety
DAL
Process assurance
Conf. mgnt.
Cert. Liaison
V&V
… (see ARP 4754)

Security Assurance
- development
- effectiveness

Security Risk assessment



OK

Certification Summary

Development processes

Functions definition

architecture

Functions allocation

System integration

Security development
- Architecture
- Measures
- Guidances

Risk Acceptability Matrix

safety

Risk Level	SEVERITY				
PROBABILITY (Likelihood)	No Effect	Minor	Major	Hazardous	Catastrophic
Frequent					
Probable					
Remote					
Extremely Remote					
Extremely Improbable					

security

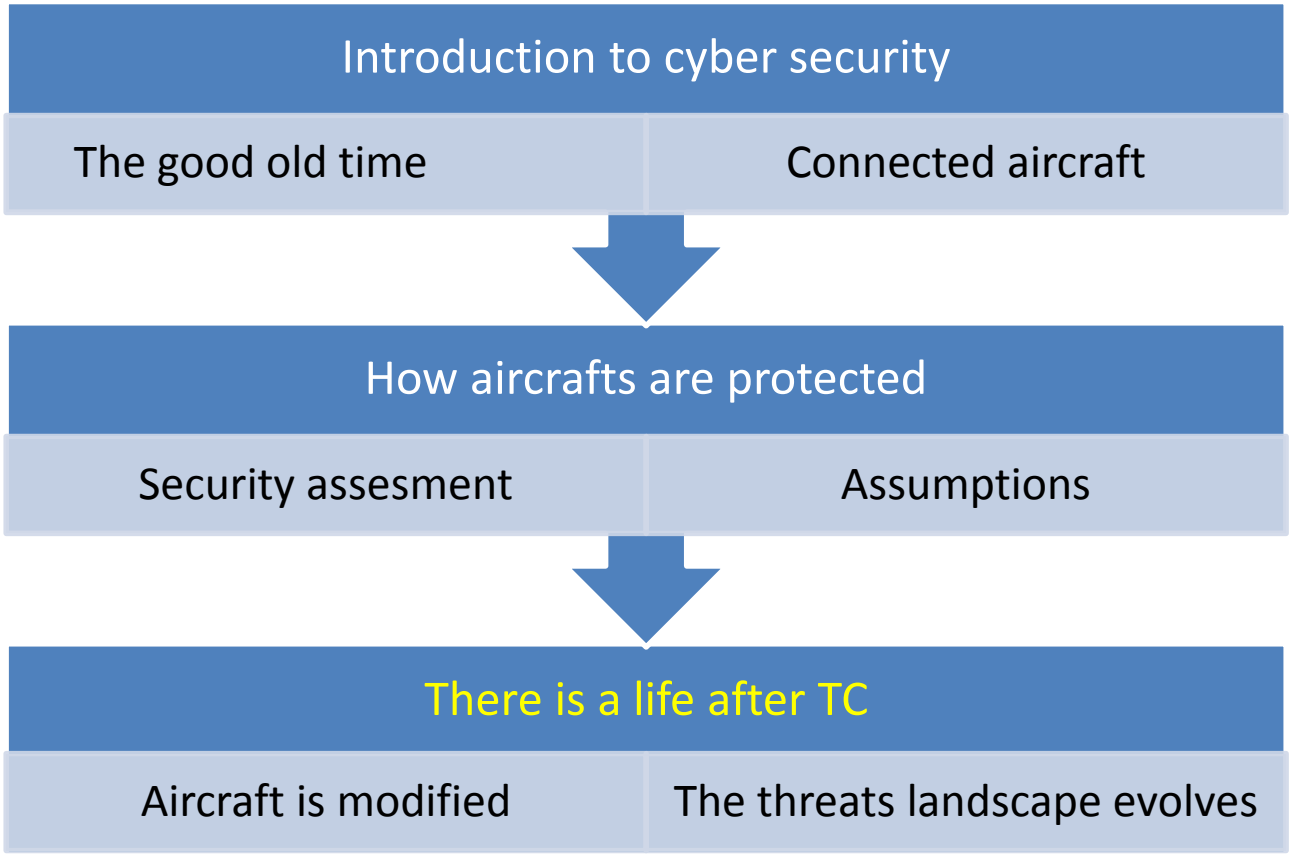
Risk Level	Threat Condition Severity of Effect				
Threat Scenario Difficulty of Attack	No Effect	Minor	Major	Hazardous	Catastrophic
None					
Basic					
Moderate					
High					

Needs to modify the architecture to reduce the safety impact

So better think security from start!

Make the scenario more difficult to succeed: add protection (eg signing sw load), or operational constraints (eg. access to the aircraft vs remote loading)

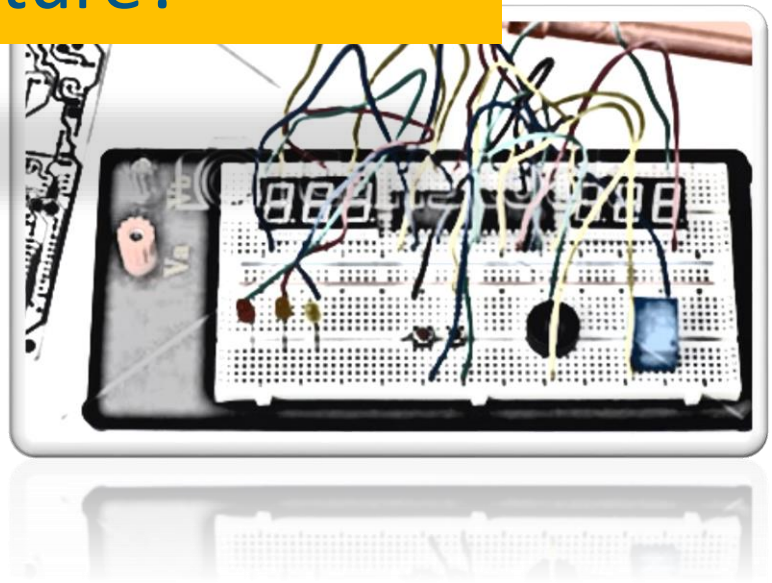
Presentation Overview



Aircraft modification

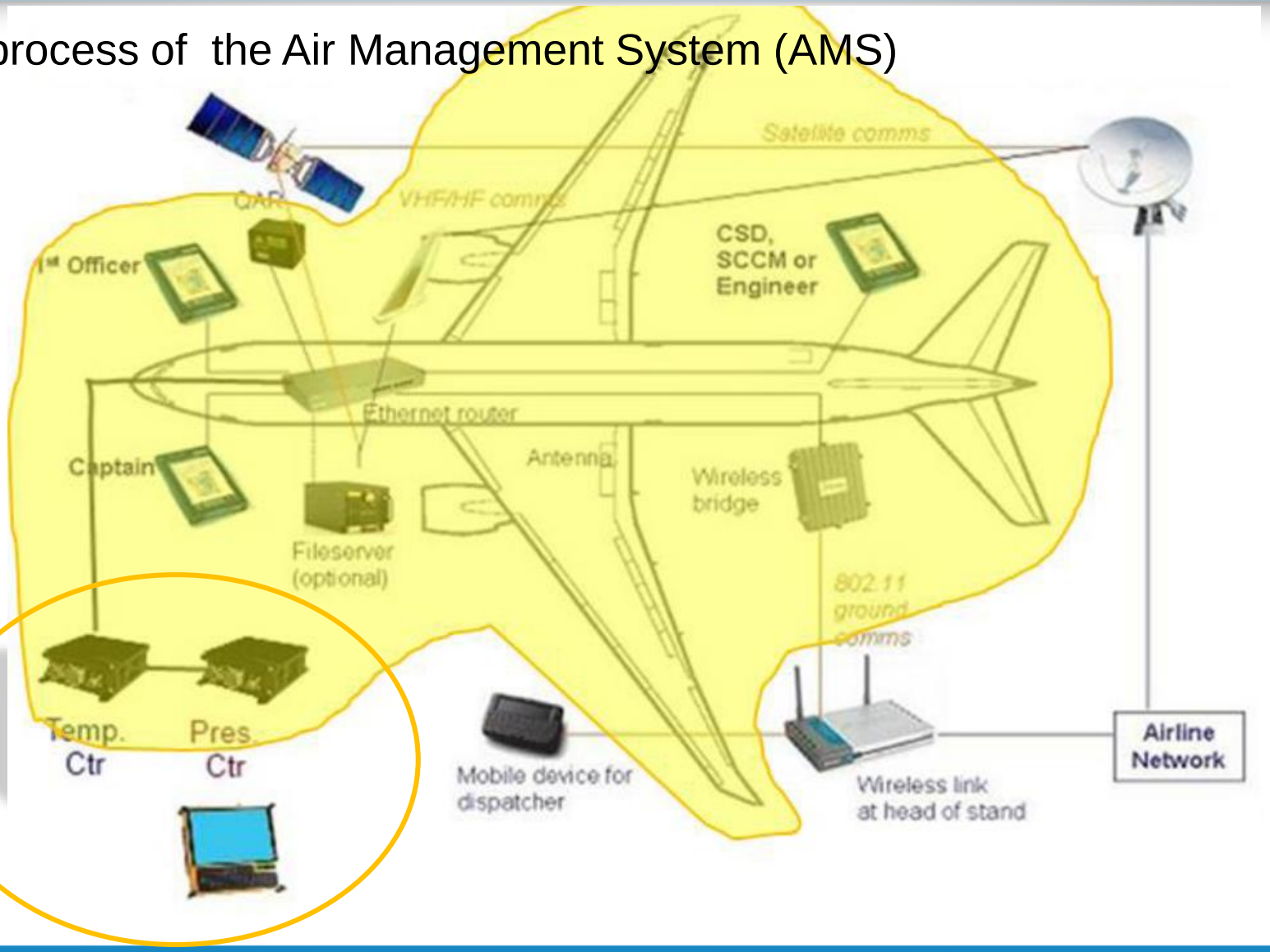
Issue:

How can we maintain the security effectiveness when modification are made on existing architecture?



Case study

update process of the Air Management System (AMS)



What does the rule say?

21.A.113 Application for a supplemental type-certificate

(a) An application for a supplemental type-certificate shall be made in a form and manner established by the Agency.

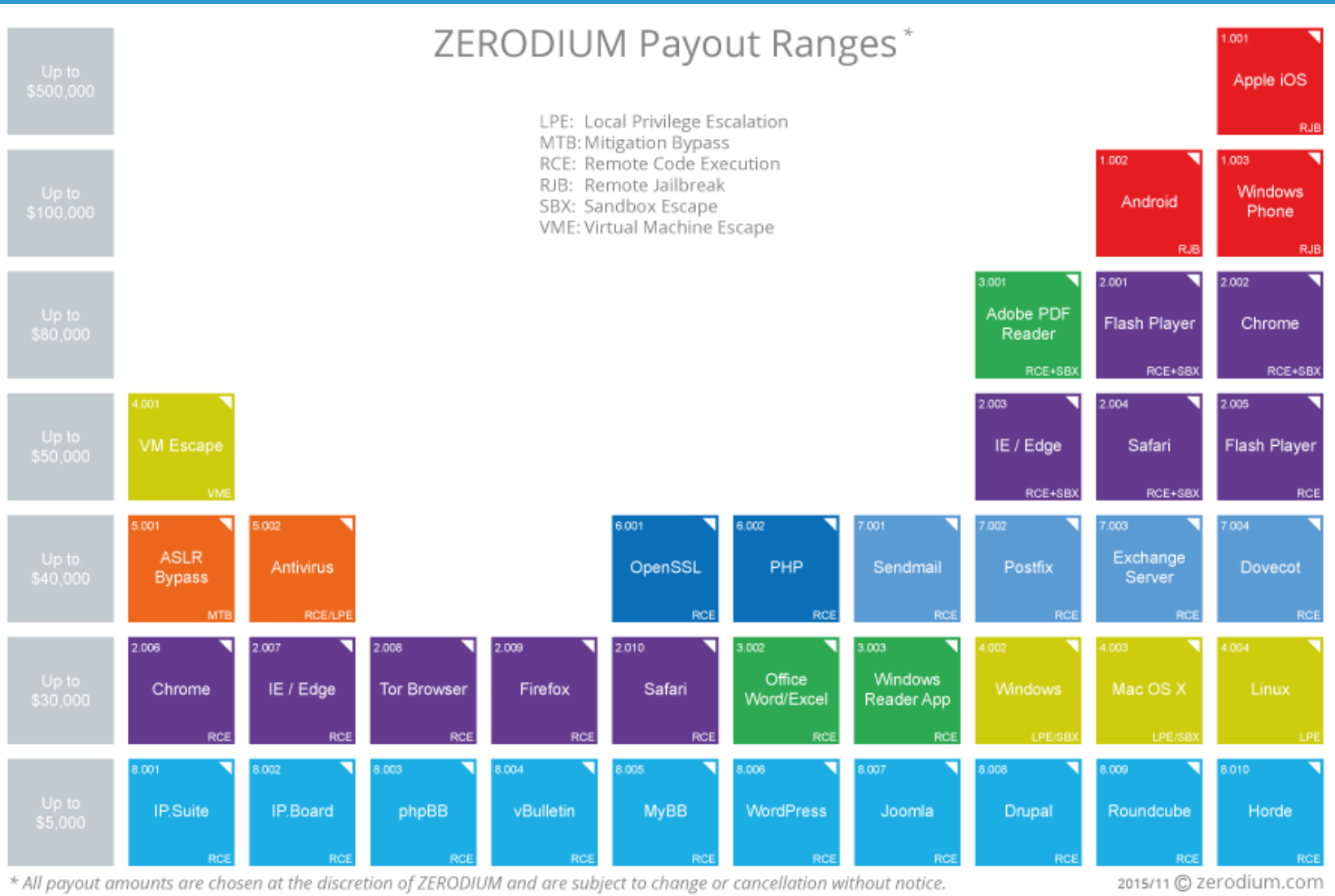
(b) An application for a supplemental type-certificate shall include the descriptions and identification, and changes to the operational suitability data required by point 21.A.93. In addition, such an application shall include a justification that the information on which those identifications are based is adequate either from the applicant's own resources, or through an arrangement with the type-certificate holder.

How?

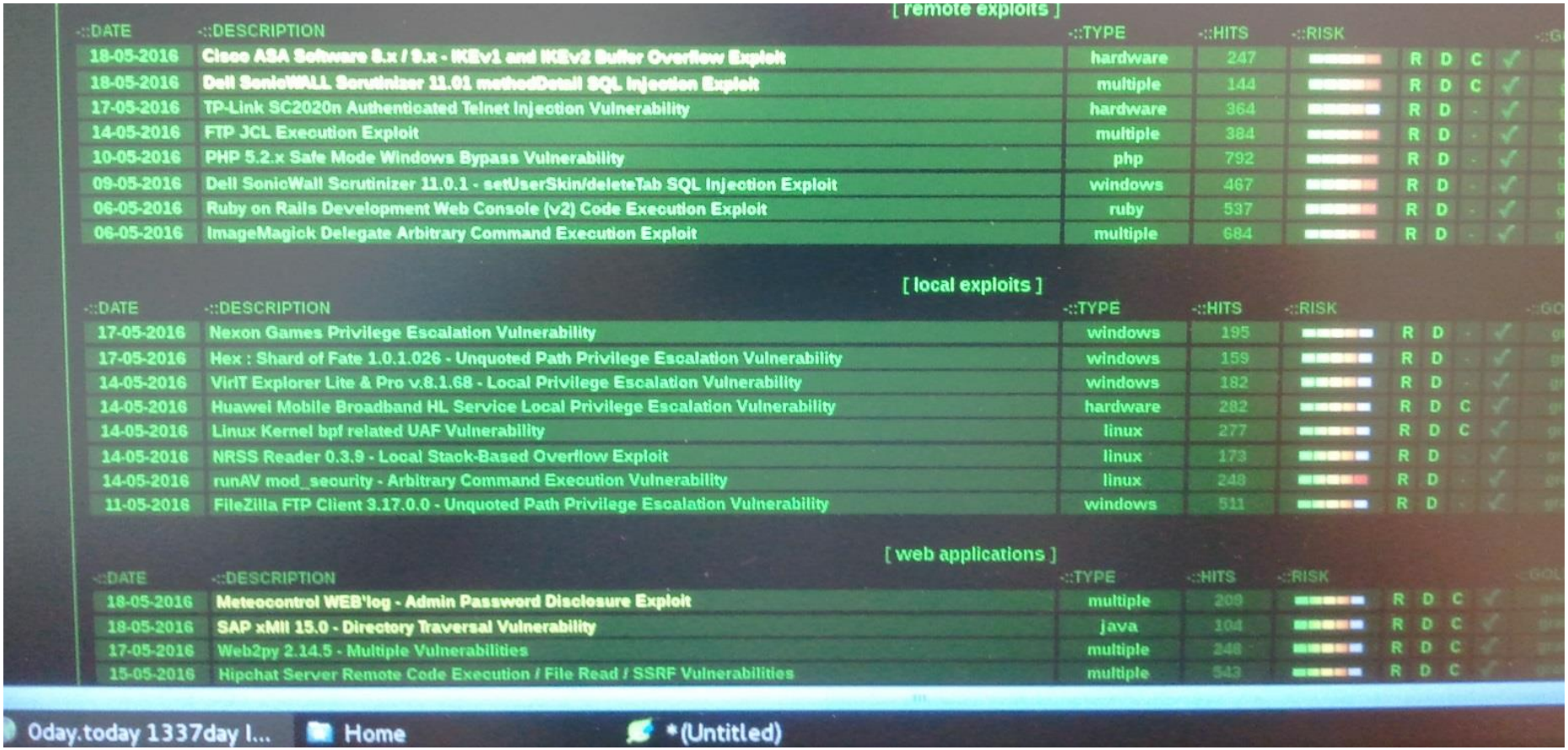
- security boundaries are available
  - Should allow modification without jeoparding existing A/C security efficiency

- STC applicant get from OEM the necessary security information to perform the change, including operational security handbook and ICA
  - Implies some binding constraints between OEM and STC applicant

Risk evolution



DW marketplace



[remote exploits]

::DATE	::DESCRIPTION	::TYPE	::HITS	::RISK
18-05-2016	Cisco ASA Software 8.x / 9.x - IKEv1 and IKEv2 Buffer Overflow Exploit	hardware	247	
18-05-2016	Dell SonicWALL Scrutinizer 11.01 methodDetail SQL Injection Exploit	multiple	144	
17-05-2016	TP-Link SC2020n Authenticated Telnet Injection Vulnerability	hardware	364	
14-05-2016	FTP JCL Execution Exploit	multiple	384	
10-05-2016	PHP 5.2.x Safe Mode Windows Bypass Vulnerability	php	792	
09-05-2016	Dell SonicWall Scrutinizer 11.0.1 - setUserSkin/deleteTab SQL Injection Exploit	windows	467	
06-05-2016	Ruby on Rails Development Web Console (v2) Code Execution Exploit	ruby	537	
06-05-2016	ImageMagick Delegate Arbitrary Command Execution Exploit	multiple	684	

[local exploits]

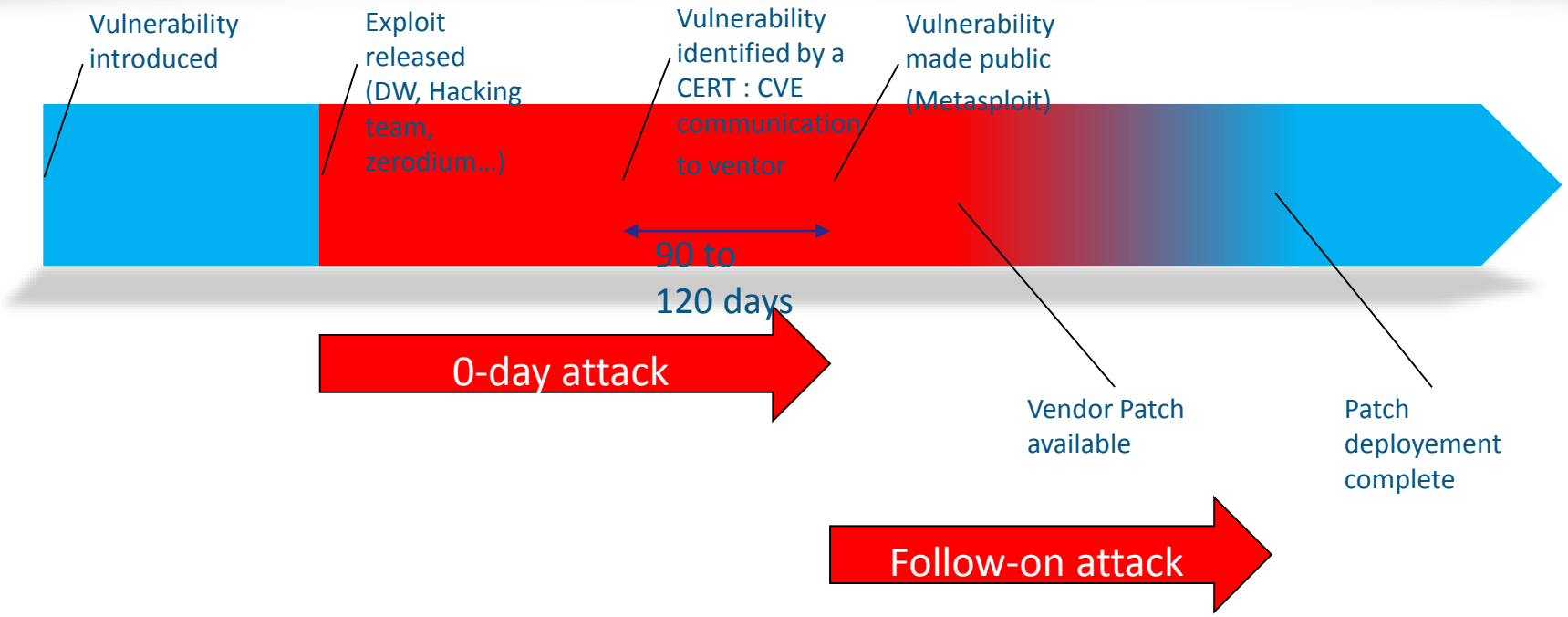
::DATE	::DESCRIPTION	::TYPE	::HITS	::RISK
17-05-2016	Nexon Games Privilege Escalation Vulnerability	windows	195	
17-05-2016	Hex : Shard of Fate 1.0.1.026 - Unquoted Path Privilege Escalation Vulnerability	windows	159	
14-05-2016	VirIT Explorer Lite & Pro v.8.1.68 - Local Privilege Escalation Vulnerability	windows	182	
14-05-2016	Huawei Mobile Broadband HL Service Local Privilege Escalation Vulnerability	hardware	282	
14-05-2016	Linux Kernel bpf related UAF Vulnerability	linux	277	
14-05-2016	NRSS Reader 0.3.9 - Local Stack-Based Overflow Exploit	linux	173	
14-05-2016	runAV mod_security - Arbitrary Command Execution Vulnerability	linux	248	
11-05-2016	FileZilla FTP Client 3.17.0.0 - Unquoted Path Privilege Escalation Vulnerability	windows	511	

[web applications]

::DATE	::DESCRIPTION	::TYPE	::HITS	::RISK
18-05-2016	Meteocontrol WEB'log - Admin Password Disclosure Exploit	multiple	209	
18-05-2016	SAP xMII 15.0 - Directory Traversal Vulnerability	java	104	
17-05-2016	Web2py 2.14.5 - Multiple Vulnerabilities	multiple	248	
15-05-2016	Hipchat Server Remote Code Execution / File Read / SSRF Vulnerabilities	multiple	543	

Oday.today 1337day l... Home *(Untitled)

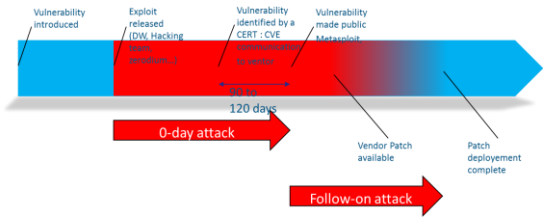
0-day timeline



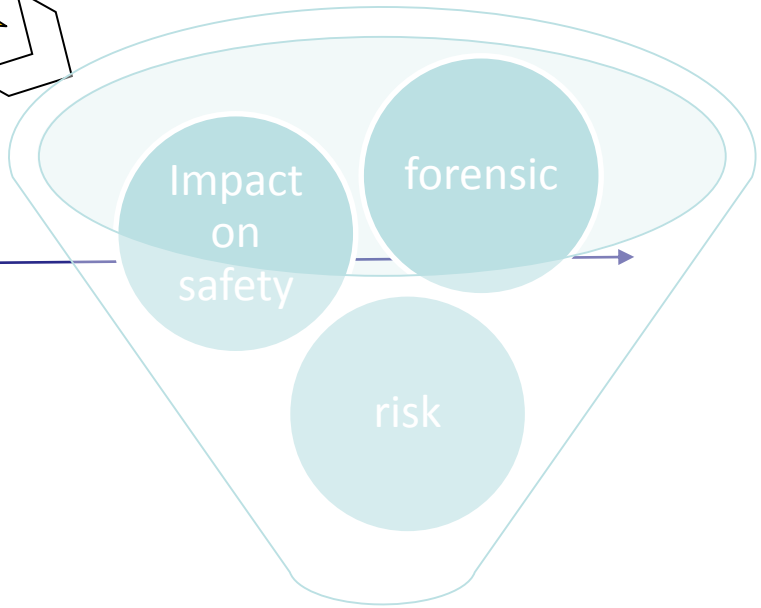
Questions:

- who, in the aviation world is looking at vulnerabilities, CVEs, patches?
- Which vendors in the aviation world is developing security patch?
- What do you think of the timeline, in particular the follow-on attack window?

0-day timeline and the occurrence reporting



Months later



solution

EASA
European Aviation Safety Agency

Questions?

Your safety is our mission.

An agency of the European Union