



How we pentested one of the largest EU international airport... and what we found.



Raoul «Nobody» Chiesa

Hackito Ergo Sum 2015
Paris, 29-30 October

Agenda

- Introductions
- (different) Scenarios
- SCADA, etc
- RFQ mistakes, other stuff
- Specific SCADA issues (SOVEMA case study)
- What we found while pentesting
 - Network
 - Internal
 - Wi-Fi
 - Fully p0wning
 - Evidences, Pictures, Fun
- Conclusions
- Reading room
- Q&A



Disclaimer

The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.

The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.

Quoted trademarks belongs to **registered owners**.

The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the views of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers** and **Swiss Web Academy** ones.

Contents of this presentation **may not be quoted or reproduced but partially (10%)**, provided that the **source of information is acknowledged**.



Introductions

Raoul «Nobody» Chiesa

- President, Founder, **The Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Special Senior Advisor on Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**



The Security Brokers

- We deal with **extremely interesting, niche topics**, giving our strong know-hows gained from **+20 years of field experience** and from our **+30 experts**, very well known all over the world in the **'Information Security** and **Cyber Intelligence** markets.
- Our **Key Areas** of services can be resumed as:
 - **Proactive Security**
 - With a deep specialization on TLC & Mobile, SCADA & IA, ICN & **Trasportation, Space & Air**, Social Networks, e-health, [...]
 - **Post-Incident**
 - Attacker's profiling, Digital Forensics (Host, Network, Mobile, GPS, etc..), Trainings
 - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
 - On-demand «Ninja Teams»
 - Security Incident PR Handling & Management
 - **Psychological, Social and Behavioural aspects (applied to cyber environments)**
 - **Cybercrime Intelligence**
 - Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, Technical & Operational support towards CERTs and LEAs/LEOs,[...]
 - **Information Warfare & Cyber War** (only for MoDs)
 - 0-day and Exploits – Digital Weapons
 - OSINT

Why I'm here?

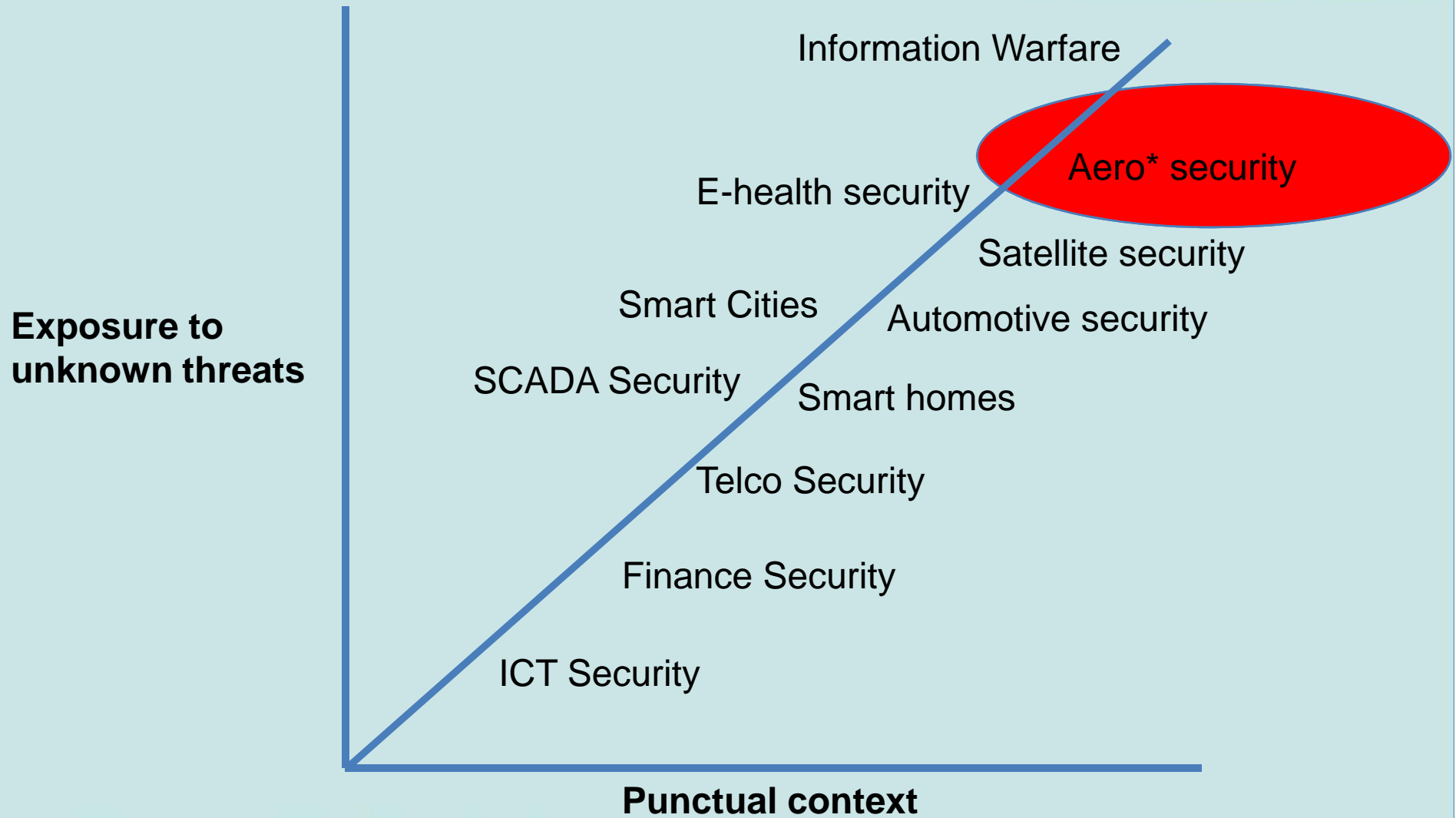
- Because I don't want to see this when it's about Air Transportation ☹️



The scenario

- Hardware and Software vendors for the Aero* market they sell **platforms, applications and systems** which, typically, are extremely **insecure**.
 - (being more polite) we may say that, at least, the **Information Security aspects** are **not on the top of their list** 😊
- **Operators** from the **transportation environment** do not have (once again: typically, giving some rare exceptions) a **correct vision**, and **enough understanding**, of those **new challenges** linked with **ICT security**.

The scenario



The (key?) issue

- Airport's network = an ISP
 - They (re)sell «services», «data transportation»
 - Think about SITA, the POS at the duty free shops, those “interlinks” with Law Enforcement (Immigration, Customs, etc...), whatever.
 - Ah, the «free WiFi» thing! 😊

Aircraft Security

- The (ethical) hacking community discovered this long time ago:
 - Hugo Teso (DE) – we'll see this later
 - Renderman (CA)
 - Ruben Santamarta (ES)
 - Myself (IT)
 - More security researchers
 - See excerpts on next slides



+



=



Hackers + Airplanes

No Good Can Come Of This

Confidence 2012
Brad "RenderMan" Haines, CISSP
www.renderlab.net
render@renderlab.net
Twitter: @lhackedWhat

RFQ mistakes

- **Scope (ToE)**
 - Missed key areas to be tested
 - Not asking for a specific pentesting methodology
 - Pretending to get “everything”
- **Budget**
 - «We want everything»: means, average 300K/400K EUR budget (at least, if you want my guys :)
 - «our budget is 100K EUR»
 - WTF!
 - We had to find a «compromise»....
 - My team badly wanted to pentest an airport!
 - We selected by Operational and Business priorities the ToE

Same issue...

- Happened with [REDACTED] ([REDACTED])
- I may say, that was *even worse*:
 - Wrong «vision»
 - 100% focused on ISO/IEC (correct, but.... That's the **theoretical** assessment ☹)
 - Poor budget (it's wasted on **useless projects & MKTG**)
 - **Not enough knowledge** on IT Security issues
 - Smth more I just can't public state, sorry!

I travel a lot...

- **Air China Boeing 777** ([REDACTED] multimedia entertainment system)
 - A Wi-Fi access point which shouldn't be there (on da plane!)
 - Default password of a Chinese brand multimedia server (to upload Chinese movies)
 - (possible) mass “video file substitution”, resulting in all pssengers getting on their seat's displays a nice porno movie (Rocco Siffredi rulez! ;)
- **Different airports in the world:** getting «the access», then straight into Airport's WAN
 - **In a Caribbean island:** access to Passport control system, POS for the shops, X-ray machines, etc...
 - **In India** (Mumbai airport): a RJ-45 plug at the men's toilet (LOL)
 -



Video: Specific SCADA/ICS issues



Source: Raoul's penetration testing team (Red Team)

What is « SCADA »?

- “Supervisory Control and Data Acquisition”
- It’s the monitoring branch of an **automated infrastructure** that decides *what to do* on the basis of *what is happening* (event driven).
- Basically, we are talking about **Industrial Automation**, that is a **reality since many years**.
- The market though is **migrating infrastructures**: from **proprietary, obscure and isolated systems**, towards **standard, documented and connected** ones.
- **Often**, among this SCADA-related users, **we find National Critical Infrastructures...**

Critical Infrastructures

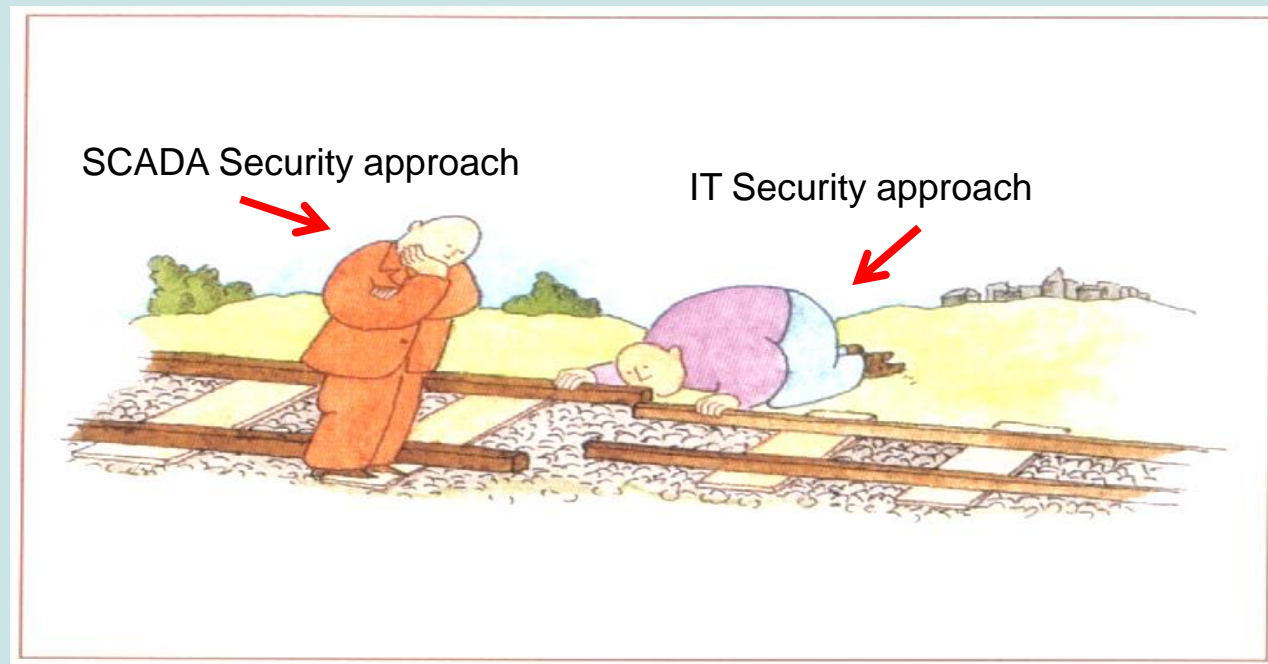
- Many SCADA infrastructures are **responsible for:**

**Power and Nuclear plants, Gas, Oil,
Water distribution, **Transports****

- **Nevertheless**, when talking about SCADA & IT Security, **true life** taught us that **lack of communication and Information Sharing**, made up more panic than real, huge incidents.

IT Security VS SCADA Security

- ❑ A **key issue** when comparing the InfoSec approach and the SCADA-related environments approach is referred to the **CIA paradigm**.
- ❑ This is the **main reason** why it is pretty **hard** to “talk” about Information Security, with our standard IT Security approach.
- ❑ The following comics should **give you the idea** of what I’m talking about ;)

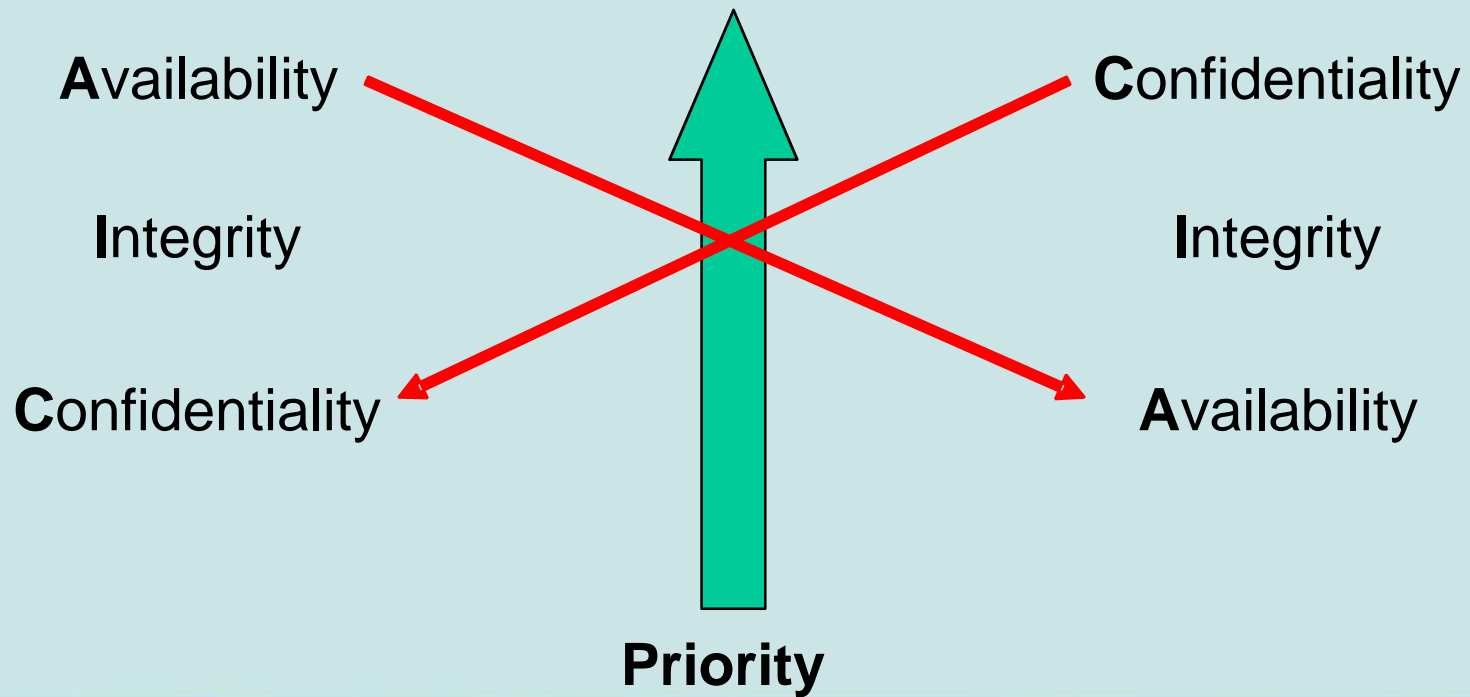


The CIA paradigm

C-I-A : Comparison of Objectives

Manufacturing and Control Systems

Traditional IT Systems



Attack techniques

- ❑ Basically, attacking SCADA-related infrastructures does **not involve** “high-level” **hacking** techniques.
- ❑ In fact, these attack techniques **do not differ that much** from “standard” IT environments attacks.
- ❑ Also, they **mainly relay** on “old-school” hacking techniques, such as:
 - ✓ General “old school hacking” (password guessing, brute forcing, ...)
 - ✓ Scanning (TCP/IP port scanning, wardialing, X.25 scanning, etc..)
 - ✓ Eavesdropping, data flows dissection/assembling and reverse engineering
 - ✓ Exploiting known and unknown vulnerabilities
 - ✓ DoS attacks
 - ✓ Web applications hacking

Insecurity by Design: Advanced attack scenarios

- After +10 years security testing on SCADA-related environments, the feedback is that it just looks like **SCADA vendors don't care about Information Security**, especially when **not implementing** those **de-facto standards** such as OSSTMM and OWASP, not mentioning ISO/IEC 27001...or a nice **S-SDLC!!!**
- The “defective by design”™ joke come from the following issues:
 - ✓ No authentication
 - ✓ No local data encryption
 - ✓ No encryption on network traffic
 - ✓ No logs management (at all)
 - ✓ Unstable/uncomplete embedded TCP/IP stacks (think about the SOVEMA case study)

NOTE: often, these have been “**needings**”, not “**limitations**” ...

Air Traffic Control Security

- Back in **2013**, I was attending a presentation at **Hack in the Box** in Amsterdam by Hugo Teso



Air Traffic Control Security

Attack Overview

DISCOVERY:

- » ADS-B

INFO GATHERING:

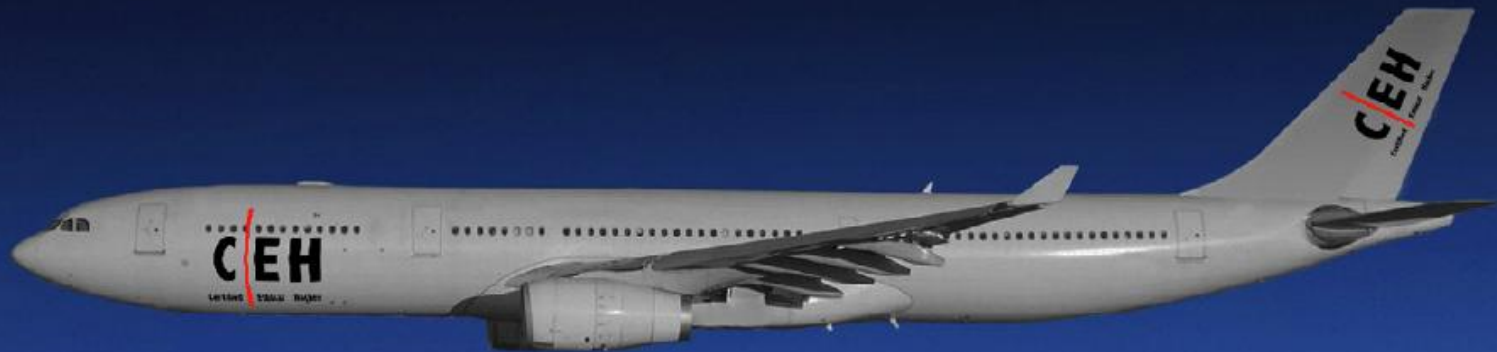
- » ACARS

EXPLOITATION:

- » Via ACARS
- » Against on-board systems vulns.

POST-EXPLOITATION:

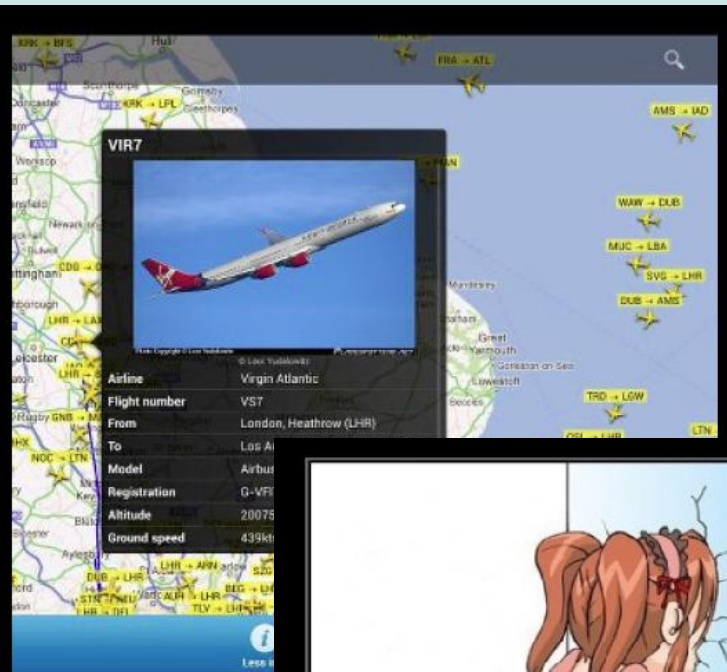
- » Party hard!



Air Traffic Control Security (ADS-B)

ADS-B 101

- Automatic Dependent Surveillance-Broadcast
- Radar substitute
- *Position, velocity, identification, and other ATC/ATM-related information.*
- ADS-B has a data rate of 1 Mbit/sec.
- Used for locating and plotting targets



FACEWALL

WHEN A FACEPALM IS NOT ENOUGH

ADS-B Security

- None at all
- Attacks range from **passive attacks** (eavesdropping) to **active attacks** (message jamming, replaying, injection).
- Target selection
 - » Public Data
 - » Local data (SDR*)
 - » Virtual Aircrafts

Air Traffic Control Security (ACARS)

ACARS 101

- ➔ Aircraft Communications Addressing and Reporting System
- ➔ Digital datalink for **transmission of messages between aircraft and ground stations**
- ➔ Multiple data can be sent from the ground to the A/C *
- ➔ Used for passive “OS fingerprinting” and plotting targets

ACARS Security

- ➔ None at all
 - » sometimes monoalphabetic ciphers
- ➔ Detailed flight and Aircraft information
 - » Public DB
 - » Local data (SDR)
 - » Virtual Aircrafts
- ➔ Ground Service Providers
 - » Two main players
 - » Worldwide coverage

Air Traffic Control Security (FMS)

FMS 101



The image is a composite of three parts. On the left is a cockpit display showing various flight parameters: speed (SPD), lateral navigation (LNAV), vertical navigation (VNAV), and path (PTH). The central display shows a command (CMD) window with a vertical scale from 200 to 300. Below it is a heading scale from 200 to 300. On the right is a physical FMS unit, a black rectangular device with a handle. In the center is a Control Display Unit (CDU) or MCDU, which is a control panel with a screen and a keyboard. The screen displays 'ACT RTE LEGS' with a list of waypoints: RBV, LOBES, COPEL, HOLD AT COPEL, and BYRDD, each with associated distance and flight level information.

- ✈ Flight Management System typically consists of two units:
 - » A computer unit
 - » A control display unit
- ✈ Control Display Unit (CDU or MCDU) provides the primary human/machine interface for data entry and information display.
- ✈ FMS provides:
 - » Navigation
 - » Flight planning
 - » Trajectory prediction
 - » Performance computations
 - » Guidance

Air Traffic Control Security (FMS)

FMS

- ✈ Goal: Exploit the FMS
 - » Using ACARS to upload FMS data
 - » Many different data types available
- ✈ Upload options:
 - » Software Defined Radio
 - » Ground Service Providers
- ✈ The path to the exploit:
 - » Audit aircraft code searching for vulnerabilities
- ✈ We use a lab with virtual airplanes
 - » but real aircraft code and HW



Air Traffic Control Security (FMS)

MY WALLET IS LIKE AN ONION

Aircraft Hardware and Software

- ✈ The good old...
 - » eBay!!
- ✈ Russian scrapings
 - » You name it
- ✈ Loving salesman
 - » Value-added products
- ✈ Third party vendors
 - » /wp-admin... Sigh
- ✈ Resentful users or former employees

WHEN I OPEN IT
I START TO CRY

Air Traffic Control Security (FMS)

Honeywell offers tools using actual aircraft FMS code...for your genuine training experience

Honeywell's PC-FMS™ free play software provides simulation based on actual flight code software.



Rockwell Collins

Building trust every day



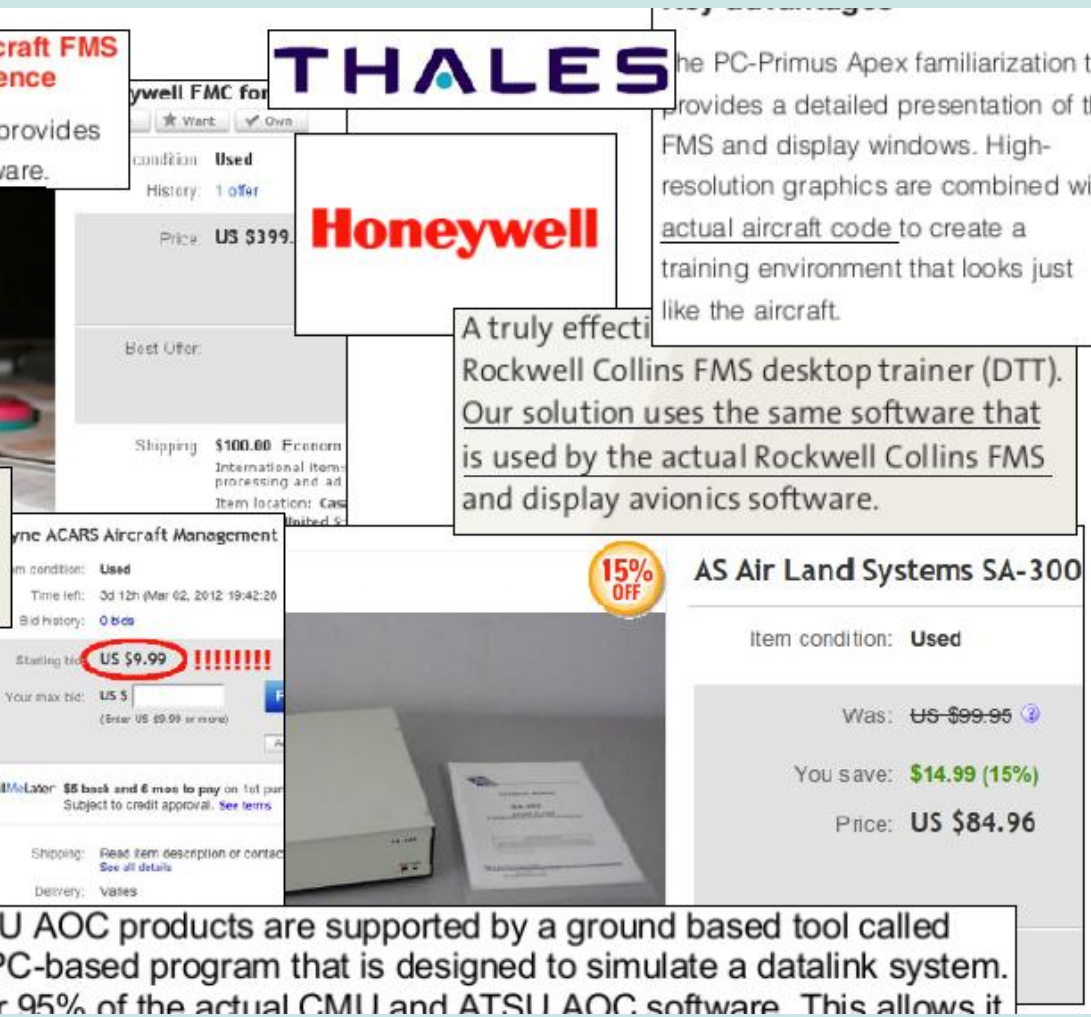
Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it

THALES

Honeywell

the PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.



Rockwell Collins ATSU AOC

Item condition: Used

Was: ~~US \$99.95~~

You save: **\$14.99 (15%)**

Price: **US \$84.96**

15% OFF

AS Air Land Systems SA-300

Starting bid: **US \$9.99** !!!!!!!!!

Your max bid: US \$

Shipping: Read item description or contact seller. See all details.

Delivery: Varies

Air Traffic Control Security /2

- Back last year, I was speaking with the guy which security tested all of those «devices» on the mountains of a European country.
- Those devices talk with the Air Control System infrastructure
- ALL of the SNMP «communities» are not encrypted and speak in clear text
- ALL of the SNMP «communities» are easy to guess («public», «ACS», etc...)
- His security report was «hidden» out somewhere ☹️

Airports security

- Without going so «extreme» as Hugo Teso (whose research impressed the European Flight Safety Authority), airports should definitely check for their ICT security.
- My experience with the another very important international airport in EU?
 - They wanted to «test it all»
 - Their budget wasn't enough, even for the 30% of what they wanted to be tested
 - It will be a public tender, and the winner will be the **cheaper bidder (!)**
 - **When (in)security impacts on human beings, there should not be «budget limitations».....**

Airplanes security

How a hacker could hijack a plane from their seat



- <http://www.sbs.com.au/news/article/2015/05/20/how-hacker-could-hijack-plane-their-seat>

Airplanes security /2

Airbus warns of software bug in A400M transport planes

Fatal crash in Spain may have been down to buggy engine control unit



- http://www.theregister.co.uk/2015/05/20/airbus_warns_of_a400m_software_bug/

Airplanes security /3

Boeing 787 Dreamliners contain a potentially catastrophic software bug

Beware of integer overflow-like bug in aircraft's electrical system, FAA warns.

by Dan Goodin - May 1, 2015 7:55pm CEST

Share Tweet 152

A software vulnerability in Boeing's new 787 Dreamliner jet has the potential to cause pilots to lose control of the aircraft, possibly in mid-flight, Federal Aviation Administration officials warned airlines recently.

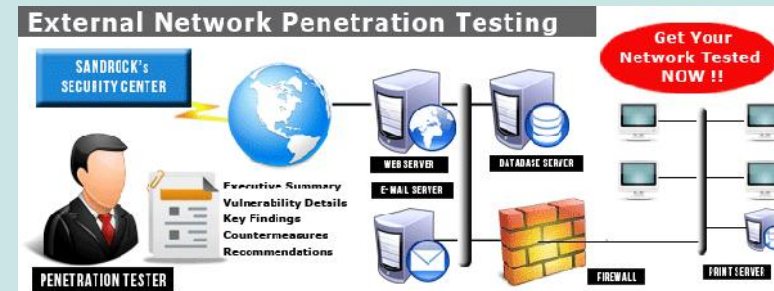
The bug—which is either a classic **integer overflow** or one very much resembling it—resides in one of the electrical systems responsible for generating power, according to **memo the FAA issued last week**. The vulnerability, which Boeing reported to the FAA, is triggered when a generator has been running continuously for a little more than eight months. As a result, FAA officials have adopted a new airworthiness directive (AD) that airlines will be required to follow, at least until the underlying flaw is fixed.

"This AD was prompted by the determination that a Model 787 airplane that has been powered continuously for 248 days can lose all alternating current (AC) electrical power due to the generator control units (GCUs) simultaneously going into failsafe mode," the memo stated. "This condition is caused by a software counter internal to the GCUs that will overflow after 248 days of continuous power. We are issuing this AD to prevent loss of all AC electrical power, which could result in loss of control of the airplane."

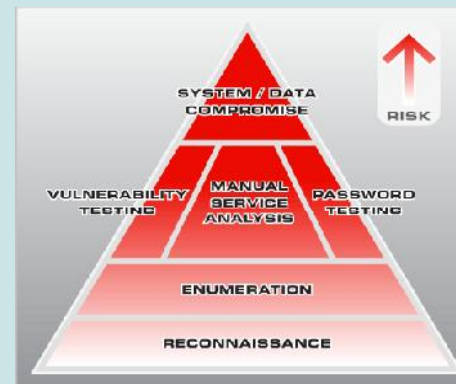
- <http://arstechnica.com/information-technology/2015/05/boeing-787-dreamliners-contain-a-potentially-catastrophic-software-bug/#p3>

OK, let's go in the real world!

- External Network Penetration Test



- Internal (LAN) Penetration Test



- Wi-Fi(s) Assessment + Penetration Test



External (network) PT: what we found....

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Consequences of Inf. Disclosure (TSA)

TSA let the press take a picture of their master keys.....Looking forward to the sets soon to be released by @tool <http://t.co>



OMG, it's actually working!!!
<http://t.co/rotJPJqjTg>



<https://mobile.twitter.com/bernard/status/641662069427847168>

Pentesting a large EU airport: what we found....

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Pentesting a large EU airport: what we found....

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Pentesting a large EU airport: what we found...

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Sample evidence: p0wning SAP

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found....

- INSECURE COMMUNICATION CHANNEL

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found...

- Username/Domain Disclosure

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found....

- Exposed Administrative Interface

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found...

- IPMI 2.0 Password Hash Disclosure - patch management problem!

..Which allowed us to extract the has files of the password (then we cracked them of course!)

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found....

- Web Application with insecure/default password (admin:admin)

SORRY!

This slide is not available in the public release of this presentation: you should have attended HES 2015!!!

Internal PT: what we found...

- “Airport Cleaning” ?!?!? WTF!
- IVR_PRIM: getting to the PSTN/ISDN and PRI area, LOL 😊

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found...

- IBM Tivoli Storage Manager Express CAD Service Buffer Overflow

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found....

- Whoooop! Netcat with remote shell INTO the LAN + without ACLs/restrictions/firewalls (TIVOLI needs to “talk”) : job done!
- P.S.: + Administrators accounts too!!

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Internal PT: what we found....

- Privilege escalation: dump of hashes from the just-hacked server ;)

Local:

Administrator
SUPPORT

4083FCA4
CA2DB52
D6389315
B729D9BFF8

securitybrokers C6

Net Cached:
(OMITTED)

Internal PT: what we found....

- Among cracked accounts (previous evidence), we found a **Domain Admin**.
- Sometimes, pentesters must be «lucky» ;)

“Dans la vie il faut aussi de la chance!”



Internal PT: what we found....

- Weak password policy

```
cracking@gpu2:~/oclHashcat-1.35$ wc -l xxx_domain_ntlm.txt
1212 xxx_domain_ntlm.txt
cracking@gpu2:~/oclHashcat-1.35$ wc -l
xxx_domain_ntlm.txt.recovered
559 xxx_domain_ntlm.txt.recovered
cracking@gpu2:~/oclHashcat-1.35\$
```

of 1212 hash extracted **559** have been cracked

Wi-Fi Assessment + PT: what we found....

We found a Wireless network which was:

- **OPEN**
- **Allowing traffic among clients (!)**
- **Allowing the routing towards the Data Center (!!)**
- **NOTE: The Airport immediately fixed the config as we phoned them while sit in a car outside of the airport's parking**

Wi-Fi Assessment + PT: what we found....

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Wi-Fi Assessment + PT: what we found....

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Wi-Fi Assessment + PT: what we found....

Wireless networks SSID3 and SSID7 are using WEP. Despite there was no traffic at that time, we needed just a SINGLE PACKET, in order to launch a ChopCop or a Frame Fragmentation Attack, thus cracking the password.

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Wi-Fi Assessment + PT: what we found....

- MITM attack, recovering the credentials when under MSCHAPv2...
- WHY???
- Because some of those devices connected to the network SSID8 (WPA Enterprise) do not verify the certificate provided by the Radius Server ☹

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Wi-Fi Assessment + PT: what we found....

- Network SSID11: Good, old DNS TUNNELING!

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

« Privacy » ?!?



BOARDING PASS

norwegian.com

JOHAN

JOHAN

FROM:

FLT NB:

DATE:

DPT:

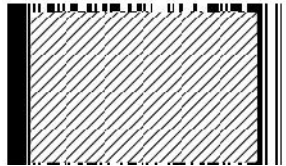
FR

TO:

NBR BAG:

DATE: DPT:

THANK YOU FOR FLYING NORWEGIAN



SEQ NB: 53

You know when they IR scan your Boarding Pass?



Last but not least, «my dream»!

SORRY!

**This slide is not available in the
public release of this presentation:
you should have attended HES 2015!!!**

Conclusions: best practices

1. Split into VLANs/DMZs
2. Firewall / Content Filtering / IDS
3. Implement device redundancy
4. Take care about **Physical security**
5. Update and verify documentation...
6. ...and apply policies! – **then, verify the whole thing!**
7. Disable unused services
8. Adopt AAA solutions
9. Use encryption (i.e. VPN)
10. Don't underevaluate **SSL** certificates
11. Correctly manage **SSH** keys (Automated, Centralized management)
12. Implement Quality of Service (qoS)
13. Use **test-bed** for simulations/security tests (where applicable)
14. Periodically run security tests (with a declared and common **penetration testing methodology**, such as the OSSTMM – www.osstmm.org)

Pentesting SCADA....

- In this slide I've chosen to share with you some key elements I have learnt from field experiences, while testing SCADA-related infrastructures.
 - **Do not run** “in-house” knowledge approach!
 - Don't run “Risk Analysis based”-only (solo) surveys;
 - Don't forget to include Risk Analysis and Risk Management into your Penetration Testing process too!
 - **Always** use a dedicated Test-Plant. Test plants do not need to be “huge” or expansive (see SOVEMA case study).
 - Do not underevaluate **penetration tester's role**, meaning do not “transform yourself” in a pentester at once.
 - Where applicable, **always apply, use and follow the existing** standards, legislations and procedures.
 - **Share your findings** with SCADA-security communities.

Extra: about open source Intelligence

- [-] Retail / Supply Chain
- [-] Transport
 - [-] Aviation
 - [-] ADS-B - Automated Dependent Surveillance-Broadcast
 - [-] Airlines
 - American Airlines
 - British Airways
 - Lufthansa
 - Ryanair Airline
 - United Airlines
 - [-] Aviation - Manufacturers
 - Airbus Group SE / EADS
 - BAE Systems
 - Boeing
 - Finmeccanica
 - General Dynamics
 - Honeywell International
 - Lockheed Martin / CIRA
 - Mitsubishi Heavy Industries
 - Northrop Grumman
 - Raytheon
 - United Technologies
 - Aviation Background Reports
 - Aviation Protocols and Systems
 - Aviation Security Alerts
 - Aviation Security News
 - [-] Container Transport

Activated subjects 1
Remaining subjects for your subscription 99

Global 100

Activated subjects 19
Remaining subjects for your subscription 81

Organization 10

Activated Search terms 0
Remaining search terms for your subscription 10



[Home](#) [Login](#) [Register](#) [Events](#) [CVSS](#)

BRI Risk Intelligence

BRI Risk Intelligence gives insight into what kind of attacks your organization is likely to experience and what are the current trends when it comes to cyber threats. This insight is incredibly valuable when it comes to determining how to allocate your security resources.

Reading Room / 1

Spam Nation, Brian Krebs, 2014

No Place to Hide: Edward Snowden, the NSA and Surveillance State, Glenn Greenwald, Penguin Books, 2014

Kingpin, Kevin Poulsen, 2012

Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking, Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009

H.P.P. Questionnaires 2005-2010

Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet, Joseph Menn, Public Affairs, 2010

Stealing the Network: How to Own a Continent, (an Identity), (a Shadow) (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to Own the Box, (V.A.), Syngress Publishing, 2003

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)

Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

Kevin Poulsen, Serial Hacker, Jonathan Littman, Little & Brown, 1997

Takedown, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997

The Art of Deception, Kevin D. Mitnick & William L. Simon, Wiley, 2002

The Art of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2004

@ Large: the Strange Case of the World's Biggest Internet Invasion, Charles Mann & David Freedman, Touchstone, 1998

Reading Room /2

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is “n3td3v”?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002

Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

Compendio di criminologia, Ponti G., Raffaello Cortina, 1991

Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44

Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Contacts, Q&A

- **Need anything, got doubts, wanna ask me smth?**
 - rc [at] security-brokers [dot] com
 - Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?

