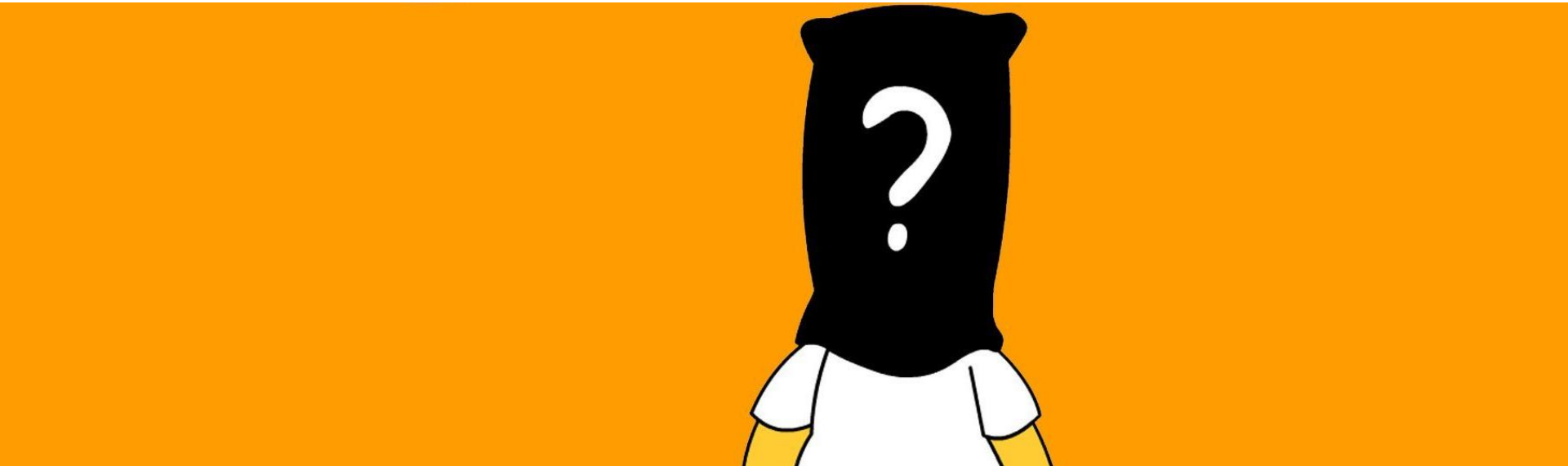
High EALs, Lightweight Certifications, Low EALs, cPPs
– European and American View –
Do we understand each other?

Index

- Who are we?
- Why this talk?
- American View
- European View
- Conclusions

jtsec
BEYOND IT SECURITY

Who are we?



Who are we?

- jtsec - CC Consultancy company - Based in Spain
- CCGEN Developers
- 7 Employees (and growing…)
- More than 10 years of experience working with different labs and CBs as evaluator, lab manager and consultant

Why are we here?

- We have experience in:
  - FIPS 140-2 tester
  - cPP evaluations
  - High Assurance (Smart cards and Security Boxes) evaluations
  - Lightweight Certifications
- Norway is a beautiful country ;)

Disclaimer

This is my personal view.
I may be wrong/right.
You may disagree, no problem at all!

Don’t hesitate to share your opinion!

jtsec
BEYOND IT SECURITY

Why this talk?

Why this talk?

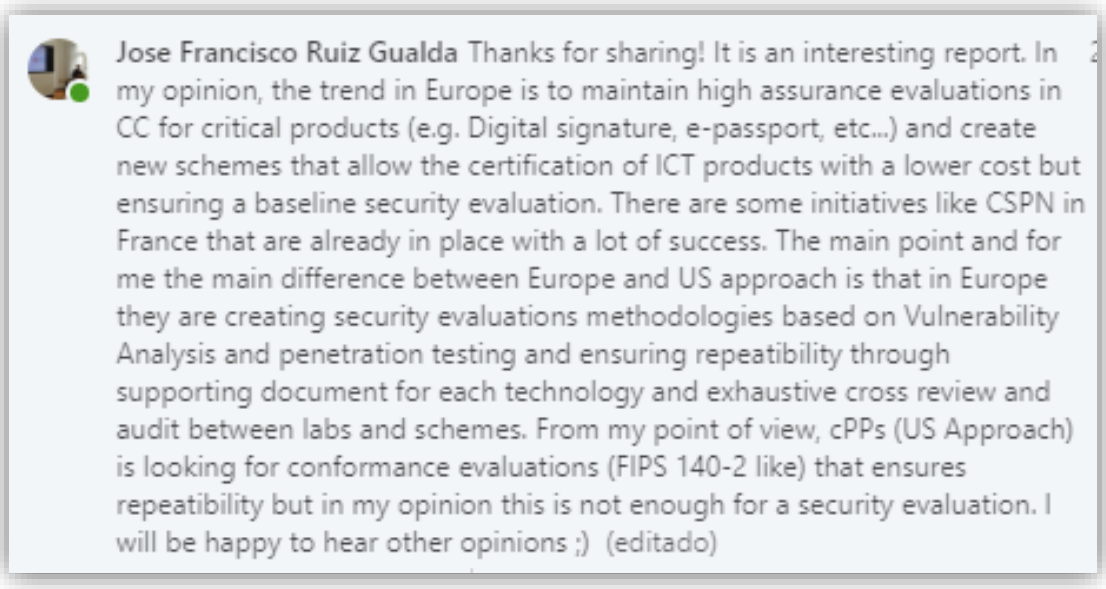
- Current Certification Status regarding CC:
  - CCRA Agreement
    - 28 worldwide countries
    - Up to EAL 2 or cPP
  - SOG-IS Agreement
    - 15 European countries
    - Up to EAL4
    - 2 Technical Domains (Smart Cards and HW Devices) up to EAL7
  - European Cybersecurity Act - Certification Framework Regulation Proposal

Why this talk?

- "Wasting" my time in LinkedIn, I found this:

Why this talk?

- And I thought… they are so wrong… So I answered with a polite comment…



Jose Francisco Ruiz Gualda Thanks for sharing! It is an interesting report. In my opinion, the trend in Europe is to maintain high assurance evaluations in CC for critical products (e.g. Digital signature, e-passport, etc…) and create new schemes that allow the certification of ICT products with a lower cost but ensuring a baseline security evaluation. There are some initiatives like CSPN in France that are already in place with a lot of success. The main point and for me the main difference between Europe and US approach is that in Europe they are creating security evaluations methodologies based on Vulnerability Analysis and penetration testing and ensuring repeatibility through supporting document for each technology and exhaustive cross review and audit between labs and schemes. From my point of view, cPPs (US Approach) is looking for conformance evaluations (FIPS 140-2 like) that ensures repeatibility but in my opinion this is not enough for a security evaluation. I will be happy to hear other opinions ;) (editado)

Why this talk?

- After that, I thought… “They must think the same of my ideas”…
- Probably… we don’t understand each other well enough…

jtsec
BEYOND IT SECURITY

American View

High assurance folks. Not my opinion!

- Press button approach

American View

- Advantages:
  - I appreciate the value of cPP for:
    - Conformance testing (FIPS 140-2 approach)
    - Security design guidelines/requirements for each product category
  - I like the NIAP Technical decisions (FIPS 140-2 Implementation Guidance approach)

American View

- Drawbacks:
  - cPP development is slow and costly
    - Applicable for non standard products and new technologies?
  - I don't understand why AVA_VAN components are missing in most of the cPPs/NIAP PPs

7.6 Class AVA: Vulnerability Assessment

For the first generation of this cPP, the iTC is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products and provide that content into the AVA_VAN discussion. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. This information will be used in the development of future protection profiles.

American View

- Positive signals:
  - Some iTCs (e.g. Network Device) has created a supporting document giving guidance for AVA activities
    - In my opinion, more focus on this activity is required

jtsec
BEYOND IT SECURITY

European View

European View: Past

Certified Products by Scheme and Assurance Level																			
Scheme	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**B**	**M**	**S**	**N**	**Total**
Australia	2	1	10	8	2	3	5	12	0	0	0	0	1	0	0	0	0	19	63
Canada	7	3	9	140	0	9	0	8	0	0	0	0	0	0	0	0	0	25	201
Germany	10	4	12	27	14	58	15	322	8	178	0	31	0	0	0	0	0	4	683
Spain	8	8	7	11	4	12	0	33	0	7	0	0	0	0	0	0	0	2	92
France	1	18	1	15	0	41	4	283	3	279	0	14	4	0	0	0	0	0	663
India	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	3
Italy	5	7	0	1	2	0	1	15	0	0	0	0	0	0	0	0	0	0	31
Japan																		4	139
Republic of Kor																		2	97
Malaysia																		0	39
Netherlands																		1	61
Norway																		0	82
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	2	0	11	2	5	4	6	5	2	0	0	0	0	0	0	0	0	1	38
Turkey	0	0	10	1	3	0	0	11	0	0	0	0	0	0	0	0	0	0	25
United Kingdom	0	0	4	6	1	3	0	26	0	3	0	0	0	0	0	0	0	2	45
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	93	93
Totals:	**46**	**41**	**99**	**314**	**65**	**202**	**72**	**774**	**16**	**506**	**0**	**61**	**5**	**1**	**0**	**0**	**0**	**153**	**2355**

Past: High Assurance is the key to save the world ;)

European View

- Is this applicable for all the technologies and markets?
  - Mobile Device?
  - Automotive?
  - IoT?
  - Industrial?
  - Etc.

- Are cPPs the solution to test the security of IT products?
  - No, they don't include Vulnerability Analysis and Penetration Testing

European View - Example

- IACS Cybersecurity Certification Framework
  - IACS – Industrial automation and control systems
  - Before the European Cybersecurity Certification Framework Regulation Proposal
  - 2016 – An Introduction to the framework was published
    - Industry Claim: "Don't mention Common Criteria"
  - 2017 – National Exercises on the framework
    - One of the Goals: Explore different methodologies applicable to IACS
    - All the NETs used lightweight methodologies

More Information: https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs

European View

What are lightweight Certifications?

- Security evaluation methodologies/certifications that focus on functional testing, vulnerability analysis and penetration testing avoiding most of the CC paper work
- Based on Common Criteria
- Origin: 2008 – French CSPN - translated by First Level Security Certification
- Other European countries have similar initiatives.

European View

- Problems with lightweight Certifications:
  - Lack of recognition – So far! It will come!

- Approach to obtain ~~repeatability or~~ equivalent results between different labs/CBs:
  - One of the main issues to be solved in the European Certification Framework

- IMHO, the approach will be similar to SOG-IS approach:
  - SOG-IS shadow Certifications and VPAs process
    - Technical audits including lab audits from a different CB
  - Attack Methods and Working Groups for each technology (used also by Global Platform or EMVco, Banking Schemes for Mobile)

Conclusions

Conclusions

- Europe is not longer just High Assurance, lightweight certifications will come to stay.
- cPPs must include AVA_VAN activities to be seen as a valid solution by European Governments.
- Obtain Equivalent results worldwide should be the goal, let's work on it.
- Wish: Work together to have Worldwide recognized methodologies and certifications.

Thank you!

jtsec: Beyond IT Security

c/ Abeto s/n Edificio CEG Oficina 2B

CP 18230 Granada – Atarfe – Spain

hola@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated.
It takes a genius to make it simple."
Woody Guthrie