ENISA workshop on Security Certification of ICT products in Europe

Minutes of the workshop

Introduction

On 16th of March 2016 ENISA organised a workshop aiming at bringing together stakeholders from the ICT security certification ecosystem and at investigating challenges for certification at EU level. For this reason, an open and structured discussion among the attendees was planned which was chaired by ENISA. This dialog allowed ENISA and the EC to pulse the impression of the audience on ICT security certification and Common Criteria (CC).

The workshop was well attended by approximately 75 experts covering different types of stakeholders; standardisation and ICT security certification bodies (both public and private), vendors, industry and end user associations, utilities, security service providers, testing labs etc. The presentations have been disseminated to the registrants via e-mail.

Agenda

DAY 1		
9.00	Registration	
9.30 – 10.45	*Presentations*	
9.30	Welcome and agenda of the day	Steve Purser, ENISA
9.35	Welcome by EC and presentation	CNECT
9.45	Setting the scene	Pierre Chastanet, CNECT
10.00	Certification for Industrial environments	Dr. Georgios Giannopoulos, JRC
10.15	Results of ENISA workshop on a common European ICT product security certification framework	Demosthenes Ikonomou, ENISA
10.30	Questions/Discussion	
10.45	Coffee Break	
11.00	*Panel 1 – Security Certification and Market Requirements*	
	(Optional) short presentations by panellists – Discussion guided by targeted questions addressed by the operator – Interaction with the audience Panel: - **Thomas Stubbings**- Chairman of the Cybersecurity Platform of the Austrian Government - **Martin David**-CESG - **David Francis**-Huawei Technologies	Moderator: Aristotelis Tzafalias CNECT

12.00	*Panel 2 – Mandatory vs voluntary certification schemes, Vertical vs cross sectorial approach to certification: use cases*	
	(Optional) short presentations by panellists – Discussion guided by targeted questions addressed by the operator – Interaction with the audience Panel: - **Martina Rohde** - BSI - **Jan Neutze** – Microsoft - **Dr. Sergey Tverdyshev -** SYSGO	Moderator: Konstantinos Moulinos, ENISA
13.00	Lunch Break	
14.00	*Panel 3 – The features of the EU certification framework of the future*	
	(Optional) short presentations by panellists – Discussion guided by targeted questions addressed by the operator – Interaction with the audience Panel: - **Marc Wouters** - FPS Economy Belgium - **Paul Theron** – Thales - **Arjan Geluk** – UL LLC labs	Moderator: Georgios Giannopoulos, JRC
15.00	*Panel 4 – Implementation issues of the future EU certification framework*	
	(Optional) short presentations by panellists – Discussion guided by targeted questions addressed by the operator – Interaction with the audience - **Thomas Weisshaupt** – ESMIG - **Beat Kreuter** – DEKRA - **Ian Bryant** - UK TSI - **Alicia Squires** – Cisco	Moderator: Clara Galan Manso, ENISA
16.00	Coffee break	
16.15	The way ahead - Summary of open issues - Actionable items by COM/Council and involvement of ENISA - Open discussion	All moderated by ENISA
16.45	Conclusions	ENISA
17.00	*Meeting ends*	

1 Presentations

The workshop opened with an introductory presentation by ENISA on the objectives of the workshop:

- Present the recent developments in the area of ICT security certification.
- Build upon the results of the ENISA workshop on ICT security certification with the public sector on 16th February 2016.
- Discuss the modalities of the ICT products' security certification.
- Discuss the necessity of a common ICT security product certification framework.

The EC shortly presented the coming NIS Directive together with the public-private partnership on cybersecurity (cPPP). The public consultation[1] finished on March 11th and more than 250 replies were received. The preliminary analysis of the results shows that certification is an important issue for security:

- Europe does not master the digital technologies but we have to maintain the capabilities needed to provide secure ICT technologies.
- There is enormous lack of trust and market fragmentation of ICT technologies.
- It is necessary to engage all different stakeholders and cPPP is a mechanism that makes this collaboration easier.
- Standardisation, training and education are key instruments to achieve the objectives set by the cPPP.

The cPPP is only one part of the collected by the EC input needed to assess the impact of certification; other input will come from the ENISA workshops on ICT security certification and the recommendations report that ENISA will prepare and publish in 2016.

Industrial and Automation Control Systems (IACS) are key for the prosperity of EU society not only because they support most of the critical business sectors but also because a market of 32bn$ billions of euros is revolving around them. The EU Joint Research Centre (JRC) presented the results from the ERNCIP project, thematic area Industrial Control Systems and Smart Grids, on a European IACS Components Cyber-Security Compliance & Certification Scheme. The scheme presented contains four different levels of compliance which reflect on the different needs of the assets owners. The needs for compliance and certification are identified based on the results of a risk assessment performed by the asset owner[2].

[1] https://ec.europa.eu/digital-single-market/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures?utm_source=twitter&utm_medium=social&utm_campaign=cybersecurityConsultation

[2] The full report is available at, https://erncip-project.jrc.ec.europa.eu/networks/tgs/ics-use-cases/53-tgnews/138-proposals-from-the-erncip-thematic-group-case-studies-for-the-cyber-security-of-industrial-automation-and-control-systems-for-a-european-iacs-components-cyber-security-compliance-and-certification-scheme

2 Panels

2.1 Key findings

Four panels followed the presentation sessions. Each panel had a specific theme to discuss. The key findings stemming from the panel discussions are the following:

- Demand by risk owners (business users or sectoral agencies) is lacking because of the high cost involved in having a product certified; there is a need to share the cost among risk owners.
- Voluntary or mandatory nature of certifications should be justified by risk assessments and the functioning of the market.
- One size does not fit all cases. We should not make generalised assumptions for the environment in which products function. Having said this, one should first do all efforts towards a global solution before identifying specific requirements for vertical markets
- Public procurement would be an important tool to promote ICT security certification, but is not used in Europe as actively as in other parts of the world.
- Products up to a specific level of criticality should have light procedures.
- It is of worth to consider an approach similar to the one followed by CE like marking system and/or the Radio and Telecommunication Terminal Equipment (R&TTE) Directive.. A system like the CE marking system is a good model for the production process but has to be enhanced with considerations regarding installation and maintenance.
- Deep understanding of technology lies more with industries than with governments.
- An EU trust label is good for market differentiation.
- ICT security certification should neither introduce barriers to SMEs nor to become bottleneck to new products.
- It is necessary that certification process is agile in order to align with technology developments or time-to-market requirements.
- We should not reinvent the wheel which means that we have to take advantage of existing tools which are based on open standardisation models. SOG-IS might be a good starting point, if an adaption effort to match the current requirements is undertaken.
- Standardisation organisations should be actively involved in the certification scheme development process. Europe should set standards but use an open global certification process to show conformance.
- The production of dedicated certification ETSI/CEN standards should be incentivized in order to use them as a strong reference base.
- ICT security certification which is based on global standards is an enabler for EU multinational companies and stimulates competitiveness.
- Security is a property that does not compose and consequently to that what is intended by ICT products. Although product structure is important knowledge of the system architecture is key. Security by design and threat modelling are tools to deal with zero day attacks.

- Safety, interoperability and security are essential factors for I4.0 and IoT. A certification framework will need to take into account safety certification of products and systems which is already in place.
- Protection profiles should be developed in a transparent, open and consensus based manner.
- ICT security certification should become a part of secure procurement guidelines.
- We need to take into account multiple aspects in order to provide a signal of trustworthiness (i.e the capability of the certifiers). Certifiers should ensure that the process is correctly followed – subject matter experts (particularly those who understand the threats) should be the ones who take part in the international technical communities developing the protection profiles and associated assurance activities
- We cannot rely on a single definition of a security problem due to the fact that the security requirements stem from a risk assessment by the risk owner.
- Russia and China have their own schemes. CCRA is the third widely accepted one. We should avoid creating a fourth new one if it proved to be possible.

2.2 Challenges

- There is no EU entity to facilitate public-private (demand supply) interaction.
- There are different ICT security certification schemes in Europe.
- It will take considerable effort to create a harmonized approach that reaches consensus.
- No harmonized approach causes higher costs for certification per asset owner because an asset owner has to recertify his products per country specific security requirements.
- There is not one single scheme that can provide EU guidance for implementation, and support national legislation.
- How do we measure what is good? It is difficult to measure security with numbers and trust marks. Certification is only a first step.
- At the moment only partial certification (people or products or systems or processes) is achievable.
- An ICT security certification scheme needs to be agile enough to keep adding to the assurance activities to cover the whole range of attacks.
- Trust needs small groups of experts. How can we scale up to big teams and at the same time maintaining the trust? The CC reform acknowledges this point and, with the cPP and supporting assurance document approach, has moved to a more scientifically sound basis involving transparent, objective, tests that can be repeated by others if necessary.
- A clear definition of what is a 'product' in complex operational environments such as IoT, cloud and smart grids is very challenging.

2.3 The future of product certification in EU

- Harmonisation is good but up to a certain level. Member States need flexibility for certain high level assurance sectors.

- Harmonisation of different national ICT security certification schemes or mutual recognition for security certification is a means to decrease the costs.
- Once a product is certified, no extra certification should be needed across Europe.
- It is necessary that any certification approach faces the challenges of recertification and patch management[3].
- Security requirements should be set by the users of the products and by EU associations.
- Different conformity assessment techniques, such as testing and vulnerability assessment, should be taken into account.
- Consumers should make decisions on the need for certification based on their own risk assessments.
- SOG-IS might be a good platform for the enhanced collaboration between the private and the public sector provided that an adaption effort to match the current requirements is undertaken.
- It is necessary that EU signs Recognition Agreements (RAs) with other regions in order to maximise the usefulness and recognition of any future certification scheme.
- Mapping activities between different standards might prove a useful tool on the way to enhance transparency in the certification market.

A certification scheme for EU should:

- Have a common baseline set of requirements recognized by all participating EU Member States.
- Facilitate public and private interaction with a clear description of roles and responsibilities for each party.
- Contain a common EU security reference model that is supported by standardisation organisations such as ISO and IEC.
- Use internationally equal security and risk levels based (bridging of different standards).
- Include support for components, systems and operation.
- Have a harmonized approach which eliminates the barriers and silos created by fragmented markets.
- Based on open standards. Threats are coming from all over the world, we need a global scheme based on open standards.

2.4 Recommendations

- An entity/scheme with EU wide powers which overlooks and follows ICT security certification matters for Europe and involves private and public sector stakeholders is necessary. This might be a self-organised scheme.
- More push from industries is necessary. We have to get inspired by other successful examples (e.g. GSMA).

[3] An interesting approach to this problem has been introduced by the EURO-MILS project, : the related White Paper Non-Interfering Composed Evaluation <http://euromils.eu/downloads/white_paper_non.pdf

- The EC should create a landing page for EU with specific explanations for all stakeholders for certification and relevant standards. This page will serve as:
    - A central web page for certified products.
    - Centralized storage and publication of national schemes.
- Some of the participants highlighted the role of certification in procuring by public authorities more secure equipment. In this regard, the certification bodies should play a significant role by advising different communities on what kind of technologies might be subject to certification.
- Since the topic "Security of Industrial and Automation Control Systems (IACS)" is getting more and more important, it would be helpful to establish an additional dedicated Technical Domain 'Industrial and Automation Control Systems' covering this kind of IT systems.
- The EC should clarify whether conformity against standards can be mandated in public procurement.
- The EC should take a stronger role in linking its policy (eIDAS, NIS) to ICT security certification based on global standards. That could be done through a voluntary approach, (e.g. based on an analysis of European industrial strengths which could inform user requirements) or through a regulatory approach.
- A description of the common denominator of the security requirements in existing standards is necessary.
- The EC should provide implementation guidance and recommendations based on best practices and informative standards.

The way forward

Using the results from both workshops and references from existing frameworks (e.g. CE marking, SOG-IS, etc.) ENISA will set up an expert group aiming at producing a roadmap and specific recommendations on how to set up a common European ICT product security certification framework.

The recommendations will cover important aspects of the potential certification scheme, namely: accreditation bodies and criteria, conformity assessment bodies' requirements, certification criteria, certified products listing, surveillance, etc. This report is expected to be published within Q4 2016.