Joint EC/ENISA SOG-IS and ICT certification workshop

Minutes of the workshop

Introduction

On 6th of October 2014 ENISA together with EC organised a workshop aiming at bringing together stakeholders from the ICT security certification eco system with the SOG-IS MRA experts and investigating challenges for certification. For this reason, an open and structured discussion among the attendees was planned which chaired by ENISA. This dialog allowed ENISA and EC to pulse the impression of the audience on ICT security certification and Common Criteria (CC).

The workshop was well attended by approximately 60 experts covering different types of stakeholders; standardisation and 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

10:00 – 10:30	Registration	
10:30 – 10:35	Welcome and agenda of the day	Steve Purser, HoD, ENISA
10:35 – 10:50	Welcome by EC	Paul Timmers, Director, DG-CNECT
10:50 – 11:15	Setting the scene – Description of SOGIS-MRA	Bernd Kowalski, Chairman of SOGIS-MRA, BSI
11:15 – 12:30	**Stakeholder presentations**	
11:15 – 11:30	The vendor's/integrator's view	Alain Boudou, Chairman of Product and System Security Committee, Eurosmart
11:30 – 11:45	The Lab's view - Presentation of an IT-security evaluation	Alain Merle, CEA-LETI
11:45 – 12:00	The role of the private sector in the certification	Willem Strabbing, ESMIG
12:00 – 12:15	Accreditation and certification scheme of Regulation 765/2008 on market surveillance	Pilar DE LA BARCENA ANGULO, DG ENTR
12:15 – 12:30	Wrap up of the session – Q&A	ENISA
12:30 – 12:45	Coffee Break	
12:45 - 14:00	**National IT security certification schemes based on mutual recognition**	
12:45 – 13:00	National schemes - part 1 - The Dutch Scheme	Rob Huisman, NLNCSA
13:00 – 13:15	National schemes - part 2 - The French Scheme	Julie Chuzel, ANSSI
13:15 – 13:30	National schemes – part 3 – The Swedish Scheme	Dag Ströman, FMV
13:30 – 13:45	National schemes – part 4 – The German Scheme	Joachim Weber, BSI
13:45 – 14:00	Wrap up of the session – Q&A	ENISA

14:00 – 15:00	Lunch	
15:00 – 16:00	**A common IT security certification framework at EU level**	
15:00 - 16:00	Panel discussion • Common denominator of and gaps between national schemes • Relationship between mandatory certification requirements in EU legislation and mandates to European standardisation organisation • IT security certification – a means to ensure European IT infrastructures and services competitiveness • Mutual recognition	Presenters moderated by ENISA
16:00 – 16:45	**The way ahead**	
	- Summary of open issues - Actionable items by COM/Council, the role of SOGIS-MRA, and involvement of ENISA	ALL moderated by ENISA
16:45 – 17:00	Conclusion and end of meeting	ENISA

Observations

3.1 Setting up the scene

The workshop opened with a presentation by ENISA which focused on the challenges of ICT security certification and the work of ENISA on this subject. Then, the issue of trust and the implications for it, by the Snowden case, were highlighted by the DG-CNECT. The certification as a means to increase trust to the users of ICT technologies was also a key message came out of this speech. Finally, the EU cyber strategy and its relationship with certification were also described.

Following the ENISA's and DG-CNECT's presentations, it was the turn of SOG-IS-MRA chair to introduce the audience to Common Criteria (CC) and the European SOG-IS Mutual Recognition Agreement (MRA). Apart from a general description of CC and SOG-IS MRA, some key concepts were explained; the protection profiles (PP) and their role in product development and certification, the Evaluation Assurance Levels (EALs), the shadowing/voluntary periodic assessments (VPA) (proofs of competency between SOG-IS MRA members), the international CC Recognition Agreement (CCRA) and its relation (backward compatibility) with SOG-IS MRA (SOG-IS MRA is more stringent than CCRA). Finally, the relationship between SOG-IS MRA and (International) Standardisation Organisations (ISOs) together with the invitation to new members were also described. Currently only 10 member states are members of the SOG-IS MRA and was explained that might be the result of the lack of certification policy by some other non-member MS.

3.2 Stakeholders

Stakeholders presented existing ICT security certification schemes in the field of smart cards (Eurosmart) and smart metering/smart grids (ESMIG). They expressed a need for a common EU approach and increased mutual recognition of certificates, to avoid national fragmentation which today converge to a large extent but not fully. While each ICT security certification is product dependent, i.e. the evaluation has to be based on the individual merits of each product, a common EU approach would have to be modular and address a group of functionalities instead of being prescriptive. The lack of recognition by EU regulation of ICT security certifications results in lost

opportunities for the EU ICT industry since they are taken over by non-European (e.g. e-payments). A question was also raised on how the ICT security certification, which is product-based, is related to areas where a whole system or solution needs to be secure. ENISA analysis points out that there are indeed gaps, but that taking a product approach permits to address a large spectrum of risks already. From a risk owner perspective most efforts focus on configuration security, rather than product security which is taken as given in some sectors.

Many of the stakeholders involved in the cybersecurity of industrial automation installations, are global players acting worldwide. For that reason, efforts to harmonize certification schemes should focus on international accepted standards e.g. IEC or ISO standards. An example of such a framework for harmonization and mutual recognition agreements is the IECEE / CB scheme. Most of the European countries take part of the activities of IECEE as well as many countries outside Europe. While applying IEC certificates is voluntary the EU Regulation sets out mandatory recognition between Member States.

3.3 National schemes

National schemes presented, all part of SOGIS-MRA, included NL (NLNCSA), FR (ANSSI), SE (FMV), DE (BSI). The national bodies mentioned all act as national certification bodies authorities with supervisory responsibility and some are ISO/IEC 17065 accredited by their national accreditation bodies. Their role is to oversee the national schemes and to issue the certificate based on the evaluation results of the laboratories. They also see to that the technical capabilities and skills of the laboratories are adequate. The certificates issued by national certification bodies cover product categories for which there is defined use-case and a protection profile specified by a technical community (stakeholder group) against which the laboratories will evaluate the equipment and certification bodies will issue the certificate. Protection profiles have until now been developed to a large extent for smart cards and also reflect the number of certificates issued, for some Member State they covered half of certificates, in addition to a very high level of assurance EAL5+.

3.4 Panel discussion

The panel discussion focussed on the advantages and challenges in using CC/SOGIS-MRA. 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. Public procurement would be an important tool to promote ICT security certificates, but is not used in Europe as actively as in other parts of the world. Harmonisation of different national ICT security certification schemes is a means to decrease the costs.

CC is the predominant standard for ICT security certification but there is room for improvement. The way to improve CC involves the strong involvement of all stakeholders. A working group which overlooks and follows ICT security certification matters for Europe which involves private and public sector stakeholders might help towards this direction. Any initiative should ensure the commitment of the involved parties, be to the point, with concrete, actionable, and relevant guidance. CBEST, financial sector, was referenced as an example for lessons learnt of what to avoid and what to consider when shaping such an initiative.; the end result of CBEST was that the document has received some criticism due to trying to do a lot of things, and it's quite complicated at that. This happened because it was just a natural result of people being too busy to engage deeply in content delivery, with the result that it does not seem totally clear to the people who are supposed to implement it what they ought to be doing. When something gets too much scope and tries to do too much, and too many stakeholders are involved, you will never get anything done. For this reason,

effort should be put to keep it small and to reputable, experienced and trusted people and focus on concrete output.

Some challenges with regards to CC and certification spotted out during the discussion:

- CC are not suitable for services e.g Cloud and big data. This is an example of why certification of components alone is not enough; we need an overall framework for certification which includes services, personnel, systems and products as well.
- It is an open question if existing applications might continue running on top of certified, and properly modified of course, products. Assessments should take place to this direction. Re-writing existing application will prove to be a big challenge.
- CC approach need to be more visible to the market.
- Re-certification after changes being made in the product is not mandatory, but should be considered case by case.

Different applications may require different certification approaches. Per application a stakeholder group should analyse the scope and possible approaches.

Most of the certification bodies support the users with writing protection profiles and they provide the industry and the technical committees with advice. Finally, some of the participants highlighted the role of certification in procuring by public authorities more secure equipment. In this regard, the certification bodies might play a significant role by advising different communities on what kind of technologies might be subject to certification.

Finally, smart grids and cloud computing[1] were referenced as new possible candidate areas for certification.

Conclusions

Recommendations for EU action coming out of the panel discussion included the establishment of a forum where risk owners, vendors , laboratories and certification bodies can come together to identify areas where there is a need to define use-cases and establish protection profiles (e.g. firewalls, USB-sticks, web browsers, cloud etc.). The Commission should take a stronger role in linking its policy (eIDAS, NIS) to ICT security certification. That could be done through a voluntary approach, e.g. based on an analysis of European industrial strengths which could inform user requirements; know-how centre; training, or through a regulatory approach. The regulatory push should be used in particular in the case of eIDAS, which should require compliance with ICT security certificates for components covered by it. Other action items include:

- The EC should also take into account SOG-IS MRA in future regulation making and security requirements specification activities.
- A security certification and CC educational programme should be established in order to educate users and buyers of products.
- The relationship between ISO/IEC 27001 and CC should be further examined.
- The EC should investigate the need for the creation of a 'know how' center for ICT security certification.
- A ICT security certification element should become part of the ENISA work programme.

Furthermore, the recommendation for European Commission should be to contribute on the European level to the worldwide not only European harmonization of certification schemes. The

[1] Perhaps with the use of other than CC standards.

scope should not only include products but also the automation solutions and the processes of the stakeholders: product suppliers, solution providers and risk owners.

The way forward

ENISA together with Commission to take actions in order to organise a second ICT certification workshop in 2015 which will built on top of the afore mentioned proposed recommendations.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece