Survival paces and challenges in cyber security development

It's interesting that when you google 'trust', many of the search results are about winning back trust, not just about establishing it. It seems that with tech companies getting a lot of negative publicity about the way they handle privacy and cyber security, simply establishing trust is not enough anymore.

Companies increasingly offer services and products that are hooked up to the cloud or even to the internet. From cloud-based file sharing to social media and smart security cams; consumers as well as enterprises today not only need to trust the services themselves, but also the way their personal and business information is handled, stored and, most importantly, protected from people with bad intentions.

Right now is the time for the tech industry, service providers and manufacturers to establish trust, or gain back the trust they lost, by taking up cyber security with both hands (or leaving it forever). (Cyber)Trust has become a business enabling (and limiting) factor and it will become incredibly relevant in the coming years.

Learn how to bring back trust

This greenpaper examines the current state of affairs in cyber security and gives three main takeaways that will help companies gain back the necessary trust in their products. It was written by Miguel Bañon, Global Technology Leader for Cyber Security at Epoche & Espri, a DEKRA company and convenor of ISO/IEC JTC 1/SC 27/WG 3.

So, where do you start?

It is not simple to determine the security of a product or system. When you try to define 'security', what it entails will vary per product and scenario. A mobile phone will require a level of protection that is fit for the complex environment with which it interacts, with many applications and connected services that have access to personal information. The definition of 'security' will be quite different for a cloud-based service as well as for an enterprise management system.

Once there is a definition for the security of a specific product, another step is to determine what security objectives should be achieved by the product or system. Also, it would be necessary to go over what security properties, functionalities and mechanisms it needs to protect to maintain the defined level of security.

Where are we coming from?

For years, there have been discussions between safety and security experts about exactly these topics. For example, some technical issues can be seen as similar for multiple cases when you analyze the properties of a system. Aspects such as intentionality and dynamism of attacks make defining security much more difficult. Providing absolute resistance of a complex product against attacks is not even attempted by the most well-known standards.

Here comes ISO/IEC 15408

The standardization committee that develops international standards, technical reports and technical specifications in information and cyber security is a cooperation by ISO, the International Organization for Standardization, and IEC, the International Electrotechnical Commission. Called ISO/IEC JTC 1/SC 27 IT Security Techniques, we will refer to it as ‘the cyber security committee’ for the readability of this greenpaper.

One of the most important standards produced by the cyber security committee is ISO/IEC 15408 “evaluation criteria for IT security”. It was published nearly twenty years ago. At that time, there were very few governmental certification bodies and they were more closely linked to national security agencies. It was mostly manufacturers who needed product cyber security certification to sell products to governments and ministries.

ISO/IEC 15408 is based on ‘levels of assurance’ that are given after thorough evaluation activities in the following fields:

> Analysis and audit of processes and procedures
> Ensuring that processes and procedures are applied
> Analysis of correspondence between design representations
> Analysis of design representation against requirements
> Verification of proof
> Analysis of guidance documents
> Analysis of developed functional tests and provided results
> Independent functional testing
> Analysis for vulnerabilities (including flaw hypothesis)
> Penetration testing

A minimum ‘Evaluation Assurance Level’ (EAL) for the security of a ‘Target of Evaluation’ (TOE) (or simply put product), as ISO/IEC 15408 defines it, can be achieved as follows:

“EAL1 provides a basic level of assurance by an analysis of the security functions using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions. This EAL provides a meaningful increase in assurance over an unevaluated IT product or system.”

On the other hand, the maximum assurance level that can be achieved through ISO/IEC 15408 would include the following:

“EAL7 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a structured presentation of the implementation, to understand the security behaviour.

What should you take into account?

Assurance is additionally gained through a formal model of the TOE security policy, a formal presentation of the functional specification and high-level design, a semiformal presentation of the low-level design, and formal and semiformal demonstration of correspondence between them, as appropriate. A modular, layered and simple TOE design is also required.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification high-level design, low-level design and implementation representation, complete independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential. The analysis also includes validation of the developer’s systematic covert channel analysis.

'These evaluation processes require a great deal of expertise and manpower.'

EAL7 also provides assurance through the use of a structured development process, development environment controls, and comprehensive TOE configuration management including complete automation, and evidence of secure delivery procedures.”

As becomes clear, these kinds of evaluation processes not only require comprehensive and in-depth security engineering from the product developer throughout the product lifecycle, but a great deal of expertise and manpower as well. Evaluations are costly adventures and interfere with the time-to-market and intentions to reduce costs. However, they have proven to have a very positive impact on the security and the quality of the evaluated products.

To support the application of ISO/IEC 15408, the cyber security committee includes companion standards and technical specifications in their catalog. They help to apply the ISO/IEC 15408 evaluation process and support the notion to achieve as much as possible comparable and objective results.

Cryptographic modules

Another standard produced by the cyber security committee is ISO/IEC 19790 'Security requirements for cryptographic modules'. Originally based on the US Federal Information Processing Standard 140-2, it has evolved to safeguard cryptographic modules against new weaknesses and attacks.

Interestingly, ISO/IEC 19790 is not based on the concept of an evaluation or assessment. Rather, it relies on objective functional tests to determine conformance with the standard's requirements. These include aspects such as the design, functionality and the construction of a product.

Separating the wheat from the chaff

In that sense, for a module to fail the validation process, the tester would not need to get the actual cryptographic keys through an attack path that could penetrate the module enclosure, but simply penetrate the enclosure. They do not need to bother with the practical implications of module integrity violation. ISO/IEC 19790 provides a very efficient mechanism to simply separate the wheat from the chaff by implementing a testing process that is shorter and less costly than an evaluation of the same module according to ISO/IEC 15408.

ISO/IEC 19790 is complemented with companion standards and technical specifications that cover the practicalities of its application, ranging from test requirements and testing methods to the guidelines for testing cryptographic modules in their operational environment.

The standards related to and including ISO/IEC 15408 and ISO/IEC 19790 have evolved from many years of experience in security evaluation and testing. Today, they are the 'standard' in procurement requirements and regulation compliance methods all over the world. Recognition agreements for, for example ISO/IEC 15408, cover a great number of countries, but for limited assurance [1], or between a reduced number of countries with more technical coordination and trust to the maximum level of assurance provided [2].

Situations and trends

Both ISO/IEC 15408 and ISO/IEC 19790 apply fundamentally different methods for assurance. The first one is based on evaluations and assessments, whereas the second one is based purely on conformity testing. Both methods have their limitations and both standards have a tendency to overlap as well.

ISO/IEC 15408 applies functional testing to gain an initial level of assurance on top of which a vulnerability analysis is performed. It may seem like a sound method to test the entropy of the output of a random bit generator to discard the bad ones. But can users rely on a generator that passes all statistical tests?

Assume that a random bit generator outputs the results of applying a hash function using a deterministic counter. Depending on the characteristics of the hash function, the generator will most likely pass all statistical tests. However, an attacker who knows about this design will be able to guess the output of the generator.

This issue has forced ISO/IEC 19790 to require analyses and to add thought to the validation process. It seems that functional testing of a black box will not provide sufficient assurance in some cases.

One trend in the application of ISO/IEC 15408 is the promotion of low-assurance evaluations, inspired by the ISO/IEC 19790 model. These evaluations are often performed with very specific functional tests based on precise functional security requirements, but with limited or no knowledge of the product design, source code, development process and a limited vulnerability analysis.

> *The goal here is to cover a wide range of products,*
> *ensuring they implement at least a well-known set*
> *of security features and mechanisms.*

Specifying security requirements and the applicable assurance methods for a generic product type, or a "Protection Profile" (PP) in the language of ISO/IEC 15408, is a very efficient tool to apply its security evaluation framework in a manner agreed by a community.

[1] - *https://www.commoncriteriaportal.org/*

[2] - *https://sogis.org/*

The PP specifies the security problem to be addressed based on the product type, the security requirements and mechanisms that it must have, as well as the assurance method to be used.

The energy and resources invested by the security community in the development of PPs have resulted in very few standards. Most of them were published as 'high assurance' European standards, to support the compliance of regulations with a secure IT element, such as in digital signature creation devices or vehicle tachographs. PPs have been developed to allow assurance through conformity tests, but to this day none of these have been published as standards.

What's happening?

We need an urgent solution to maintain assurance of and confidence in a certified product when it has been modified.

Cyber security certification processes, such as those applied by the Common Criteria Recognition Agreement [3] or the Cryptographic Module Validation Program [4], were designed when products were not so widely used and, more importantly, not so frequently updated as today. They have been criticized often for not offering a certification model that follows the constant need to update or patch products. Naturally, the validity of a certificate can be lost when a product is modified.

Standards used today refer to a static 'Target of Evaluation' (ISO/IEC 15408) or 'Item Under Test' (ISO/IEC 19790) instead of a continuum of evolving product versions. That's logical: cyber security tends not to react in a linear way to change i.e. just a small change in the source code can cause a substantial vulnerability [5]. So there is a sound base to support a static approach.

The cyber security committee is exploring assurance related to product patching. A solution will most likely require building a sort of incremental assurance process by including the development and maintenance process, the proper TOE evaluation, and the conditions and assurance activities related to vulnerability handling and mitigation processes, patch management and evaluation.

The need for a high assurance level is just as pressing as the need for a timely response to these issues. Efforts to promote conformity-testing based cyber security certification as a cost-effective solution to improve the general security landscape are supported by the industry. It reduces efforts and certification time, but it compromises assurance.

This comes at a time in which end users have the lowest level of trust in technology and service providers. Cyber security 'plots' that years ago could only be conceived in spy novels share the daily news with sports and weather reports [6].

3 - https://www.commoncriteriaportal.org/

4 - https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program

5 - https://github.com/openssl/openssl/commit/bd6941cfaa31ee8a3f8661cb98227a5cbcc0f9f3#diff-38dc72994741420e2b6c5ee074941a45

6 - https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4

Manufacturers that used to protect their intellectual property are now offering to share their source code with customers or are even publishing it as open source in an attempt to gain trustworthiness. Manufacturers who already share their source code are questioned as to whether their product only contains that source code. In the field of hardware, some great challenges have arisen in the supply chain as well as a lack of knowledge in undesirable functionalities of foundational components.

Naturally, the classic requirements to the testing, inspection and certification industry still hold. Providing certification processes that are compatible with the time to market and updating the lifecycle of products remain relevant. However, in addition to that obtaining a high level of assurance through evaluations has become a priority. Manufacturers and service providers cannot wait to ensure the level of trust their users demand.

"We need to help consumers understand the importance of cyber security and what certification means and stands for"

Finally, we need to help end users understand the real value of cyber security and the 'semantics' of the certification scope. Consumers have adopted new tech without much consideration of the risks. We tend to favor trendy products and services without thinking of the security aspects that come into play.

Initially, reports on product vulnerabilities or breaches in services were seen as remote threats, more of a concern to specialized media than to individuals. However, this has changed. Ransomware attacks in the last two years have affected a considerable number of small and medium-size enterprises, forcing their employees to learn about, for example, crypto currencies, waiting to pay the demanded ransom[7].

In the recent hearing of Mr. Mark Zuckerberg by the US Senate Commerce and Judiciary committees, the Cambridge Analytics leak directly affected family and staff of the Senators involved, making the hearing much more personal to them than normal [8].

There is a notion of distrust that surrounded the hearing. The only option now seems to be to stop using these kinds of services, or even disabling them, like teenagers in the know who cover their laptop's webcams with stickers. However, a proper counter-measure would be to select those products and services end-users can rely on.

"We need mechanisms, like security seals or marks that help consumers identify secure products"

We need mechanisms to identify these. Privacy by design security seals and certificates of IT security should be made available so end-users can identify trustworthy products and applications.

Helping the end-user

Understanding what an ISO/IEC 15408 certificate stands for means that end-users need to analyze the 'security target', written by development engineers or technicians. Deciphering this kind of formalized language is actually only possible if you have a sound knowledge of the standard itself. So pretending that this is an option would be optimistic to say the least.

Attempts to simplify the certified assurance concept have not been very successful. Just using labels leads to the wrong idea that equal labels stand for equal security or the bigger the number, the better. For example, the four security levels of ISO/IEC 19790 may seem to indicate a higher level of security as the level goes up. But a module certified at level four may only be certified for a hash function, while another module may protect the user's keys at level three.

EAL4 of a product, such as a data diode, provides more assurance than the same EAL4 on a complex operating system. For most people, it is hard to fully comprehend in what way these types of products differ and therefore the difference in assurance is hard to grasp as well.

It might be worthwhile for the cyber security committee to explore the 'fit for purpose' concept as a dynamic process to approve or disapprove a product for a specific use. Combined with dynamic certification management and paired with vulnerability handling and emergency response services, this may well provide a useful bridge from the existing certification standards to the daily use of certified products.

What we expect

Right now, ISO/IEC 15408 is in the works; a revision, which will already incorporate many current needs, will be published in 2020. Other important topics, which still need a solution, are being researched to either produce a complementing standard or trigger an early review of ISO/IEC 15408 if required.

"Together we need to speed up the revisions of our standards to bring back common sense in cyber security"

All this happens at a time in which cyber security certification is more in demand than ever before. We have reached a peak of distrust in products and services. Among others, European legislation is on its way to bring back common sense.

A proposal regulation by the European Parliament and the Council on Enisa, the EU Cyber Security Agency, is currently under discussion as well as a proposal to repeal Regulation (EU) 526/2013. These efforts aim to establish a pan-European cyber security certification policy with specific certification schemes.

Other European regulations aimed at protecting consumers were drafted at a time when products like toys or medical devices were not connected to the internet. That is no longer the case; to ensure the protection of consumers now and in the future these regulations will need to be updated with the incorporation of cyber security certification aspects.

We expect the Cybersecurity Act to create a 'boost' in product-specific cyber security requirements for entering the EU market. However, the methods for compliance, certification and labeling will most likely vary.

7 - https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

8 - https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.832b44391fd5

One debate in assurance methods is about the tradeoff between conformity testing and self-declaration of conformity versus security evaluations and third-party certification. You could argue that products with a lower relevance and impact in daily life, such as a fish tank thermostat, could do with a quick and low-cost assurance process to enter the market. You would 'only' risk losing the fishes if the thermostat is compromised.

An actual analysis should not be based on the immediate effect that the abuse of an irrelevant device, such as a fish tank, has. It should be based on the role that these kinds of devices can have in a much more complex scenario, like a recent attack on a casino through a fish tank thermostat, believe it or not, has shown [9]. And what about home routers that are being compromised by state-sponsored hackers? [10]

A compromised router might not affect the quality of service and performance of media streaming services, but it can be catastrophic when brought into a coordinated, global attack. Assurance through third-party certification seems to be the best mechanism so far to rely on technologies.

If the cyber security committee succeeds in addressing the needs of the market, their standards might well become the preferred choice. They build upon practical experience in security evaluations and certification, which has produced some very good results in standards for two decades already. Improving or modifying existing methods is less difficult than trying to completely reinvent security evaluation methods. In addition, manufacturers need the right instruments to achieve trustworthiness and transparency. International approvals and recognitions with a broad focus can be the right tool for that[11].

Even though regional legislations, such as the EU Cyber Security Act, the Chinese Cyber Security Law and the US NIST Cyber Security Framework are in place, the technical standards that can be used to comply are still in development. Among others, the cyber security committee will do their best to provide manufacturers as well as society with excellence, now and in the future, as is expected.

Sources & acknowledgements

This greenpaper was created in cooperation with Miguel Bañon, Global Technology Leader for Cyber Security at Epoche & Espri, a DEKRA company and convenor of ISO/IEC JTC 1/SC 27/WG 3.

9 - https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on&utm_term=.25a315086a10

10 - https://www.forbes.com/sites/thomasbrewster/2018/04/16/russia-accused-of-hacking-network-infrastructure/#629eabd1744e

11 - https://blogs.oracle.com/security/common-criteria-and-the-future-of-security-evaluations-v2

Contact

Telephones	+34 952 619 432
E-mail	wireless.es.global@dekra.com
Internet	www.dekra-product-safety.com/en/cyber-security

DEKRA