THALES Secure CMS: from a highly secure to the Trusted Information Exchange

Dr. Ing. Michael Frank Glinka, M.B.A. , Dipl.-Ing. , PMP , CISSP , CSPO

Thales Netherlands

Synopsis

THALES Netherlands Naval is recognized as a distinguished, high class system integrator who provides cybersecurity as an integral part of its complex systems, where the Tacticos naval CMS (Combat Management System) is just one example taken out of its large portfolio.

Mastering Security requires a professionally managed, orchestrated evolution of all underlying cybersecurity technologies. Latest when it comes to secure and even trusted computing on THALES systems, the presented results contribute to THALES' discriminator solutions that excel not only in the naval CMS realm. THALES Research and Technology directorate manages the stepwise, well-considered application of emerging cybersecurity technologies, leading to high technology systems that navies worldwide can trust upon, both now and in the future.

To illustrate this fascinating ongoing THALES cybersecurity journey, the current paper provides realized examples that demonstrate some of the important early steps taken. For successfully mastering the complexity of naval IT platform systems an optimization approach is derived where Security necessarily comprises of more than only these three dimensions that are commonly known as confidentiality, availability and integrity. This paper focuses on 'Information and communication technologies'. In particular, the discussed Machine Authentication Continuum and Remote Attestation provide new insights on some techniques to power THALES solutions to a new distinctive level of cybersecurity.

It is elaborated how well-considered applications of these technologies enhance the trust that navies globally can rely on: well-thought-out use cases demonstrate how Trusted Hardware harnesses the trusted information exchange between the complexity of subsystems that constitute the overall naval IT platform. This paper will further show how a concept of i.a. signed messages fits into complex architectures.

Keywords:
Authentication Continuum; Enhanced CIA-Triad (multidimensional); Cybersecurity; Naval Risk Management; Risk Perception; Silicon-based Root of Trust (RoT); Silicon-based Security; Trustworthiness; Trade-off Space; Trusted Hardware.

Author's Biography:

Dr. Michael Frank Glinka is presently Project Manager leading cybersecurity projects: internal research projects within THALES as well as by leading an external consortium for the Dutch Navy. He joined THALES Germany as a System Engineering Manager in 2010 and moved to THALES Netherlands in 2014.

In total more than 20 years he fulfilled several roles in R&D and operations as coach, docent, consultant and global team-lead: for larger telecommunication programs (W-CDMA, 2G/3G/4G), on air-interfaces/core-networks, worldwide optimization activities, or finally as a project manager managing IT-Security R&D projects since 2004. Scientific parts included complex mathematical modelling, algorithm- / professional sw-development, databases, electronics and cyber-/ Security.

Prior to THALES he obtained the diploma and Doktor -with distinction- (the best mark that is possible at all) in Electrical Engineering at the TU Braunschweig in Germany in 2002. Again, in parallel to the full-time job, he added his 'Master of Business Administration' (M.B.A.) at the OU in the UK. He holds several certificates, i.a. 'Certified Information Systems Security Professional' (CISSP) or 'Project Management Professional' (PMP) each for more than 15 years or 'Scrum Certified Product Owner' (CSPO) since almost 4 years. (Further certifications are in preparation.)

Dr. Michael Frank Glinka published several papers and applied for 9 patents (each as the sole inventor); his patents granted for the areas of cybersecurity and HF-antennae are still active.

 https://doi.org/10.24868/issn.2515-818X.2020.042

1. Introduction

The provision of trust to a platform can be realized even for typical Commercial-Off-The Shelf (COTS) hardware when it is combined with a Trusted Hardware technology that is available in the form of i.e. Trusted Platform Modules (TPMs). Further forms of Trusted Hardware exist for different scopes.

One prominent state Security-player who is dealing with the strongest Security protection concepts worldwide, the German 'Bundesamt für Sicherheit in der Informationstechnik' (BSI) observes this technology since the early beginning of this millennium and publishes under the heading 'Cyber Security' the most recent information for using these TPMs as a central Security building block [1].

If these modules are applied within a broader Security concept for complex systems (of systems), like naval platforms, such modules contribute considerably to various inter-connected Security protection goals which are in a first approximation represented by well-known Security dimensions and often reduced -admittedly very rough- to only three quantities: Confidentiality, Integrity and Availability.

These three quantities are often summarized as the CIA-triad. This is partly done to describe Security protection goals, but mostly for trying to keep the very complex topic of Security simple enough to grasp. By dealing with cybersecurity it is unfortunately way too often forgotten that Security in practice consists of much more than only these three basic quantities, especially in the complex Naval realm.

A first example deals with the control of data. Even if all data in a platform has full Integrity, full Confidentiality and full Availability: if somebody else is able to control e.g. the gun fire at his own will, then there is definitely a breach in Security.

Or, a second example: if in a normally well working publish-subscribe system the keys are forged by somebody, then a situation exists where the integrity of its payload data is untouched (as it is not changed), available (it is actually still there) and confidential (payload data confidentiality is not breached), but no one would state that this system is secure. Finally, both examples lead to the question: how to protect a system vs. the control of data?

A third, similar example occurs when a password that protects data is forgotten and no recovery measure for the lost password exits. One may call this missing Security quantity Usability: the protected data is still there, even unchanged, but it became useless.

Since the early days of Security research various other examples occurred when an often too-simplistic CIA-triad is not sufficient, cf. the raison d'être of the Parkerian Hexad [2].

Especially in the Naval realm another Security dimension –that is also not covered by the CIA triad– gets dominant: 'accreditability' meaning the capability of a system to receive future accreditation by the state authorities. From the earliest steps it is thus essential to design Security into the future naval platform in a way that the chance of meeting the future accreditation expectations is maximized.

To succeed in meeting the strong Security demands of governmental authorities in the Defense realm, cf. the mentioned German BSI as well as the usually prevailing naval stakeholders, various Security viewpoints must be considered and be modelled clearly.

This is finally the rationale why Security research at THALES Naval is based on a specific Security model that does not only balance perspectives holistically, but also looks deep into details the CIA-triad does not directly offer.

To explain the author's approach, notice just some of the further perspectives that usually are perceived by the different stakeholder groups of a naval platform architecture when discussing about Security: instead of trading-off between three {C; I; A} Security dimensions, more Security dimensions in terms of {i.e. intervenability, authenticity, safety, legitimacy, .. etc.} suddenly appear when heading towards a new platform architecture with a sought degree of Security. At this point the CIA-triad gets insufficient to cover all necessary Security aspects.

Indeed, beside Security (and whatever stakeholders think it requires) further considerations and way more stronger constraints always appear. Experience shows that these two additional dimensions are Cost and Usability. They are shown in the three-dimensional diagram below.

 https://doi.org/10.24868/issn.2515-818X.2020.042

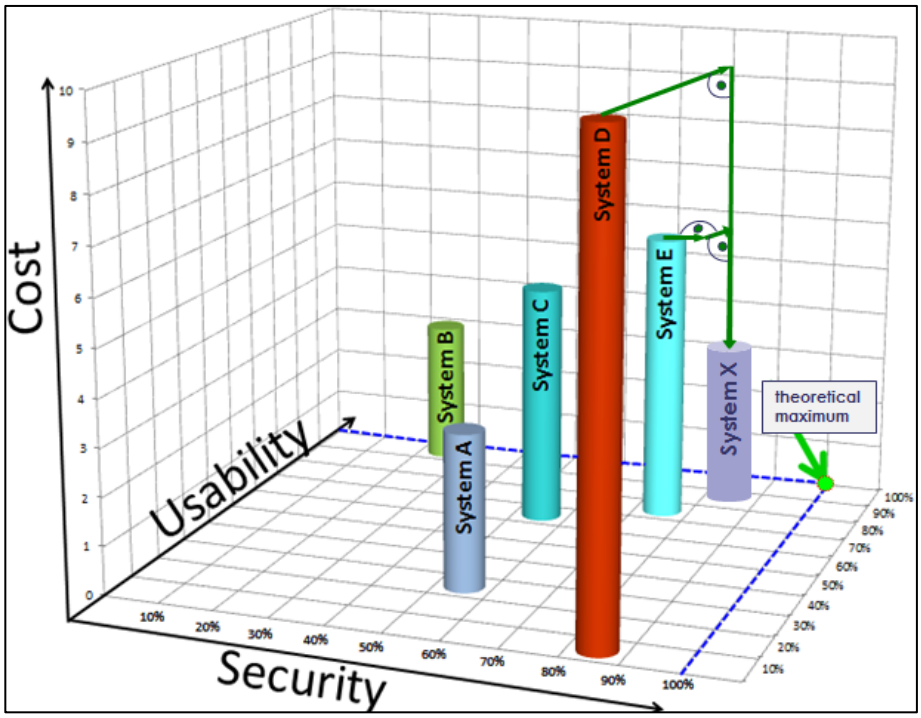

Fig. 1-1. *Trade-off space: constraining dimensions of complex systems (of systems) beyond the CIA-triad*

Above in Fig. 1-1 six different platform architectures {A; B; C; D; E; X} are placed within one trade-off space. Each architecture describes a different trade-off point that is formed by a certain degree of Usability and Security and -often utmost important- Cost, as there is often an overruling price label attached. Note that in the above diagram Security consists of more dimensions than the CIA-triad offers. Reality proves that the platform architecture that will be chosen by all stakeholders, finally is a tradeoff amongst Security with more than just the three 'basic' CIA-dimensions, Usability and Cost.

Experience shows that Cost often is the most constraining dimension. Security is in practice nothing else than the residual risk that is agreed by all stakeholders. Indeed, the perception of direct Cost is often stronger -*because taken as granted*- than the perception of Risk -that relates to a probability that *may not always* manifest- [1]. A further explanation may be that the notion of Risk that commonly is used within risk-management oriented industries (i.e. in the insurance and banking sector) points to *similar* quantities than cost, c.f. the 'Value At Risk': this is similar to a Cost position, but one that has not manifested yet. Cost is for real and therefore it is perceived almost as most important.

This explains why Cost was and is often seen as *the* strongest constraint when analyzing all different system solutions identified within the tradeoff-space of Fig. 1-1: this is a situation when people just *talk* about the hard-to-quantifiable Security/Risk and -as all too often evident- *think* about Cost instead.

Combining the different risk-perceptions and viewpoints of various stakeholders into a structured approach provides another rationale why THALES Naval has developed a new Risk Analysis (RA) method that is based on the EBIOS method. And more important: this RA is especially tailored on its underlying naval context. This explains also why other different families of risk management standards, cf. ISO 31000:2018, are not chosen: they are not meeting the proper risk analysis scope of complex naval platform systems.

Independent of a chosen standard it is further important to state that there is *no optimal* system, cf. the (theoretical) point the green arrow in Fig. 1-1 points to. This is exactly what professional experts have seen for many decades: the absolute theoretical maximum with {100% Usability; 100% Security} is often sought, but never achieved. Because this ideal Trade-off point exists only in theory, but never in practice.

[1] Interesting to note is the paradigm shift seen in ISO 31000:2009 [3] and ISO Guide 73 [4] where the definition of 'risk' has changed from 'chance or probability of loss' to 'effect of uncertainty on objectives'.

 https://doi.org/10.24868/issn.2515-818X.2020.042

Even more, since the early days of Security discussions it has often been seen that this 'perfect point' at the same time was requested to be reached at zero Cost, ideally. But the right answer of Security experts was always: no, it is impossible to reach this theoretical point in practice.

What did we learn from this all? To come *as close as possible* to this green point, new and innovative approaches are needed! This is the reason why THALES Netherlands Naval heads for Security while always regarding *several perspectives*: *First*, Security consists of more than the well-known three {C,I,A}–dimensions, and *second*, Cost has to be seen as *one* factor (admittedly important), but not as the single-one overruling factor within the whole context of complex system integration activities.

To underpin this conclusion, compare the different platforms in Fig. 1-1: A provides more Security than B, but less Usability. C is better than A and B, but only for the price of a higher Cost. One architect may have found D that provides even more Security than C, but again, only for even higher Cost. The 'optimization' E may then reduce this cost while sacrificing only some degree of Security: E gives less Security than D, but on the other hand compensates by Usability gains. This may be the phase where in absolute terms no better trade-offs can be found -*given the recent technological progress state*-.

A company can only make a difference -*beyond E*- by harnessing new Security technologies to their solution. This is the main reason why commercial Security research is done. The rise of new Security building blocks enables to realize new Security aspects within an orchestrated solution built upon the latest new cybersecurity technologies: here, the platform architecture X provides more Security and Usability compared to all other platform architectures {A..E}. And yes, even at the lowest Cost. How to realize such a promising, most optimal platform architecture X is thus the main topic of this paper.

2. Considering the real Security Aspects of modern Naval Platforms

Chap. 1 has justified that an entire corporate, or just a part of it, i.e. imagine a Combat Management System (CMS) supplier, needs new and innovative technology approaches in order to create a platform with more Security dimensions than the CIA-triad offers. By doing so and by challenging additional Security dimensions, cf. the Parkerian *hexad* [2] vs. the CIA *triad*, value can be added even for conventional systems. System X as shown in Fig. 1-1 is offering this extra value beyond systems A-E by providing the highest degree of Security, highest Usability, and the lowest Cost at the same time.

To illustrate this finding with real Security aspects within the real existing business contexts of modern Naval platforms, the following Fig 2-1 lists three of the actual main naval themes of the Research and Technology (R&T) business line of THALES Nederland's Above Water Systems (AWS).

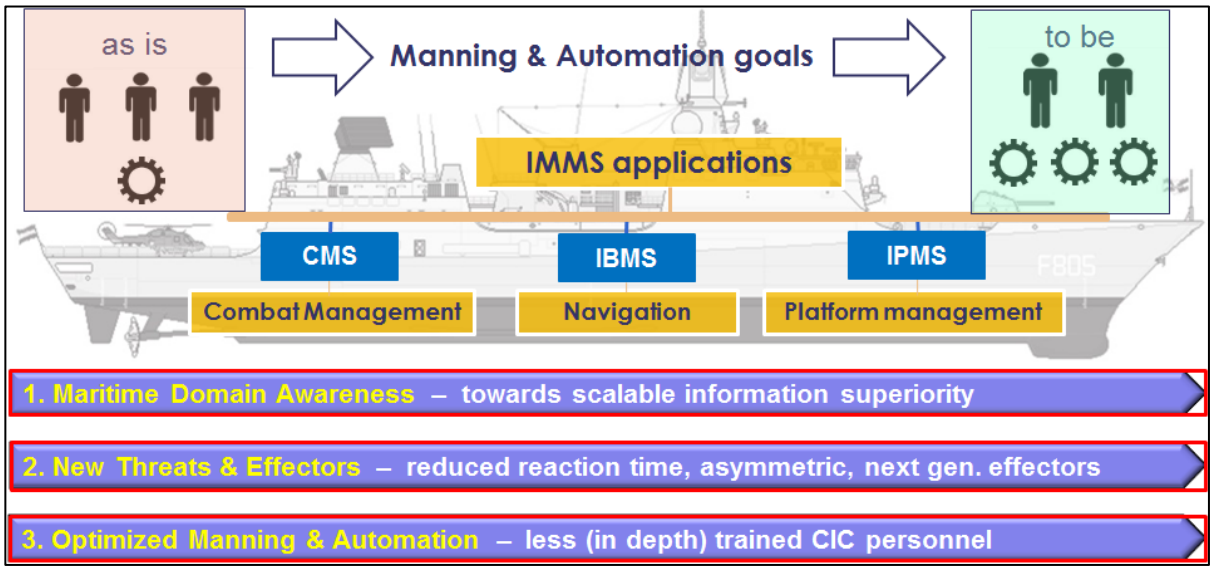

Fig. 2-1. A *CMS fulfilling the three main themes of actual R&T business lines*

 https://doi.org/10.24868/issn.2515-818X.2020.042

This explains why R&T needs the latest technologies to provide solutions (beyond system E) for their themes.

2.1. Harnessing Innovation for the Realization of R&T main themes

The new innovative technology approaches that allow to create a System X beyond optimized conventional systems A-E are now represented in their main general lines. Quite understandable, this paper introduces only the main directions of solutions proposed in very limited manner due to confidentiality and space.

2.1.1. Trust vs. Trustworthiness: the need for silicon-based Security

The following example explains the notion of trust vs. 'trustworthiness', a term that once was coined by Microsoft. Trust –it does not matter if in 'real life' or in Cyber– is something that was earned in the past. If a system worked well in the past, then one may think of it as a trusted system. Always clear, with no 100% guarantee that this system in the current and at any future moment will be working well, too: cf. Fig. 1-1 with the green, theoretical point that promises 100% Security: yes, but only in theory.

A system that can prove that it is operating secure -at any one given moment in time-, can be seen for that moment as 'trustworthy'. Now, we will focus again on trust instead of trustworthiness.

If a system was built in a way that its integrity can be checked from another system entity, then the checking system is able to attest that the checked system possesses this integrity at a given moment in time. (It will be further shown that for our trusted system X it is inevitable to enforce Security by strong hardware-based measures in further dimensions, i.a. like authenticity and non-repudiation.)

Now, from an ensured integrity property one may conclude that the checked system is secure. This is the idea behind using a separate system that checks the integrity of another system where it is attached to. It is a well-known fact in Security that a system cannot check its own integrity reliably. Therefore, this second separate system is absolutely necessary in order to check the integrity of the first system.

When this 'integrity-checking' capability is enhanced in more dimensions like authenticity and non-repudiation and if it also enforced by a special hardware (that compared to software is more difficult to tamper), we then speak of Trusted Hardware. Trusted Hardware is an inevitable Security building block for the creation of trusted systems, e.g. the trusted CMS.

Embodiments are i.a. Trusted Platform Modules (TPMs) as originally specified by the Trusted Computing Group (TGC), or Hardware Security Modules (HSM) where THALES is one of the world-leading suppliers, besides further other products.

2.1.2. Risk Analysis precisely tailored on any given Naval Context

Like any other 'conventional' Security measures, the usage of silicon-based Security hardware is not proposed for every point, every node, every real- or virtual-machine within a THALES naval platform. This would just lead to unwanted effects like the maximization of the attack surface. So, more scrutiny is needed here.

The chosen approach is to identify crucial points by a rigorous in-house developed (agile) RA. As a concerted effort this RA is undertaken based on an agile EBIOS Risk Manager [5] method and the RA is thus filled with the broad and diverse expertise of Security experts, naval architects, system engineers and customer feedback.

The further thoroughly considered, stepwise application of the findings is key for shifting Security, Usability and Cost to better levels, or in words of Fig. 1-1: shifting from system E to system X.

2.1.3. Considering the real Security Aspects of modern Naval Platforms

As said, this chapter can only explain some of the general basic Security principles that silicon-based Security hardware offers within an orchestrated solution that must be derived from a thoroughly thought-out, rigorous RA. The following examples focus on fully automatized authentication procedures for which the term Machine Authentication Continuum is coined. It can be executed within milliseconds triggered by timers or other events, maybe as part of a (intrusion or any other) detection system.

 https://doi.org/10.24868/issn.2515-818X.2020.042

2.1.4. The Machine Authentication Continuum between two parties

When two parties, Alice (A) and Bob (B) are present, three different main stages exist in general: A authenticates vs. B, B vs. A, or anything in between. The following figure depicts this in form of a continuum.

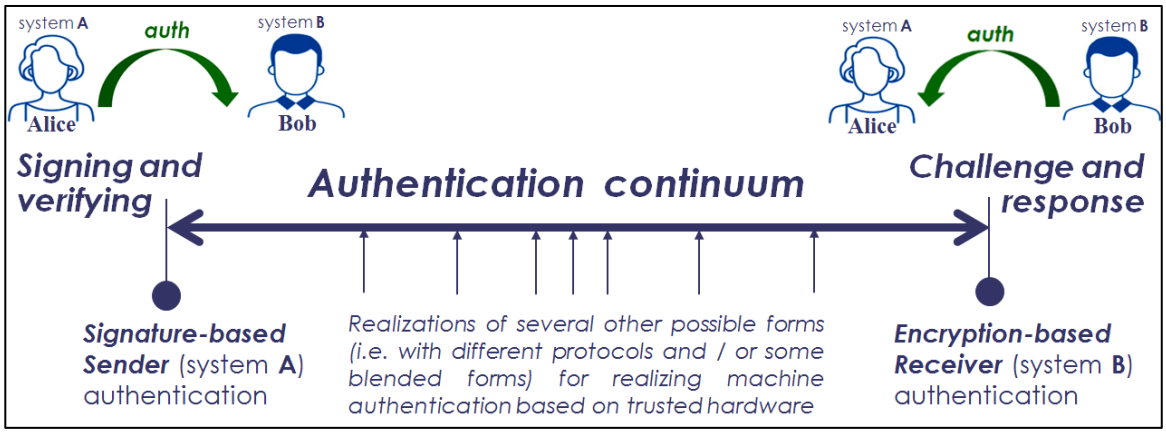

Fig. 3-1. *The Machine Authentication Continuum for two parties:* Alice (A) and Bob (B)

The left side of this Machine Authentication Continuum, signing and verifying, explains the principle of using electronic signatures, see the figure below, with one silicon-based Security hardware element contributing to a trusted communication.

2.1.5. Left side: sign/verify on silicon-based Security hardware

A working CMS-demonstrator has been realized based on the following scheme:

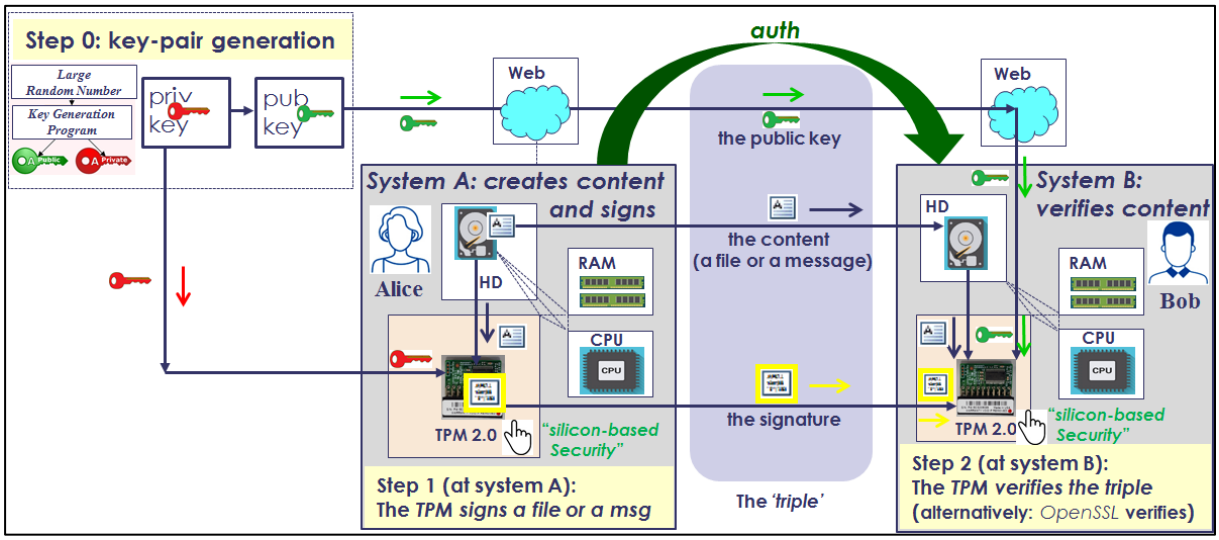

Fig. 3-2. *Trusted Hardware based principle of electronic signing and verifying:* Alice authenticates vs. Bob

The principle works as follows: in a first preoperational step a public-private key pair is generated. This can be done via a key generation program, or in this case it was directly realised by a TPM 2.0. The private key is then loaded into the TPM of A.

The public part is transferred via the ship network to B where it is loaded into the TPM of B. (Alternatively A and B can of course be realised by pure software solutions, i.e. in the form of OpenSSL.) One advantage of using silicon-based Security hardware is that it is way more difficult to tamper than software that is 'soft'.

 https://doi.org/10.24868/issn.2515-818X.2020.042

When A creates content (this can be a document, a file or part of a message) the TPM of A can calculate an electronic signature that together with the content is sent to B, where all three parts of the 'triple' (the public key of A, the content of A and the signature of A) are used by the TPM of B (or alternatively, the OpenSSL of B) in order to verify if the electronic signature matches to the public key and the content.

The cryptographic strength that TPM A (or alternatively, the OpenSSL of A) provides, ensures that the content of A actually comes from A and that it has not been tampered with, i.e. by a man-in-the-middle between A and B. B can rely on the fact that only A has signed the message and offers thus -beyond integrity- further Security qualities like non-repudiation and authenticity.

When the content is extended to the internal system state of A, i.e. measurements that A only can provide after a successful trusted boot, or more general, only after providing the right system integrity measures, B knows for sure that not only the content, but also the whole system A is within a trustable state, or in other discussed terms: in a trustworthy state at this given moment in time.

A further advantage is that the triple, here generated by silicon-based Security, can even be sent in plain between A and B. It can of course be encrypted for the transfer, but for guaranteeing the above just named Security quantities, this is not a necessary precondition.

Again, this is a further advantage in realizing trusted communication within complex systems (of systems), i.e. for a trusted information exchange with or within a trusted CMS within very short time intervals and maybe continuously generated encryption keys.

2.1.6. Right side: Challenge/Response on silicon-based Security hardware

The right side of the authentication continuum, cf. Fig. 3-1, is used when Bob needs to authenticate vs. Alice, where the challenge and response procedure again is realized by silicon-based Security hardware. (Alternatively, this can be realised by pure software solutions, i.e. in the form of OpenSSL.)

The first step, to prepare both systems A and B, needs to be done before the procedure starts. It is beneficial to do this preparation work e.g. at the supplier's factory. It is shown in the figure below:

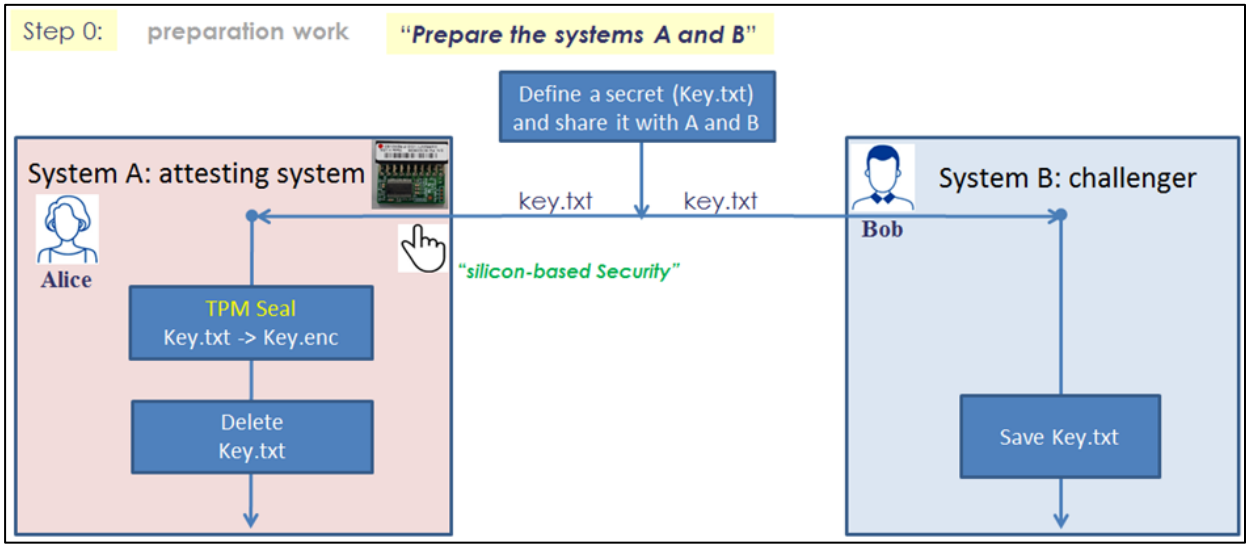

Fig. 3-3. *Trusted Hardware based principle of challenge and response:* Step 0 – preparation work –

After having the common initial key at both systems, a challenge is sent from Bob to Alice. This can be initialized by a trigger sent from A, i.e. a connection request, or at B, i.e. by the expiry of a timer as shown in the figure below:

 https://doi.org/10.24868/issn.2515-818X.2020.042

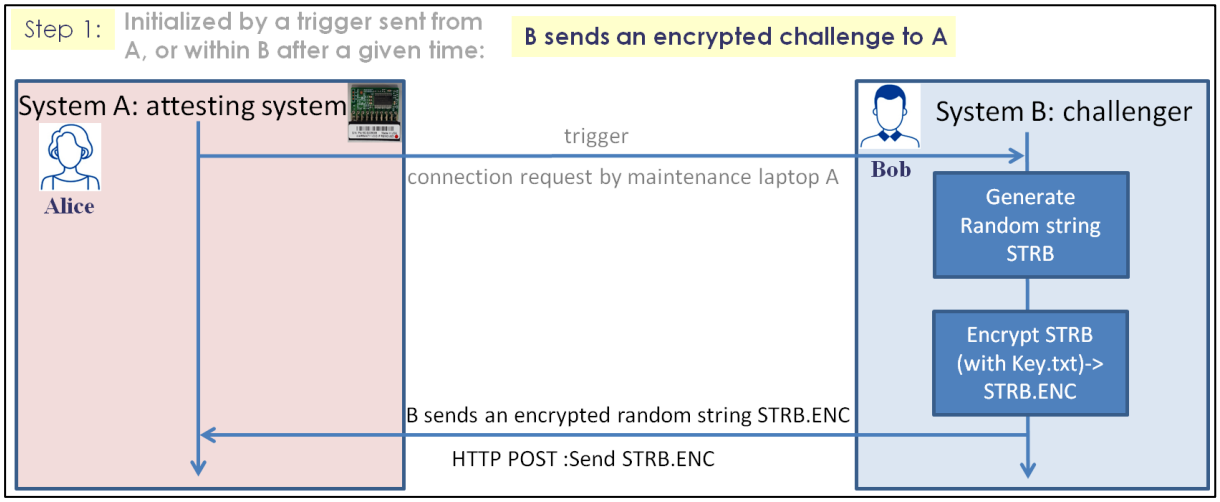

Fig. 3-4. *Trusted Hardware based principle of challenge and response:* Step 1 – the challenge –

For step 1 no silicon-based Security hardware is necessary. After having received at A the request from B, A sees -by using his TPM- if B has correctly authenticated by using the correct encryption key.

Based on a Security policy, A can decide on any other steps (deliberately not drawn here) or step 2:

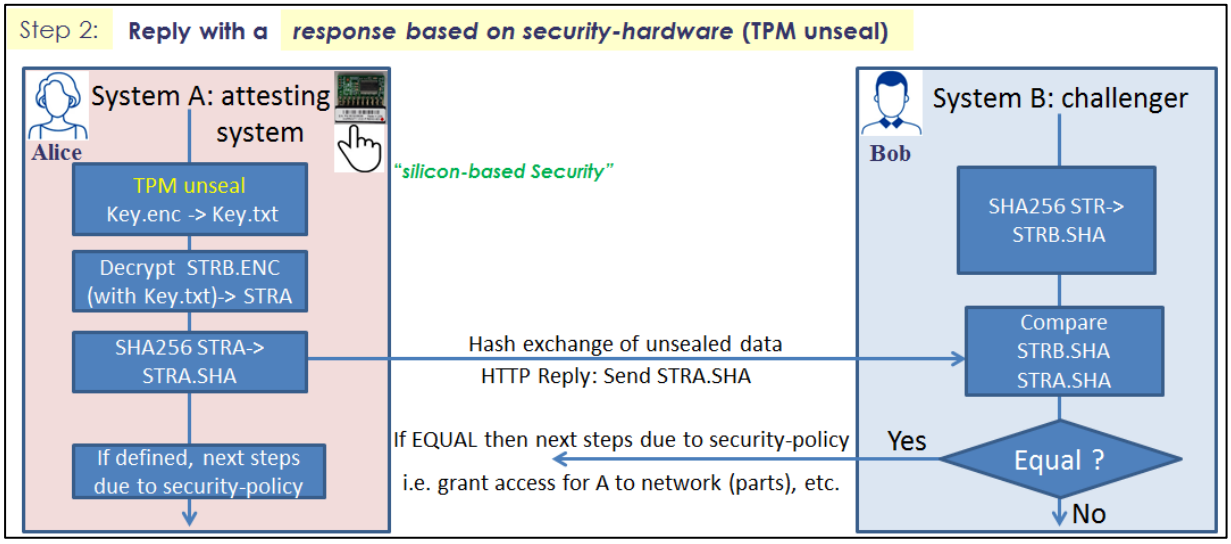

Fig. 3-5. *Trusted Hardware based principle of challenge and response:* Step 2 – the response –

Let us assume A decided to response by sending the hash value of his decrypted string. The challenger B can then compare if this response of A, the hash of his challenge B sent earlier, is equal to the calculation executed by his *maybe* own silicon-based hardware at B (therefore not shown in the figure above), or alternatively by software.

Depending on the result of this comparison B can then follow any steps proposed by a Security policy.

As already indicated in chap. 2.1.5., A and/or B can of course be realised by pure software solutions, i.e. in the form of OpenSSL.

By using silicon-based Security hardware, the same previously discussed advantages apply. One of them is again that the usage of silicon-based Security hardware is way more difficult to tamper than software that is 'soft'.

 https://doi.org/10.24868/issn.2515-818X.2020.042

2.1.7. Further new innovative Security solutions by THALES Naval

With these and the innovative application of further cybersecurity principles that are not disclosed here for obvious reasons, one can expect new and innovative approaches that are already in preparation.

2.2. Transition from Challenge/Response to Remote Attestation

To provide a general example of a practically possible use case, think about extending the discussed challenge and response procedure, now in terms of remote attestation (RA). Remote attestation is simply said: an attestation of the integrity and proper function of a crucial system A by a separate, challenging system B. This points to use cases that are interesting not only for naval contexts:

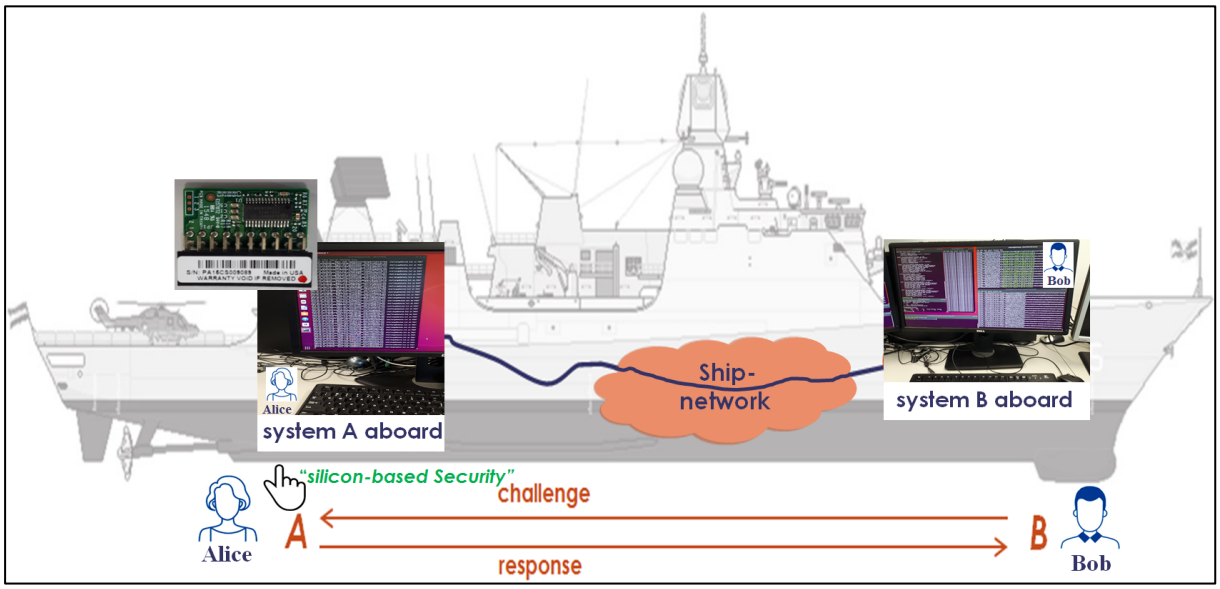

Fig. 3-6. *Remote Attestation where the challenging system B is local (aboard own ship)*

This remote attestation can be done aboard the own ship for separated systems, or network segments. Or generalized, the remote attestation can be realized extended between own ship and shore, too.

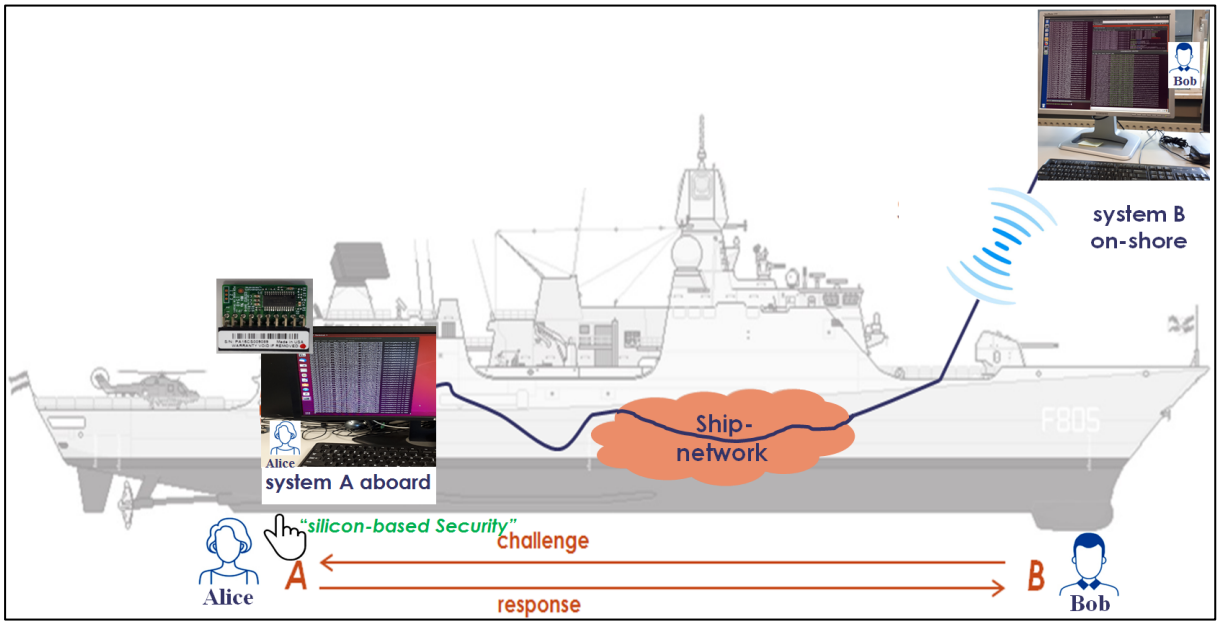

Fig. 3-7. *Remote Attestation where the challenging system B is remote (on-shore)*

 https://doi.org/10.24868/issn.2515-818X.2020.042

2.3. Integrating Security into modern platform architectures

It is worth to notice that the principles that are discussed here as part of a trusted CMS information exchange are just a very small set of the way broader set of cyber capabilities that silicon-based Security hardware offers.

The R&T business lines are thus further continuously checking and developing new methods to provide high-class Security systems as part of the fascinating ongoing THALES cybersecurity journey.

3. Summary

3.1. Conclusion

The discussion of the Machine Authentication Continuum shows the high degree of protection potential that silicon-based Security can deliver, provided that it is applied based on a thoroughly worked out in-depth risk management that considers more Security perspectives than just the three dimensions of the CIA-triad.

When such a rigorous risk analysis (independently if it is EBIOS or any other method suited for a given context) is properly undertaken with the help of (naval) stakeholders, their discussed risk perception will finally lead to decisive Security insights, so that finally the right and well balanced Security measures can be identified.

To optimize a complex system beyond conventional borders, usage of new and suited technologies is inevitable. Here, even the simple use cases that were derived from the elaborated Machine Authentication Continuum, demonstrate how silicon-based Security can considerably improve the Security of naval platform systems.

3.2. Outlook

The progress seen in recent developments of silicon-based IT solutions lets emerge new Security innovations that future, strong competitive IT-environments will incubate. Even the silicon-based COTS hardware that was used here for demonstrating all delineated Security schemes, already encompasses a plurality of Security functions and Security features. The skilled person can imagine what is possible in a close future.

Acknowledgements

The author thankfully expresses his gratitude to THALES team members for their fruitful review contributions.

References

[1] Bundesamt für Sicherheit in der Informationstechnik: ‚Das Trusted Platform Module (TPM) und vertrauenswürdige Informationstechnik. Informationen zum zentralen Baustein des Trusted Computing…‘, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/dastrustedplatformmoduletpm_node.html

[2] Parker, Donn B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. New York: NY: John Wiley & Sons. ISBN 0-471-16378-3.

[3] ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques

[4] ISO Guide 73:2009 – Risk Management – Vocabulary

[5] EBIOS (Risk Manager) method https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

 https://doi.org/10.24868/issn.2515-818X.2020.042