Cyber Resilience Assessment and Certification: from Standards to Practice in the Context of NIS2, CSA & CRA

Emil SIMION

Associate professor, University POLITEHNICA of Bucharest

BlueSpace Technology SA

emil.simion@upb.ro, emil.simion@bstech.ro

Motivation

- Increase of cyber attacks on systems: Killnet
- Complex architectures: Crowdstrike incident

Killnet

- **Main activity:** DDoS attacks on critical infrastructures.
- **Targets:** Government websites, NATO institutions, airports, hospitals, critical digital infrastructures.
- **Notable attacks:**

  Romania (2022): Government websites, transport infrastructures (Otopeni Airport) https://www.antena3.ro/actualitate/site-aeroporturi-romania-atacate-hackeri-killnet-638078.html

  Lithuania: Government platforms, in response to sanctions.

  Italy: Hospitals and other public services.
- **HC3 report:** https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf

Crowdstrike incident (2024)

- https://hbr.org/2025/01/what-the-2024-crowdstrike-glitch-can-teach-us-about-cyber-risk
- https://healthmanagement.org/c/artificial-intelligence/News/crowdstrike-global-it-outages-impact-on-healthcare-and-beyond
- **Analysis:** The flawed update was the result of an error in the development and testing process for software updates. Instead of being rigorously tested before deployment, the update was distributed without proper checks, leading to incompatibilities and system crashes.
- **Lessons Learned:** The Importance of Rigorous Testing, Implementing a Gradual Update Process, Monitoring and Responding Quickly, Collaborating with Partners.

Agenda

- Black swan
- Model for security
- Types of evaluations
- Relevant standards & legislation
- Use case: MERISD3C-QKD project

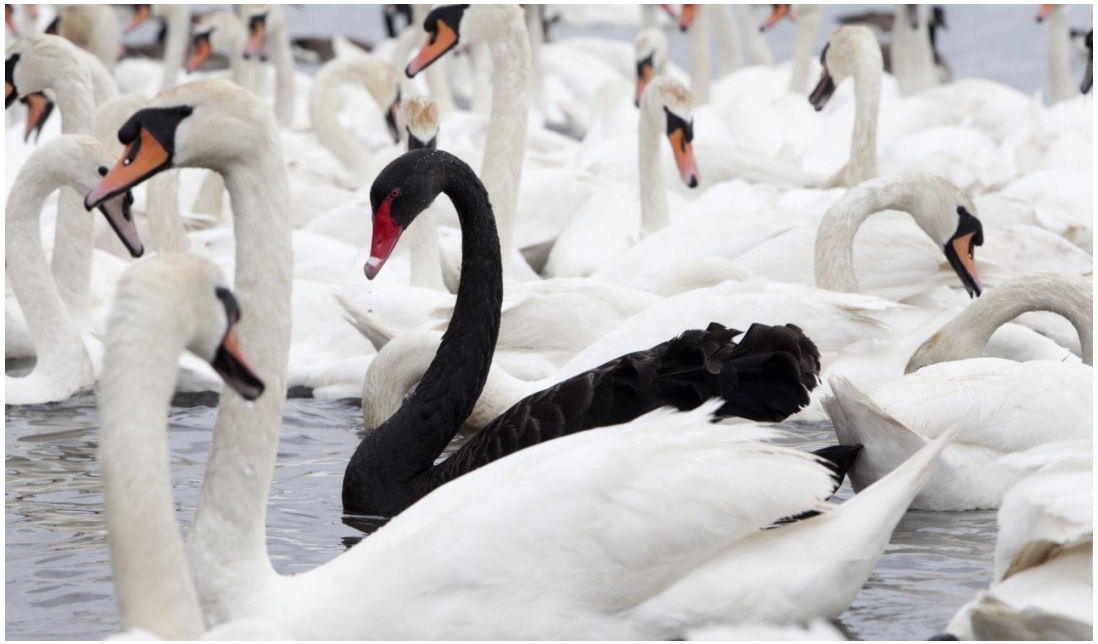
Threats classification

- Terrestrial
- Maritim
- Air
- Spatial
- Cyber

Factors that enhance cyber threats

- the existence of technological, procedural and human vulnerabilities that manifest themselves at the level of targeted networks and IT systems;
- the availability and accessibility of hacking resources;
- the low level of cybersecurity culture and hygiene in cyberspace;
- insufficient training and specialization in the field of cybersecurity of employees and managers;
- normative and procedural deficiencies;
- the expansion of the range of devices;
- the lack of a regulatory framework and policies for managing cyber risks in the supply chain.

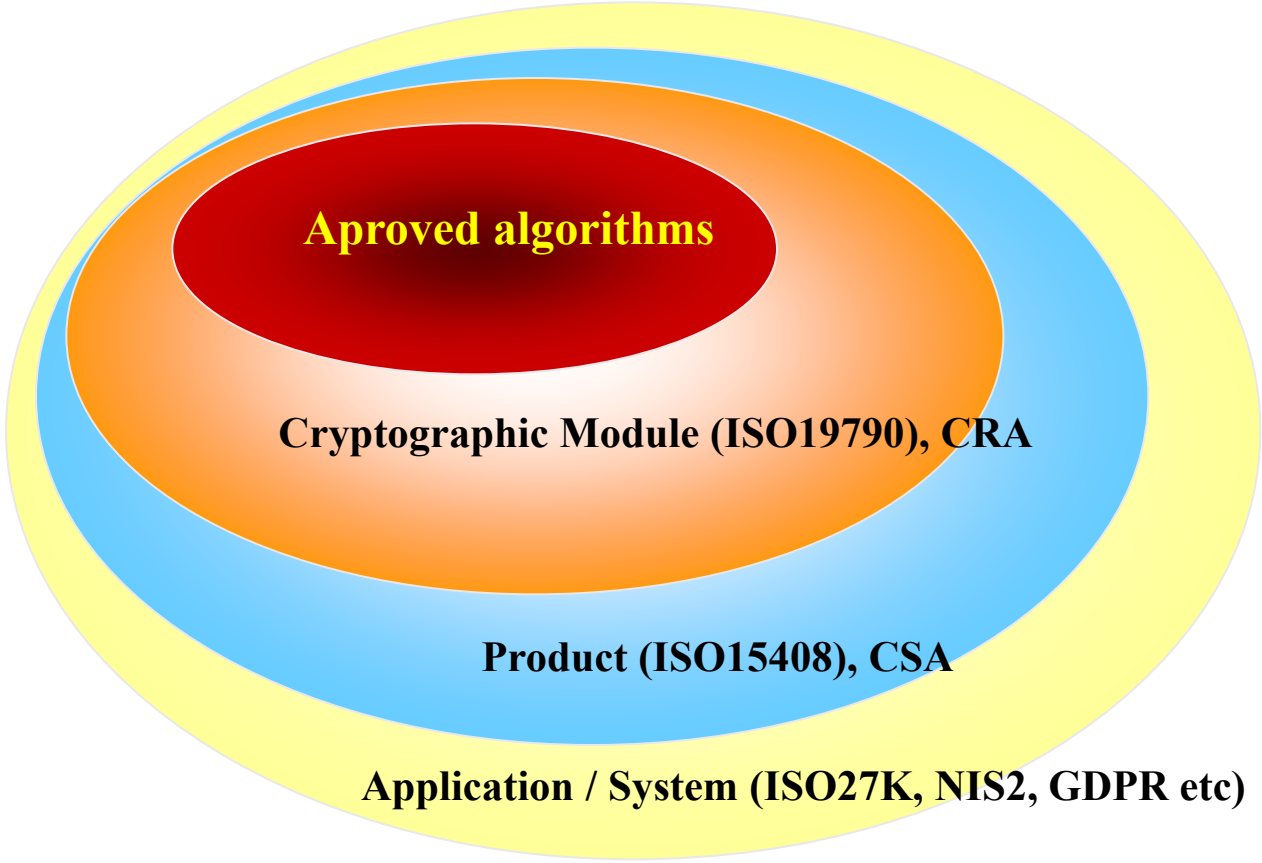
Black swan in real world (physical & virtual)?



- Nassim Nicholas Taleb: Black swan event to be rare, to be unforeseen (hence an unlikely event), to have a major impact and to be explained ***only*** after its occurrence.
- Examples: the rise of the Internet, the personal computer, World War I, the dissolution of the Soviet Union, the September 11, 2001 attacks, Fukushima Daiichi nuclear disaster.

Model for security

Cryptographic algorithms are mathematical objects used in cryptographic modules (software, firmware and/or hardware) . These **crypto-modules** are used to **design cryptographic products** (applications and/or devices). The cryptographic products are used to protect data in **communication systems** or in **specific applications**.

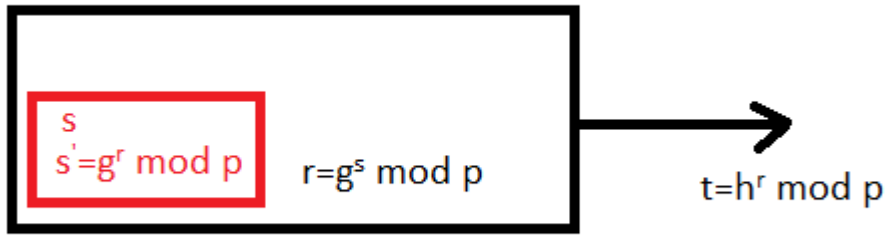


Algorithm evaluation

- Easy to understand and implement;
- Memory requirements;
- Suitable for both hardware and software implementations;
- Processing speed adaptable to new technologies;
- Security evaluation under different modes (e.g.: cryptanalysis, MITM, brute force attacks etc.)

Example of randomness failure ...

- p prime number, g și h (random) < p;



- Trap: $g=h^e \bmod p$:
  - Can not be proved!
  - Usage: $t^e \bmod p = s'$ exposing the secret code.

Cifrare cu autentificare

- Necesitatea cifrării autentificate. Există 3 posibilități de implementare a cifrării autentificate:

  SSL: a = *Auth*(x), C = *Enc*(x, a), transmit C

  IPSec: C = *Enc*(x), a = *Auth*(C), transmit (C, a)

  SSH: C = *Enc*(x), a = *Auth*(x), transmit (C, a).

Cryptographic module evaluation

- FIPS 140-3 echiv ISO19790;
- 4 leves of security;
- Functional security requirements;
- Security requirements;
- Others aspects.

Security requirements

- Cryptographic Module Specification;
- Cryptographic Module Ports and Interfaces:
  - L3-L4: Data ports for unprotected critical security parameters logically or physically separated from other data ports;
- Roles, Services, and Authentication:
  - L1: Logical separation of required and optional roles and services.;
  - L2: Role based; L3: Identity based
- Finite State Model;
- Physical Security;
- Operational Environment;
- Cryptographic Key Management;
- Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC);
- Self-Tests: Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests;
- Design Assurance;
- Mitigation of Other Attacks.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Common Criteria (echiv. ISO15408)

- **Trusted Computer System Evaluation Criteria** -1983, NSA;
- **Canadian Trusted Computer Product Evaluation Criteria**, 1993 by the Communications Security Establishment to provide an evaluation criterion on IT products;
- **Information Technology Security Evaluation Criteria,** May 1990 in France, Germany, the Netherlands, and the United Kingdom;
- **Common Criteria**, 30+ members.
- **EUCC**

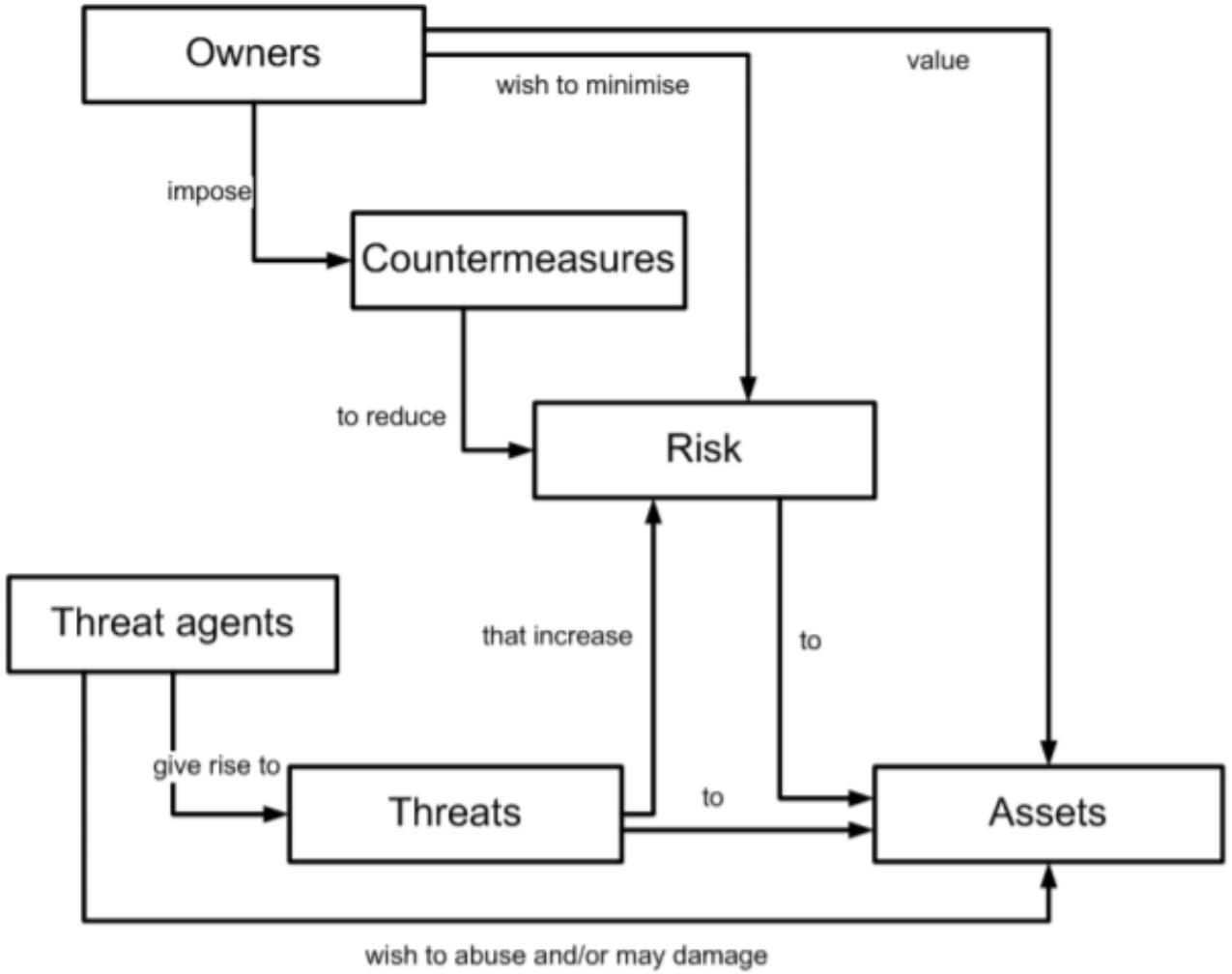
Evaluation

- Security Assurance Requirements (SARs) – descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality;
- Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements:
  - EAL1: Functionally Tested
  - EAL2: Structurally Tested
  - EAL3: Methodically Tested and Checked
  - EAL4: Methodically Designed, Tested and Reviewed
  - EAL5: Semiformally Designed and Tested
  - EAL6: Semiformally Verified Design and Tested
  - EAL7: Formally Verified Design and Tested
- The fourth document called the Common Methodology for IT Security Evaluation (CEM) describes the methodology that evaluators use to check compliance for each required Security Assurance component.
- The Protection Profile (PP) document establishes a set of security marketing requirements for a class of products to serve a specific market. The intent of the PP is to allow consumer groups and communities of interest to express their security needs, for instance a PP may address firewalls or for Java-enabled smartcards. The PP provides details on the level of security that must be met, including a description of security threats to be mitigated, and establishes security assumptions regarding the environment.

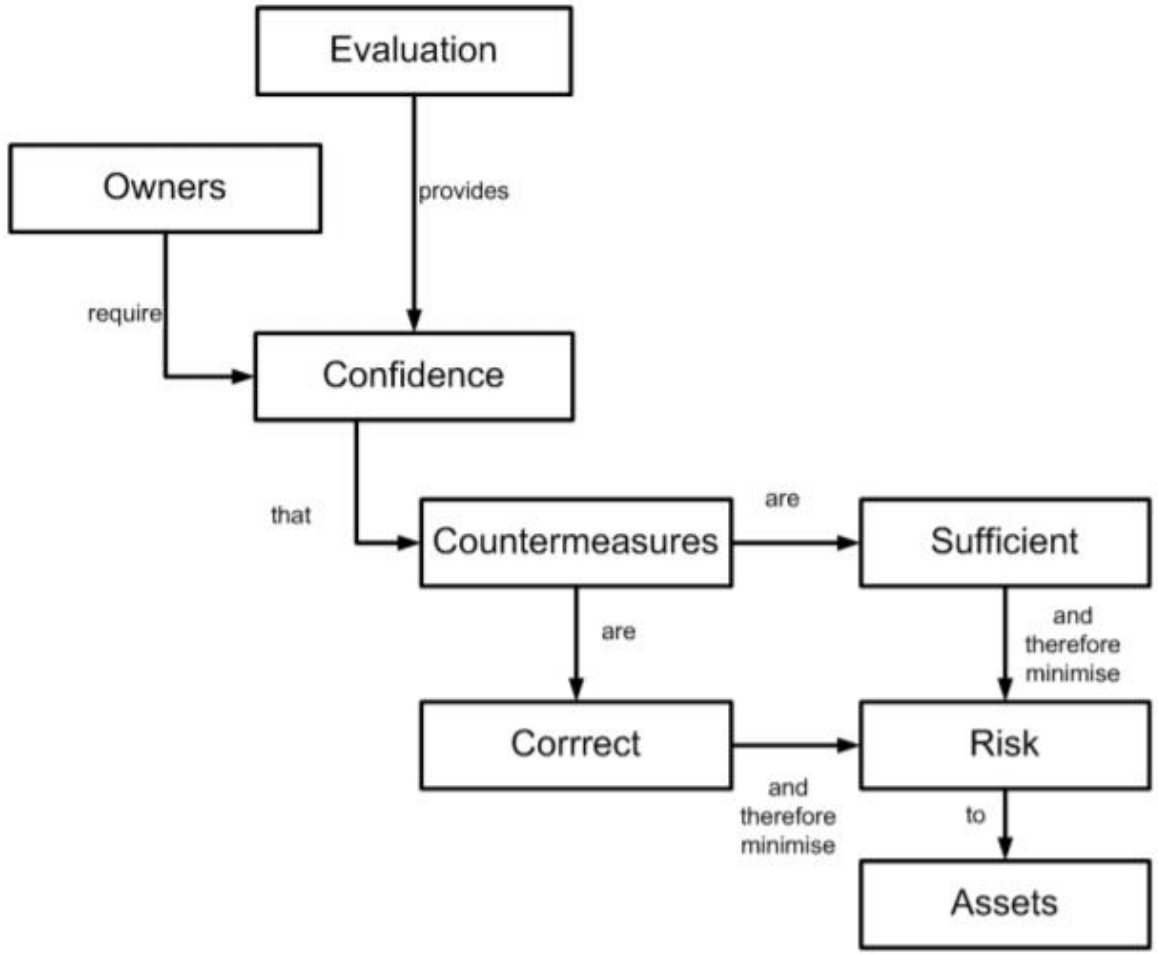
Application/product evaluation

- Common Criteria (https://www.commoncriteriaportal.org/) echiv. ISO15408;
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements
- Target of Evaluation (TOE) – the product or system that is the subject of the evaluation;
- Protection Profile (PP) – a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose;
- Security Target (ST) – the document that identifies the security *properties* of the target of evaluation. The ST may claim conformance with one or more PPs;
- Security Functional Requirements (SFRs) – specify individual security functions which may be provided by a product;

Part 1: General Model: Security concepts and relationships



Part 1: General model: Evaluation concepts and relationships



Part 2: Security functional requirements

- Security functional components: class/family/component
- Class FAU: Security audit: Security audit automatic response, Security audit data generation, Security audit analysis, Security audit review, Security audit event selection, Security audit event selection;
- Class FCO: Communication: non-repudiation of origin, non-repudiation of receipt;
- Class FCS: Cryptographic support: Cryptographic key management, Cryptographic operation
- Class FDP: User data protection: access control policy, access control function, data authentication, export form TOE, information flow policy, …. 11- families;
- Class FIA: Identification and authentication: auth failures, user attribute definition, specification of secrets, user authentication, used identification, user-subject binding,
- Class FMT: Security management: management of functions in TSF, management of security attributes, management of TSF data, revocation, security attribute expiration, specification of security functions, security management roles;
- Class FPR: Privacy: Anonymity, Pseudonymity, Unlinkability and Unobservability
- Class FPT: Protection of the TSF: 14 families;
- Class FRU: Resource utilization: Fault Tolerance, Priority of Service, Resource Allocation
- Class FTA: TOE access: 6 families;
- Class FTP: Trusted path/channels: inter-TSF trusted channel, trusted path.

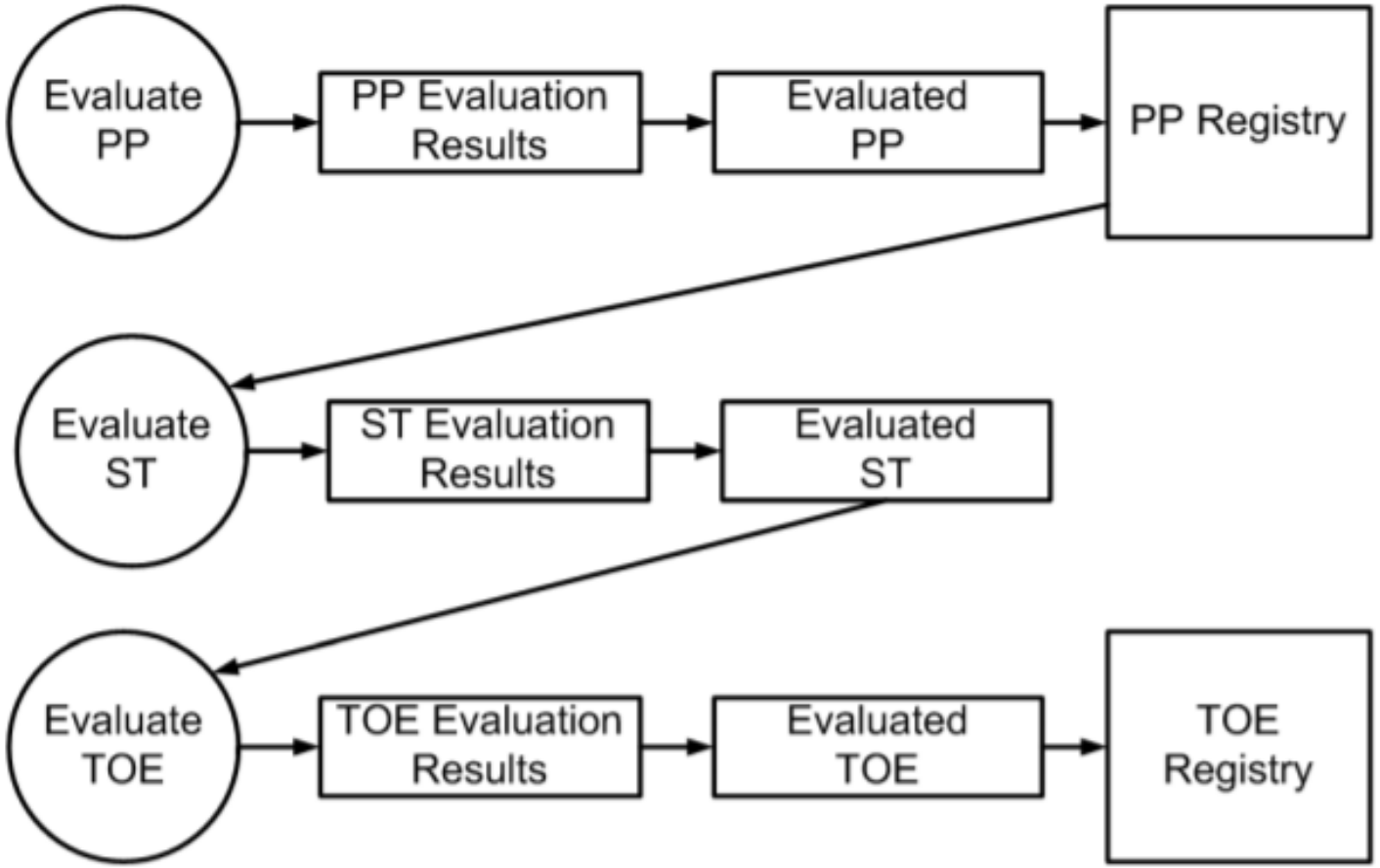
Part 3: Security assurance requirements

- **Development**: arhitectural design, functional specification, design of toe, implementation representation, TSF internals, security policy modeling;
- **Guidance Development**: operational user guidance, preparative user guidance;
- **Life Cycle**: life cycle definition, configuration management scope and capabilities, security during development, delivery security, flow remediation, tools and techniques;
- **Tests**: functional testing (plans, procedures and records), testing coverage analysis, testind depth analysis, independent testing;
- **Vulnerabilities Assessment**: Vulnerability Analysis;
- **Composition**: composition rationale, development evidence, dependent component, base TOE testing, composition vulnerability analysis.

Evaluation

- Security Assurance Requirements (SARs) – descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality;
- Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements:
  - EAL1: Functionally Tested
  - EAL2: Structurally Tested
  - EAL3: Methodically Tested and Checked
  - EAL4: Methodically Designed, Tested and Reviewed
  - EAL5: Semiformally Designed and Tested
  - EAL6: Semiformally Verified Design and Tested
  - EAL7: Formally Verified Design and Tested
- The fourth document called the Common Methodology for IT Security Evaluation (CEM) describes the methodology that evaluators use to check compliance for each required Security Assurance component.
- The Protection Profile (PP) document establishes a set of security marketing requirements for a class of products to serve a specific market. The intent of the PP is to allow consumer groups and communities of interest to express their security needs, for instance a PP may address firewalls or for Java-enabled smartcards. The PP provides details on the level of security that must be met, including a description of security threats to be mitigated, and establishes security assumptions regarding the environment.

Evaluation results



Common points and differences

- FIPS focuses on cryptographic module itself <->CC examines the security functionality of the module;
- An interesting point regarding Common Criteria is that the “certification” of cryptographic mechanisms is usually left to the FIPS 140-2 process, rather than detailed in the Common Criteria standard;
- Both FIPS 140-2 and Common Criteria require design and manufacturing teams to follow a written configuration management process and user-guidance manuals;

Evaluation/certification process FIPS vs. CC;

- An outside evaluation laboratory conducts evaluation and/or validation of a security product for both FIPS 140-3 and Common Criteria. An early step with both certification processes is to contract with a lab to perform evaluation, and turn the results over to NIST for certification. The typical sequence for each certification process follows.

FIPS Certification	CC Certification
- The product vendor selects an evaluation laboratory; - The evaluation lab conducts a 2 or 3-day initial assessment work session with vendor; - A schedule is prepared to map out availability of FIPS required documents, module design changes that are required, FCC testing, FIPS 140-3 testing, etc; - A letter from NIST formally kicks off the evaluation effort by the laboratory; - The FIPS process allows that once FIPS 140-3 required testing documentation is received by the laboratory, the product can be listed on the NIST Pre-Validation website as “under test”; - During the evaluation, the implementation of each of the cryptographic algorithms is tested by the evaluation lab; - On-schedule delivery of deliverables and timely resolution of problems is required to keep the project on-track; - When the testing is successfully completed, the lab turns over the final evaluation results to NIST for review; - If successful, NIST will issue a FIPS 140-2 certificate within 8-to-20 weeks, depending on the NIST activity level.	- The vendor selects a CC evaluation laboratory for NIAP or ISO-15408 certification; - The evaluation lab conducts a 2-or-3 day initial assessment work session with the vendor; - Creation of Security Target document for submission to the lab A Project Plan and schedule are prepared for availability for all NIAP required deliverables (Typically prepared in parallel with the ST document creation) ; - A formal contract is provided by testing lab; a signed contract is ready; - NIAP Oversight Board project launch meeting–Requires ST for submission, the Project Plan, and approved testing-lab contract - Evaluation of ST begins first. Formal evaluation of the ST is not complete until entire NIAP evaluation is completed; - Evaluation of design documentation, Configuration Management, testing and other Security Assurance evidence continues; - On-schedule delivery of deliverables and timely resolution of problems; - Preparation of Evaluation Technical Report by lab; - Submission of Evaluation findings to NIAP; - Review by NIAP. (usually takes about 4-to-10 weeks) and Certification is granted by NIAP.

System evaluation

- ISO/IEC 27000 provides an overview of information security management systems;
- Some evaluation areas:

  - Information **S**ecurity **M**anagement **S**ystem requirements standard, formally specifying a certifiable ISMS;
  - Code of practice for information security controls describing good practice information security control objectives and controls;
  - Information security management measurement;
  - Information [security] risk management;
  - Auditing the *management system* elements of an ISMS;
  - The assessment of 'technical' security controls;
  - **P**ersonally **I**dentifiable **I**nformation in public clouds;
  - Cybersecurity
  - ….

Vulnerability scanners

- NESSUS: https://www.tenable.com/products/nessus
- MBSA: Microsoft Baseline Security Analyzer
- Checkmarx: https://www.checkmarx.com/
- HCL (IBM) Appscan: https://www.hcltechsw.com/products/appscan

Relevant standards & legislation

Level	Act / Schemes	Main Purpose	Status
Legislative	**Cybersecurity Act (2019/881)**	Legal framework for EU certification	In force
Schemes	**EUCC, EUCS, EU5G**	Certification of products / services	EUCC completed, EUCS & EU5G in progress
Complementary	**CRA, NIS2, CER**	Obligations for operators and manufacturers	Under implementation
Standardization	**ISO/IEC 15408, 27001, etc.**	Technical basis for evaluation	In use

Technical challenges (in health systems)

- 5 knows in security
- Confidential computing
- Decentralized trust
- Intelligent automation and AI Governance

Takeaway

Protection level	Short decryption
Algorithm	Type: Symmetric, asymmetric Security: Unconditionally secure, computationally secure
Cryptographic module	FIPS140-3/ISO19790, 11 areas
Application	CC/ISO15408, 11 areas
System	27000k, more then 50 standards, NIS2

- 5 Knows in security.
- Remember don’t ask if a black swan will appear! It is a question of time.

Cyber challenges

- Atacuri bazate pe IA care pot produce deep fake cu impact;
- Vulnerabilitatea sistemelor traditionale (actualizari nesigure, probleme de compatibilitate);
- Securitatea in cloud;
- Securitatea sistemelor din zona de sanatate;
- Atacuri pe lantul de aprovizionare;
- Atacuri cibernetice motivate financiar (manipularea pietelor financiare).

RESPONSABIL NIS



Politici de securitate

Risk Management

Răspuns la incidente

Conformitate legală

Studiu de caz: MERISD3C-QKD

- **Parteneri:** BLUESPACE TECHNOLOGY și Institutul Național de Micro Tehnologie, PN-IV-P7-7.1-PTE-2024-0735, Perioada de derulare: 24.07.2025-23.07.2027.
- **Scopul proiectului:** Dezvoltarea unui lanț complet de comunicație cuantică (TX–RX) integrabil în sisteme de distribuție de cheie cuantică, cu nivel ridicat de securitate și reziliență cibernetică.
- **Descriere:**
  - Subsistem TX – emisie controlată de fotoni individuali cu polarizare randomizată (RNG–FPGA–Laser).
  - Subsistem RX – detecție optică, etichetare temporală și corecție a erorilor, asigurând integritatea și sincronizarea datelor.
- **Integrarea TX și RX prin implementarea rezilienței cibernetice end-to-end:**
  - protecție împotriva scurgerilor de canal lateral (EMSEC, atacuri prin temporizare);
  - controlul aleatorismului și al polarizării verificabile;
  - sincronizare si tolerantă la erori sub constrângeri fizice.
- **Prototipul integrat TX–Rx** este construit astfel incat să poată fi validată rezilienta cibernetice în conformitate cu Anexele I si II din CRA (Proiectare și testare).
- https://bstech.ro/category/academics-ro/meris3c-qkd/

References

- Common Criteria portal https://www.commoncriteriaportal.org/
- ISO 15408: https://www.iso.org/standard/50341.html
- FIPS 140-2 portal: https://csrc.nist.gov/publications/detail/fips/140/3/final
- ISO 19790: https://www.iso.org/standard/52906.html
- NIAP portal: https://www.niap-ccevs.org/
- CSA: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0881-20250204
- CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R2847-20241120
- NIS2: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227
- CER: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
- AI ACT: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=OJ:L_202401689
- https://bstech.ro/category/academics-ro/meris3c-qkd/

Q&A