INTERNET OF TRUST

Securing the dynamic: adapting certification and increasing assurance for Moving Target Defense

Mohamad Hajj

AMTD 2025 - International Workshop on Applications of Moving Target Defense

Bucharest, 28th of May 2025

Agenda

- MTD techniques across domains
- Why this matters
- Certification Conundrum: Static vs. Dynamic
- Introducing Common Criteria (CC)
- What is the EUCC (EU Common Criteria Scheme)?
- Case study: SE Singularisation
- Adapting Certification for MTD
- Recommendations for Certifiers and Evaluators
- Takeaways

MTD techniques across domains

- OS/Software: e.g., ASLR, ISR, binary obfuscation
- Cloud/Infrastructure: e.g., IP hopping, container re-deployment
- Hardware: e.g., SE singularisation
- Network: e.g., dynamic routing/topology (SDN), port mutation

Why this matters: static defenses vs. dynamic threats

- Digital landscape is inherently dynamic: new threats, Evolving software, Cloud environments

- Traditional approach: largely static
  - Build a wall
  - Patch known vulnerabilities
  - Assume fixed attack surface

- The mismatch:
  - Cyber threats are increasingly adaptive and fast-moving.
  - Static defenses are being outpaced by dynamic attackers.

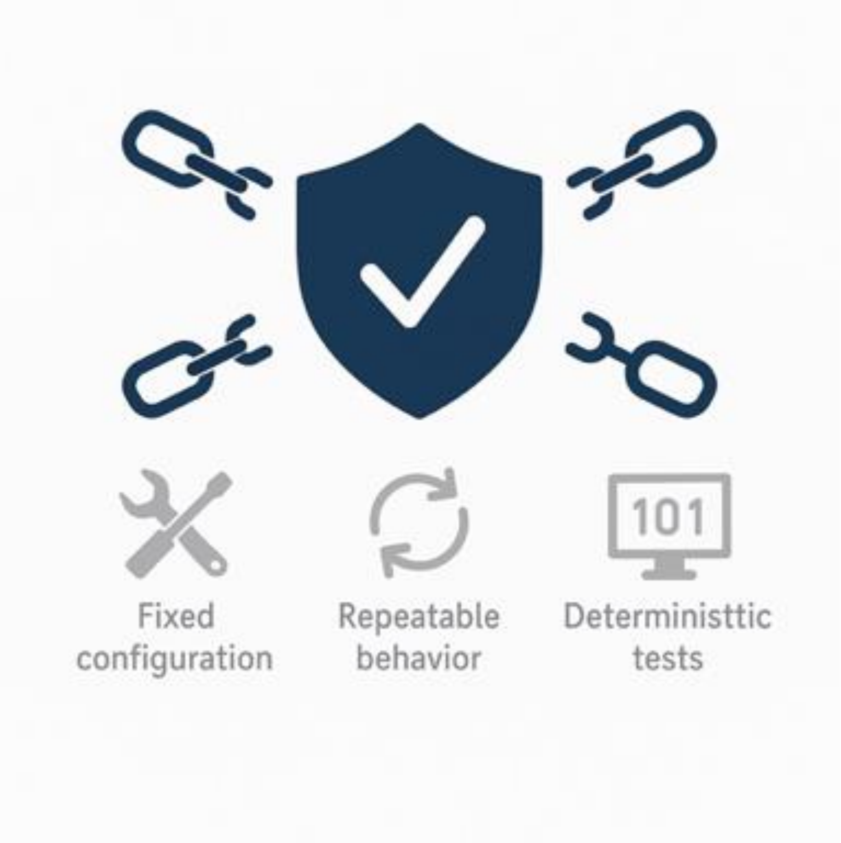
- The question:
  - How can we make security harder to map, predict, or exploit?

The core challenge: certifying the dynamic

- The mismatch: dynamic systems vs. static assurance models
  - Traditional assessments (e.g., Common Criteria, pen-testing) rely on stable, fixed targets.
  - Evaluating a constantly moving target introduces fundamental complexities.

- Key question:
  - What does "certified" even mean if the system is never truly "fixed"?

- Implications:
  - Difficulty in defining a "snapshot" for testing.
  - Meeting compliance and regulatory requirements built on static assumptions.
  - Risk assessment becomes more complex.



Introducing Common Criteria (CC)

- Current version CC:2022 (https://www.commoncriteriaportal.org/index.cfm)
- CC (ISO/IEC 15408) is the leading international framework for certifying ICT product security.
- Widely adopted by EU member states and global certification schemes.
- Based on:
  - Protection Profiles (PPs): Standardized security requirements
  - Security Targets (STs): TOE-specific claims
  - Evaluation Assurance Levels (EALs): EAL1 to EAL7 — increasing depth and assurance
- Evaluation Framework: CEM and AVA_VAN
  - CEM: Common Evaluation Methodology — prescribes how evaluators assess SFRs and SARs
  - AVA_VAN: Defines vulnerability analysis and attack potential scoring

TOE: Target of Evaluation

What Gets Certified Under CC?

- Smart cards, secure elements and security boxes (e.g., SIM, TPM, eID, HSM)
- Firewalls, VPNs, and network devices
- Operating systems and hypervisors
- Trusted execution environments (TEE)
- IoT and industrial control products
- Security software (crypto libraries, secure bootloaders)

What is the EUCC (EU Common Criteria Scheme)?

Established by the European Commission's Implementing Act Regulation (EU) 2024/482, linked to the Cybersecurity Act (CSA) (Regulation (EU) 2019/881).

The EUCC is the first certification scheme developed under the CSA requirements.

Other schemes are currently under development, including EU5G and EUCS, with more expected in the future.

Sets the rules, obligations, and structure for certifying Information and Communication Technology (ICT) products.

Built upon established international standards:

- Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
- Common Evaluation Methodology (ISO/IEC 18045)

Requires conformity assessments to be performed by accredited IT security evaluation facilities (ITSEFs).

Certificates are valid for a maximum of five years, with potential for extension only with authorization from a National Cybersecurity Certification Authority (NCCA).

EUCC: Key Enhancements & Applicant Focus

- Enhanced Security Focus:
  - Patch Management: Emphasizes systematic updates for "assurance continuity". Can be evaluated to maintain certificate validity.
  - Vulnerability Handling: Requires certified entities to establish and execute detailed vulnerability management protocols, including monitoring, remediation, and stakeholder communication.

- Applicant Information Transparency: Applicants must publicly provide:
  - Guidance for secure product use.
  - Period of security support.
  - Contact information.
  - Procedures for receiving vulnerability info.
  - Reference to public vulnerability repositories.

- Is EUCC Compliant with the upcoming CRA? The EUCC scheme and the Cyber Resilience Act (CRA) work in tandem to present compliance, however, achieving complete adherence to the CRA requires further actions in EUCC.

- Reference Documents: "State-of-the-art" documents are available via ENISA and the EUCC Implementing Act Annexes. https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

Assurance Levels

CSA	CC/EUCC
Basic	- Not covered in EUCC scheme
Substantial	- AVA_VAN.1 to AVA_VAN.2 - EAL1 to EAL3
High	- AVA_VAN.3 to AVA_VAN.5 - EAL4 to EAL7

What AVA_VAN bring

- AVA_VAN (Vulnerability Analysis):
  - Assesses the effort required for an attacker to exploit identified vulnerabilities

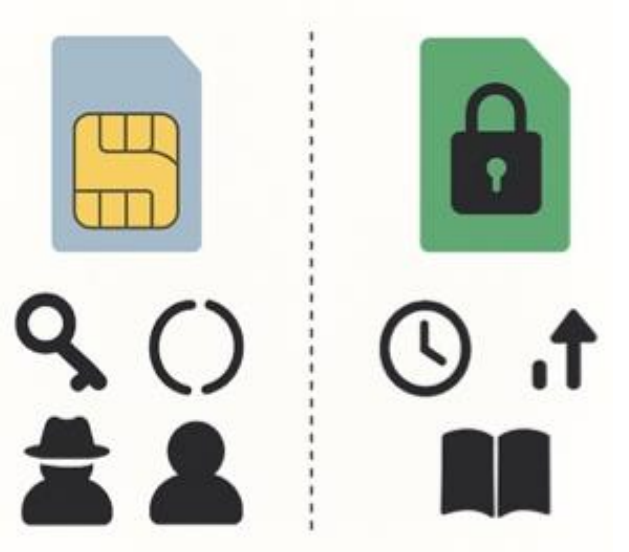
- Assessment factors:
  - Elapsed Time – Time needed to identify and exploit vulnerabilities
  - Expertise – Knowledge level required (Layman → Multiple Experts)
  - TOE Knowledge – Understanding of internal architecture/code
  - Access to TOE – Number and type of samples needed
  - Equipment – Tools required (basic → custom high-end)
  - Open Samples – Availability of known test samples

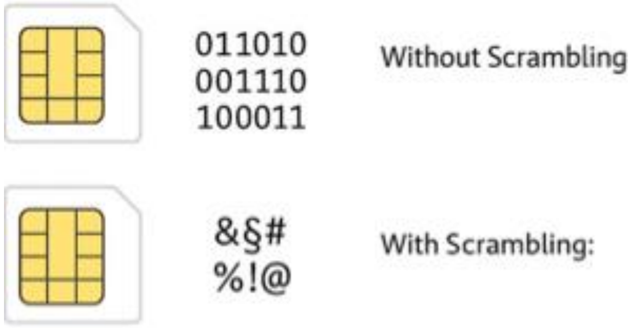
- Attack Potential Ratings:
  - (AVA_VAN.2–3) → Minimal effort; common vulnerabilities
  - (AVA_VAN.4) → Moderate effort, some expertise
  - (AVA_VAN.5) → Requires advanced knowledge, tooling, and time

- MTD impact:
  - Increases difficulty across multiple AVA_VAN metrics
  - Shifts classification from Basic to High
  - Raises assurance level without needing new hardware

MTD case study: SE singularisation (1/2)

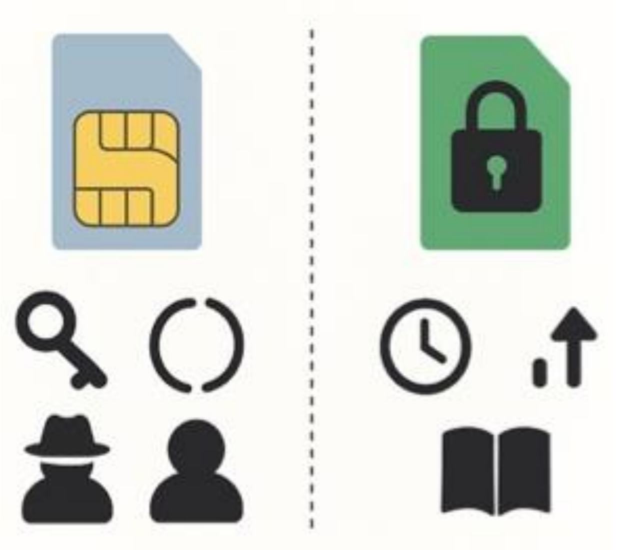
- Singularization in practice
  - Apply unique, randomly selected "scrambling functions" (Pre/Post-SF) to a core Security Function (e.g., AES).
  - Functions chosen from a secret, diverse catalogue (XOR, Feistel, arithmetic etc.).
  - External "Singularization Service" tracks and deploys the Singular Security Function (G) and its verification counterpart (V). G is deployed on the user's device (SIM), and V is deployed in a Proxy accessible to Service Providers.
  - Attackers faced dramatically more effort trying to bypass or reverse-engineer the individual scrambling functions for each unique instance, rather than just the core algorithm.

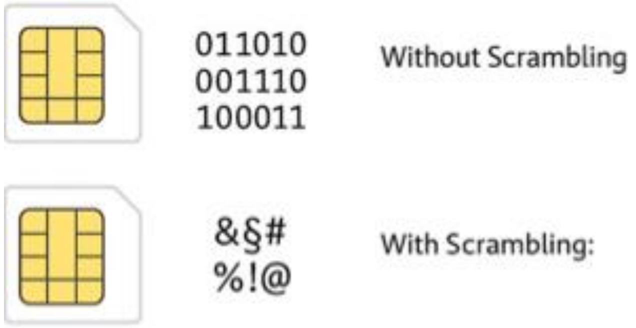




MTD case study: SE singularisation (2/2)

- **Without singularisation:**
  - Cloning risk;
  - Predictable function layout; vulnerable to SCA (Side-Channel Attacks) and fault injection
  - Attack potential limited to AVA_VAN.3 (Enhanced Basic)
- **With singularisation:**
  - Unique functional variants per device
  - Cryptographic cloning is impractical due to functional scrambling
  - Dynamic behavior adds noise, obfuscation, and unpredictable patterns
  - Attack potential elevated to AVA_VAN.5 (High)
    - ▸ Higher Elapsed Time
    - ▸ Increased Expertise required
    - ▸ Greater TOE Knowledge
- **In Common Criteria terms:**
  - Singularisation effectively raises the Attack Potential rating
  - Demonstrates defense through unpredictability and individualized resistance
  - Aligns with Moving Target Defense principles





Challenges with traditional CC for MTD

- Snapshot assessment: CC provides a snapshot of security at the time of evaluation. An MTD system is never in a single 'state.'

- Scope definition: Defining the precise scope of a TOE that constantly changes its attack surface is extremely difficult.

- Assurance maintenance: Once certified, how is assurance maintained if the system's configuration is constantly changing?

- Cost and time: Re-evaluating a constantly changing system would be prohibitively expensive and time-consuming.

Strategies for adapting Common Criteria to MTD

- **Certifying the MTD mechanism (the "Engine of change"):**
  - The core MTD components (e.g., the singularization service, the randomizer, the deployment mechanism).
  - What to evaluate: The correctness, randomness, integrity, and security of the process that generates and deploys variations. Is the source of diversity secure? Is the distribution truly unpredictable? Are the changes correctly applied?
  - CC application: This part could still fit traditional CC. You'd define a TOE as the "MTD Orchestrator" or "Diversity Generator."

- **Certifying the framework or Policy for MTD:**
  - Focus: The overarching rules, policies, and management processes that govern how MTD is implemented.
  - What to evaluate: Does the MTD strategy meet defined security goals? Are the chosen parameters appropriate for the threat model? Is there a secure way to manage the catalog of variations? Is the "refresh rate" adequate?
  - CC application: This is closer to a process-oriented certification, potentially aligning with higher EAL levels that emphasize development and operational procedures.

The path forward: adapting CC components

- Define a flexible TOE: static + dynamic components

- Tailor Security Functional Requirements (SFRs):
  - Refine existing requirements for addressing dynamism and randomness
  - Introduce entirely new requirements to cover MTD-specific properties that are not addressed by existing CC components.

- Security Assurance Requirements (SARs) for dynamic systems
  - Change how compliance with SARs is demonstrated. Move from single-instance testing to statistical testing, and from static vulnerability analysis to "adaptive attacker" models.
  - Need new SARs or extensions focusing on "assurance continuity under dynamic change”

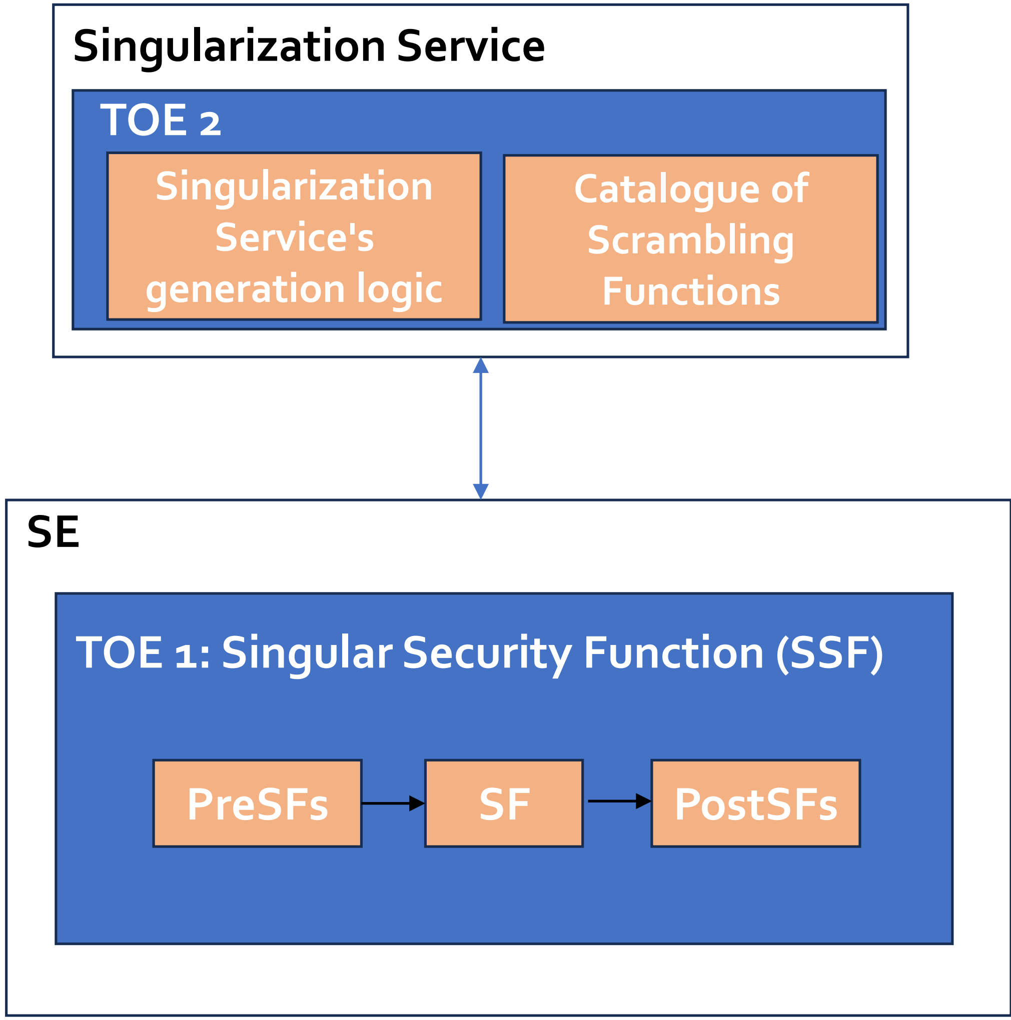
- Specific MTD Protection Profiles (PPs)
  - Develop PPs for classes of products implementing specific MTD techniques

Example - how to adapt CC for singularization in SEs

- **TOE 1 (within the SE)**: Primarily contains the Singular Security Function (SSF), which is the original security function wrapped with unique, instance-specific pre- and post-scrambling functions.

- The **Singularization Service (within the service provider)** including the secret catalogue of Scrambling Functions and the management framework that orchestrates the generation and deployment of these singularized functions.

- **TOE 2 (within the Singularization Service)**: the creation of the Singularization Service's generation logic, the management of the "Catalogue of Scrambling Functions"


Singularization Service
TOE 2
Singularization Service's generation logic
Catalogue of Scrambling Functions
SE
TOE 1: Singular Security Function (SSF)
PreSFs
SF
PostSFs

Examples - Most relevant Security Functional Requirements (SFRs)

- **FDP_IFC.1 (Information Flow Control) (existing, refined)**
  - Focus: Protects the secrets of singularization within the SE.
  - Refinement: "The SSF shall ensure that the internal state of its Pre/Post-Scrambling Functions (e.g., specific algorithms, parameters) is not disclosed through side channels, fault injections, or error messages."
  - Why it's key: If the attacker can learn the current unique scrambling, the MTD benefit is lost for that instance.

- **FPT_MTD_UNP.1 (Unpredictability of Response) – (proposed new)**
  - Focus: Quantifies the MTD benefit.
  - Requirement: "The SSF's output (after Post-Scrambling) shall be functionally unpredictable to an attacker without knowledge of the specific active Pre/Post-Scrambling Functions and their parameters."
  - Why it's Key: This forces a measurable increase in attacker effort to understand the output.

Examples - Most relevant Security Assurance Requirements (SARs) (1/2)

- ATE (Testing)
  - Challenge:
    - Exhaustive testing of all possible dynamic states is impossible.
    - Manually verifying each instance's uniqueness is labor-intensive.
  - Recommendation:
    - Test a statistically significant sample of diversified TOE instances.
    - Develop or use automated tools to verify diversity, unpredictability, and absence of common patterns across generated variants.
  - Example (Singularization): Automated tools to check that each deployed SSF indeed has a unique Pre/Post-Scrambling function composition.

- AVA_VAN.4 (Methodical Vulnerability Analysis)
  - Focus: Simulate an attacker's ability to learn about one instance and then adapt their strategy to compromise subsequent different instances.
  - Refinement: "Vulnerability analysis shall include penetration testing on representative singularized SSF variants, explicitly focusing on: 1) Bypassing or disabling scrambling, 2) Deriving scrambling functions/parameters, 3) Assessing the difficulty (e.g., Attack Potential) of transferring knowledge between instances."
  - Why it’s key: This is where the MTD's effectiveness is validated against real-world attack models.

Examples - Most relevant Security Assurance Requirements (SARs) (2/2)

- ALC_DVS.2 (Security Measures during Development)
  - Focus: Protecting the MTD "secrets" and processes.
  - Audit focus:
    - Secure development environment: Audit the physical and logical security of the development environment where scrambling functions and generation logic are created and stored.
    - Code integrity: Verify secure coding practices, vulnerability scanning, and testing for the scrambling functions themselves and the Singularization Service's software.
    - Access control : Audit strict access controls to the Catalogue of Scrambling Functions (critical secret!), the source code of the generation logic, and the sensitive configuration data.

- ALC_DEL.1 (Delivery Procedures)
  - Focus: Secure delivery of the dynamic components.
  - Audit Focus: Verify secure procedures for:
    - Encrypting and authenticating the unique SSF binaries during transmission from the Singularization Service to the SE provisioning entity.

Recommendations for Certifiers and Evaluators

- Focus on certifying the mechanisms of change and the assurance that dynamism is maintained.
  - A certificate attesting to the dynamic security properties (e.g., unpredictability, increased attacker effort).

- Intensify focus on ALC (Lifecycle Support)
  - Certify the secure SDLC, generation processes, and management procedures of the MTD service (e.g., the Singularization Service).

- Invest in R&D for new ATE (testing) and AVA methods
  - Standardized ways to test unpredictability, and effectiveness of dynamic defenses.

Takeaways

- MTD is a crucial paradigm shift, proactively changing the attack surface to increase attacker effort and uncertainty.
- Use cases like Singularization for legacy SEs demonstrate that MTD significantly raises the "Attack Potential" (e.g., from Moderate to High), making systems much harder to compromise in practice.
- Traditional certification frameworks (like Common Criteria) are designed for static targets and must evolve to certify dynamic systems.
- Achieving high assurance requires a collaborative effort from developers, evaluators, and certification bodies to rethink established paradigms.

INTERNET
OF TRUST

www.internetoftrust.com

Get in Touch

With Us:

E-mail:

- mohamad.hajj@internetoftrust.com

77 Avenue Niel, 75017 Paris, France

Phone:

- Insert your phone number

Company overview

Leader in cybersecurity consulting and certification for complex connected systems: embedded, IoT, industrial, Cloud/Edge

Created in 2014, all founders active

Continuous growth and profitability since creation

Track record to renew and build expertise in innovative standards

IP portfolio: external publications, internal knowledge base, client references, capability building programs

Based in France, with headquarter in Paris 17

Operating Worldwide

Expertise and offerings

- Cybersecurity analysis
- Evaluation support
- Scheme definition
- Certification
- Trainings

Clients

- Longstanding, senior relationships in the cybersecurity ecosystem with 30+ years' participation in global standards organizations
- Client profiles: security certification labs/bodies, semiconductor/IP owners, telecom providers, industrial OEMs