COMMON REQUIREMENT ENUMERATION

Helping security standards succeed

Rob van der Veer, representing the team behind the CRE initiative, including Spyros Gasteratos and Elie Saad

October 17 2020

Background for CRE

- Today's **cyber security standard and guidelines landscape** contains a tremendous amount of useful knowledge, yet it turns out to be difficult for most of its users to gain overview and find the information they need. As a result it is difficult for the makers of these standard and guidelines to attain effective use of their work. The landscape has become fragmented, complex and confusing to users, causing security incidents, adding unnecessary expenses and making it hard for standard and guideline initiatives to add value.
- Common Requirement Enumeration (CRE) is an **initiative** based on experience and research: experience form working closely with cyber security standardization organizations for many years and research for ENISA and work funded by the Dutch government on how to model software security.
- CRE builds on the **ENISA recommendation** to create a repository that brings standards and guidelines together, from a recent ENISA report on the security standard landscape.
- Currently, the CRE concept is **being implemented** at OWASP, to provide for more consistency, more clarity and easier development and maintenance of the standards and guidelines at OWASP.
- The idea of CRE is to **link** sections of standard and guidelines to each other, using a mutual topic identifier, enabling standard and scheme makers to work efficiently, enabling standard users to find the information they need, and attaining a shared understanding in the industry of what cyber security is.
- Additionally, the CRE repository is a place to keep **metadata** on requirements, such as hierarchy, usage and discussions.
- The CRE initiative has no commercial intentions whatsoever. It is by the community, for the community. Furthermore, the CRE does NOT introduce a new standard, as the content is still maintained by the linked standards and guidelines.

Presenter introduction

Rob van der Veer, representing the CRE initiative with other co-leads: Spyros Gasteratos and Elie Saad

r.vanderveer@sig.eu

@robvanderveer

+31 6 20437187

www.sig.eu/security

- Estabished and leads the security & privacy practice at Software Improvement Group
- Advisor to ENISA. Co-author of report ‘Advancing software security in the EU’
- Project leader of government-funded research on security requirements
- Project leader at OWASP (Co-lead of the *Standard integration* project)
- Contributor to various standardization initiatives: CIP (Grip on SSD), OWASP (SAMM), NCSC, IEEE

CRE

Challenge: the security standard landscape is a puzzle

The complexity of the security standard landscape is illustrated by the size of ECSO's *Overview of existing Cybersecurity standards* (2018) >200 pages:

The current standard and guideline landscape for security is **fragmented, complex and confusing** to many of its users. It is hard for engineers, testers and clients to select and apply appropriate standards, causing cyber security to stay behind.

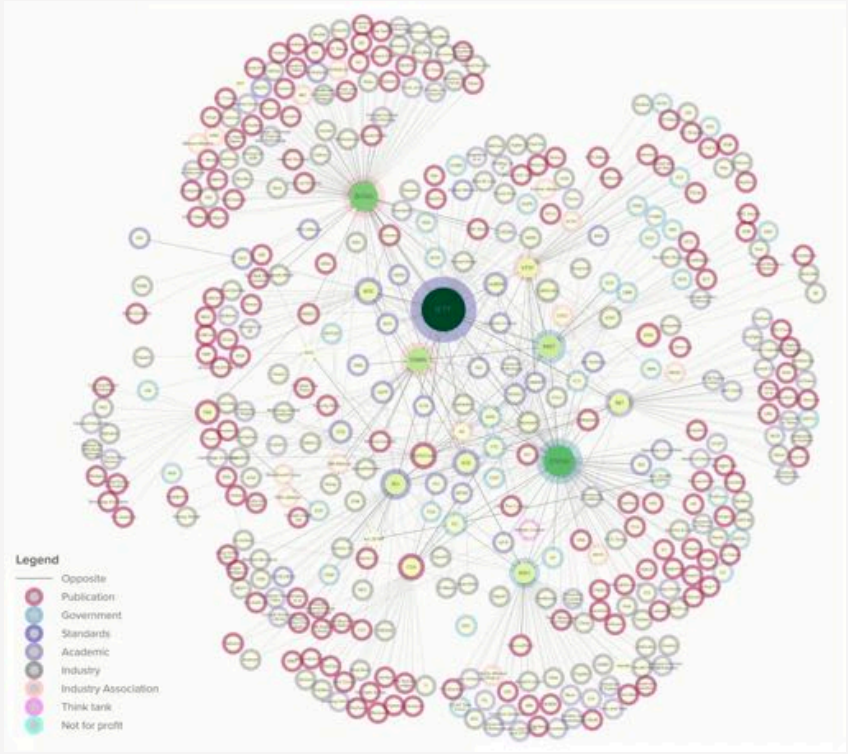
Also, it is hard for **standard makers** to develop and to maintain their publications, link in a maintainabile way to other sources and to attain successful adoption.

Initiatives can benefit from **each other's content**, to save work in development and maintenance, but also to attain more consistency.

Example 1: iotsecuritymapping.uk

In an effort to make sense of IoT security recommendations and standards, a UK initiative has been manually mapping about a hundred sources. At the moment that one of these sources is updated, the mapping is outdated.

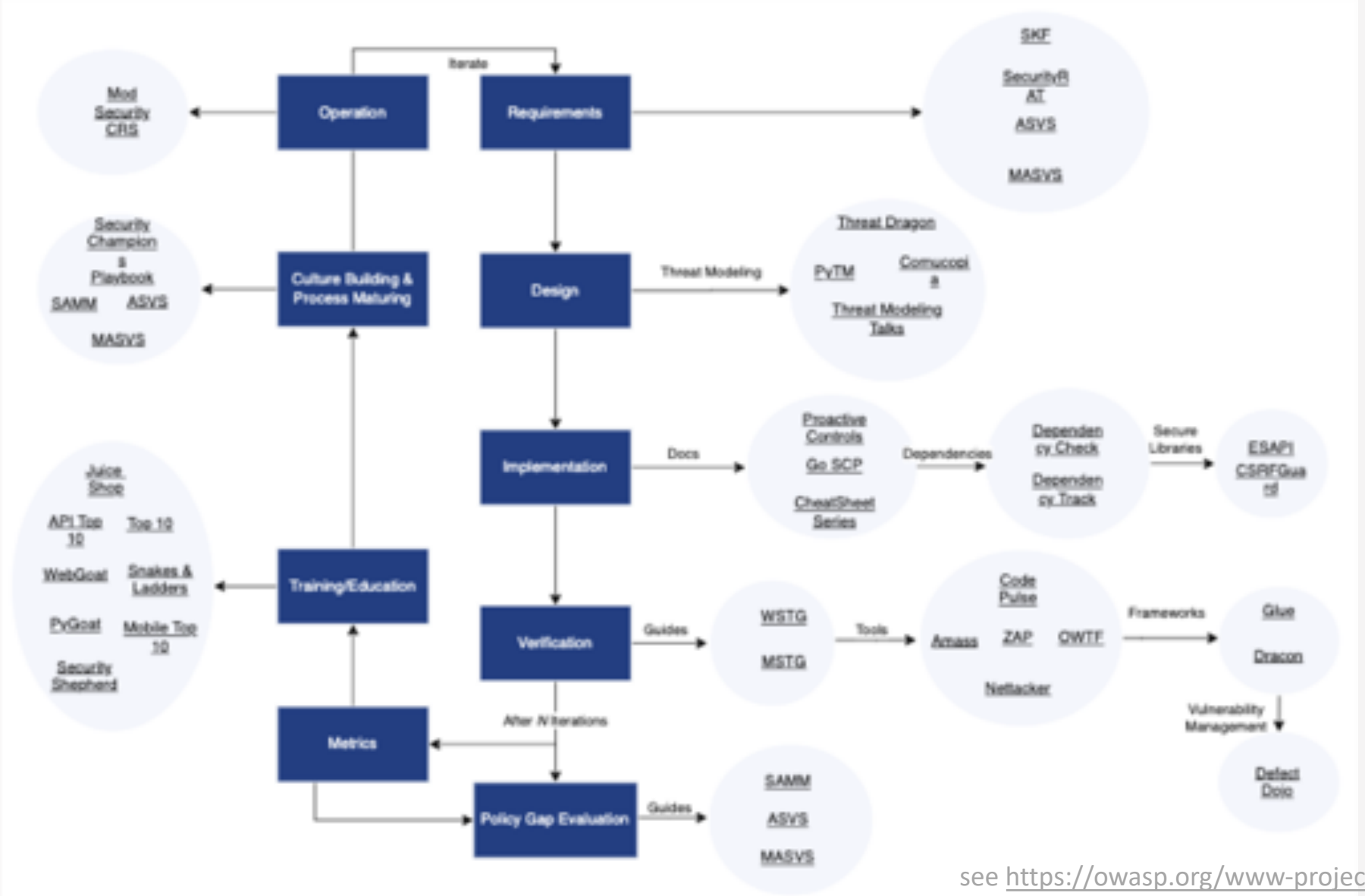
The mapping is stored in about a thousand pages of JSON specifications. It is a useful effort but **extremely hard to maintain** – let alone if the scope would need to be more general and extended beyond IOT.



CRE

Example 2: the great work of OWASP is a puzzle as well …

That's why we created the *Application security Wayfinder. Next: link them on detail level*



see https://owasp.org/www-project-integration-standards/

It is time to harmonize security standards

ENISA report:

“Requirements largely overlap, demonstrating that software security is mainly a generic problem and both Standards Developing Organizations (SDOs) and European Standards Organizations (ESOs) or good practice producers are often working without proper coordination and effective liaisons “

“DEVELOP A COMMON REPOSITORY FOR SHARED SECURITY MEASURES”

“Aligning on requirement commonalities across different schemes prevents proliferation and fragmentation, while also making drafting and maintaining a scheme more efficient in terms of mitigating the risks."

CRE

Enter: the Common Requirement Enumeration (CRE)

After extensive research and interviews with standard makers, procurement, industry, academia, engineers, testers and certification bodies, the idea for CRE was born, and it is now in the initial implementation phase.

Goal: enable alignment and cross-reference between security standards and guidelines, to:

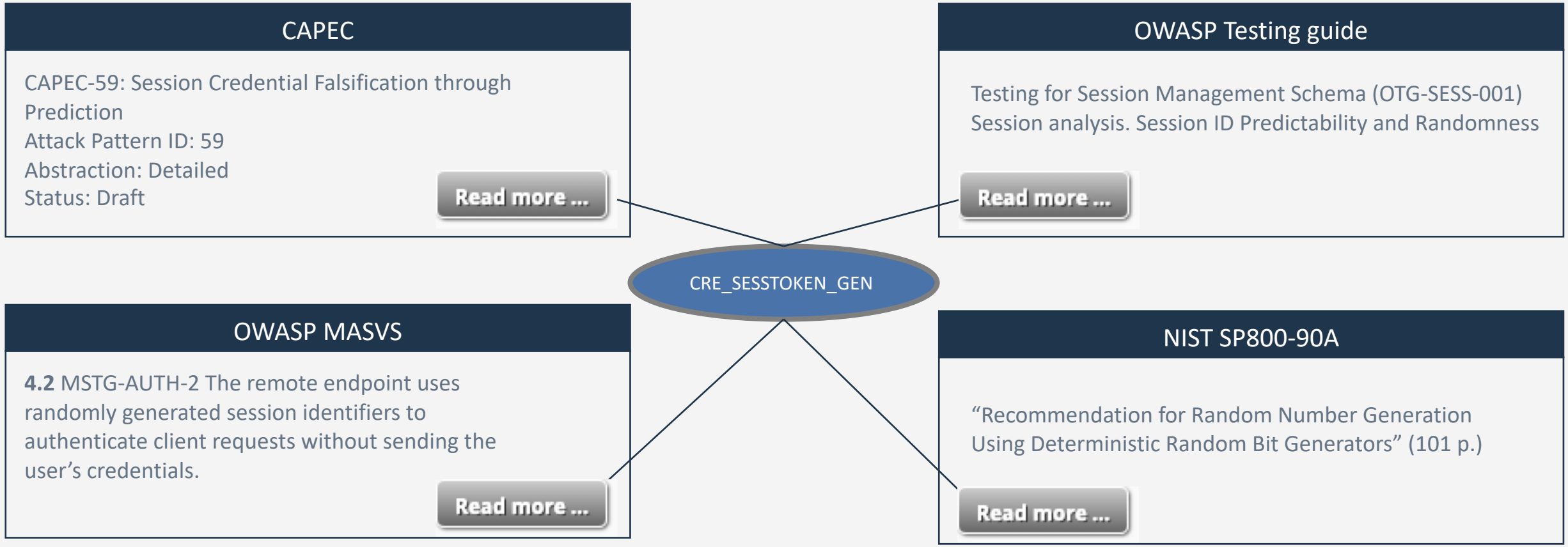
- Attain shared understanding in market and industry on what security means (engineers, testers, and procurement).
- Make development and maintenance of standards and schemes easier
- Make it easier to find relevant work based on the context
- Achieve more consistency and less gaps between standards

Method: provide a central repository of Common Requirement identifiers, to which standards can link their coverage of that topic, and by doing so, link to all the other relevant sources in other standards that refer to the same – and vice versa.

Deliverables:

- A r**epository** of technical requirement links in the form of an online service, offering just an identifier, metadata and links-content is in the standards.
- Policy, guidelines and organization how the repository **changes over time**
- Tools and methods for standard makers to **link** using the repository

Common Requirement Enumeration example



Each rule in a standard links to the corresponding Common Requirement identifier and by doing so, standards link to each other. This allows readers to find all the information they need on a topic, as if they were using one single source – without links becoming outdated. For standard makers, maintenance, focus and consistency becomes easier, and a larger audience can be reached. For the industry, it becomes easier to define sets of requirements for different domains and types of systems, which allows procurement, engineering and testers to use one language in consensus when dealing with criteria for cyber security.

How are users referred?

OWASP MASVS

4.2 MSTG-AUTH-2 If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials. CRE

This section of a standard shows a CRE link.

When clicked, a pop-up menu is shown, or the user is taken to the CRE website.

CRE12459
Appsec-Session "Session management"
-Proactive Controls

CRE12452 -Appsec-Session-TokenGeneration
-ASVS 145, 146
-WSTG
-NIST
-CWE

CRE12451 -Appsec-Session-Removal
-ASVS 141
-WSTG
-NIST
-CWE

The CRE website shows the name of the requirement, links To relevant sources, and (through metadata) related requirements, including those on a higher level (in this case *session management*) with links to sources that cover that topic.

This allows multi-level browsing and exploration of requirements.

Standard users can find the right information and standard makers can provide access to their work, and they do not need to elaborate – just link.

CRE-linking is self-maintaining

CAPEC

CAPEC-59: Session Credential Falsification through Prediction
Attack Pattern ID: 59
Abstraction: Detailed
Status: Draft

CRE_SESSTOKEN_GEN

OWASP Testing guide

Testing for Session Management Schema (OTG-SESS-001)
Session analysis. Session ID Predictability and Randomness

CRE_SESSTOKEN_GEN

OWASP MASVS

4.2 MSTG-AUTH-2 If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests with[illegible]dentials.

CRE_SESSTOKEN_GEN

NIST SP800-90A

“Recommendation for Random Number Generation Using Deterministic Random Bit Generators” (101 p.)

CRE_SESSTOKEN_GEN

By storing the CRE-identifier IN the standards, the mapping become self-maintaining. It is updated constantly without new effort.

How does the self-maintenance work?

CRE supports two models of maintaining links:

1. A **mapping file** for a standard that contains the CRE identifiers that are covered with the hyperlinks to where they are covered. This can be maintained by a third party (e.g. the CRE team) and ideally by the standard maker.
2. **Embedded mapping**: the source files of the standard contain the CRE links which are scanned by the CRE parser to automatically create the mapping file. This approach makes things completely self-maintaining.

Example:

OWASP MASVS
** 4.2MSTG-AUTH-2 ** If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials. Read more

The CRE parser is configured to scan for CRE references (last line) and then register the CRE identifier and link that to the first section before that link with the class "ruletitle" and pick the corresponding ID (first line).

In this example this leads to the following entry in the mapping file:

CRE_SESSTOKEN_GEN,
http://www.owaspmasvs.org/rules.html#rule123

Advanced features of CRE linking

Reference flexibility:

- Using the CRE mechanism it is also possible to refer directly to a specific source, which is automatically kept up to date.
- Similarly the CRE link can control how the information is presented (e.g. OWASP sources first)

Furthermore, users can manage their own account or sessions on the CRE website and specify what sources they prefer to see.

Intel: The (anonymous) use of CRE leads to interesting insights into the use of standards and specific topics.

CRE roadmap

1. Create Application security wayfinder as a first service to the community
2. In progress: build first CRE system to harmonize the flagship standards at OWASP: https://owasp.org/www-project-integration-standards/
   Co-leaders: Elie-Saad, Spyros Gasteratos, Rob van der Veer
3. Take CRE implementation outside of OWASP and arrange independent governance
4. In progress: seek alignment with standard makers and other stakeholders
5. Process new ideas and learning points
6. Establish a consortium to govern CRE
7. Further connect more standards using CRE