I am really excited about this speaking opportunity, as openCRE is important to me personally. And you'll find out why later on.

In a nutshell, for those that haven't seen it yet:

OpenCRE stands for Open Common Requirement Enumeration.
It basically is a gigantic index for security requirements, across major standards.
It links standards at the level of requirements, so when you are performing a check in the OWASP ASVS standard for example,
you can use OpenCRE to find more information on how to test that requirement, how to use tools, how to code solutions for it.
You learn more about the related threats and read what NIST has to say about it.
It gives you all the information on a topic from various standards and guidelines, like it is one single resource.

So it makes all standards into one.

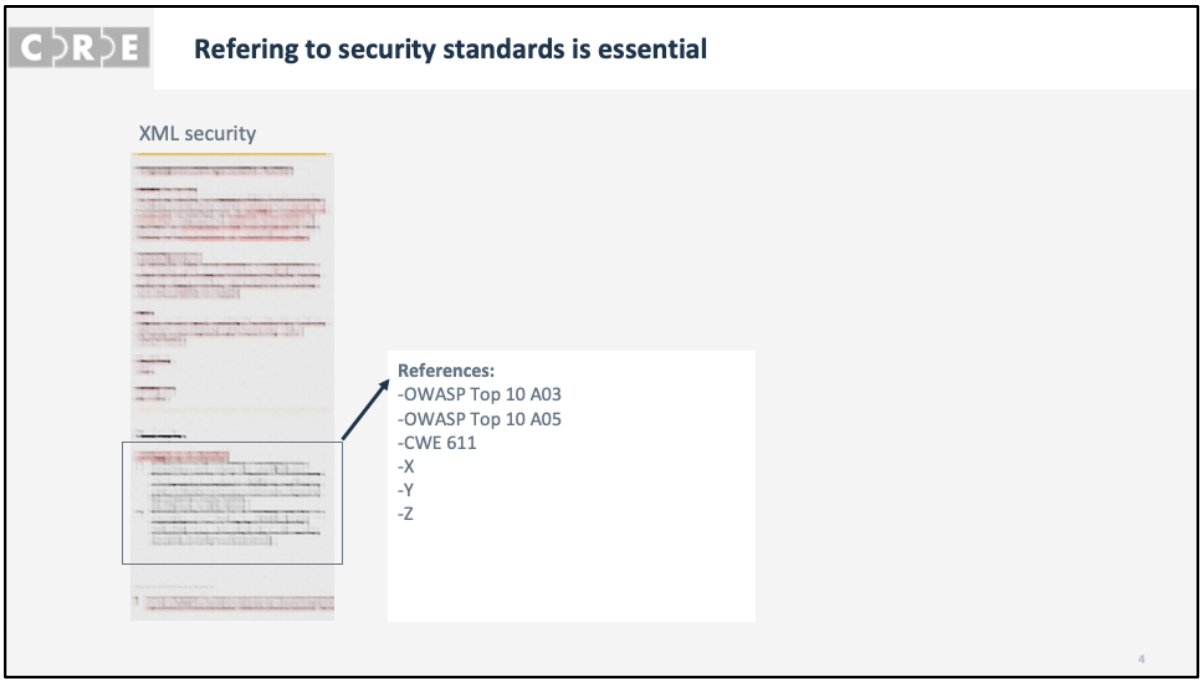
At last nights Halloween party, here at the conference, I was dressed up as the ‘Ghost of security standards’ with the weight of many many different standards on my shoulders.

THIS is the issue that OpenCRE solves – by making all these standards into one clear resource. It’s the Ghostbuster of this ghost.

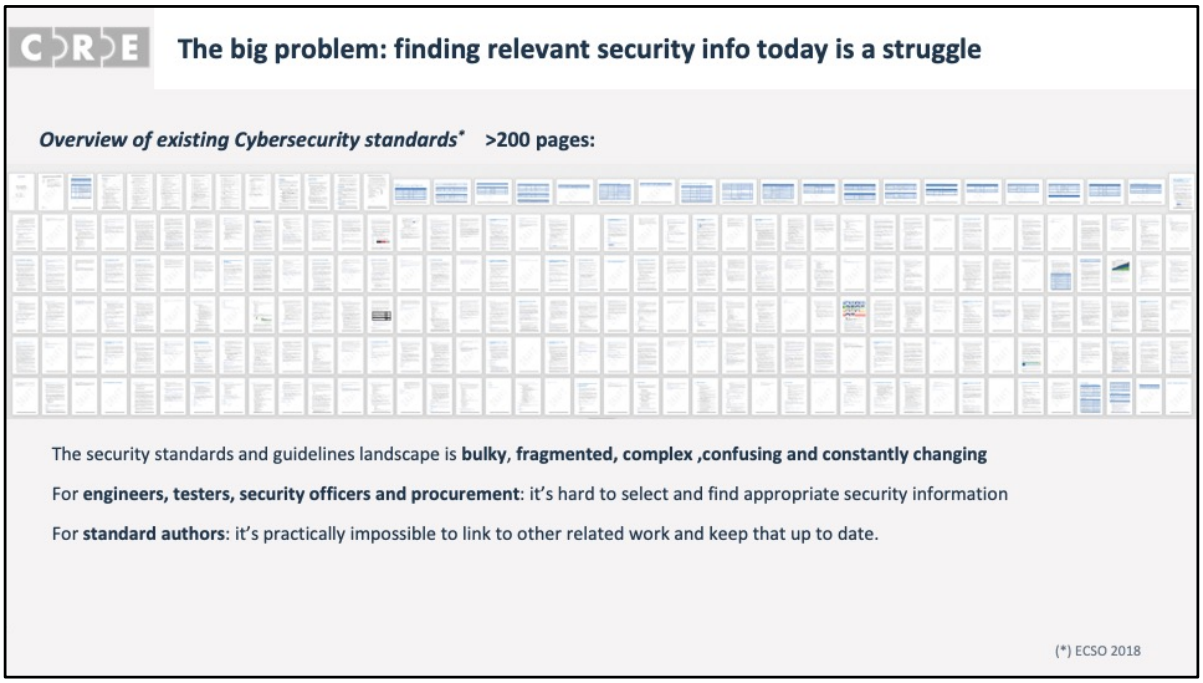
Hello, I am Rob van der Veer. I like to build bridges in organisations and in the fields of security, privacy and artificial intelligence.

I work for Software Improvement Group, where I started the security & privacy practices about 10 years ago. If you don't know us: at SIG we measure software quality, maintainability, security, privacy and more, to help organisations get software right.

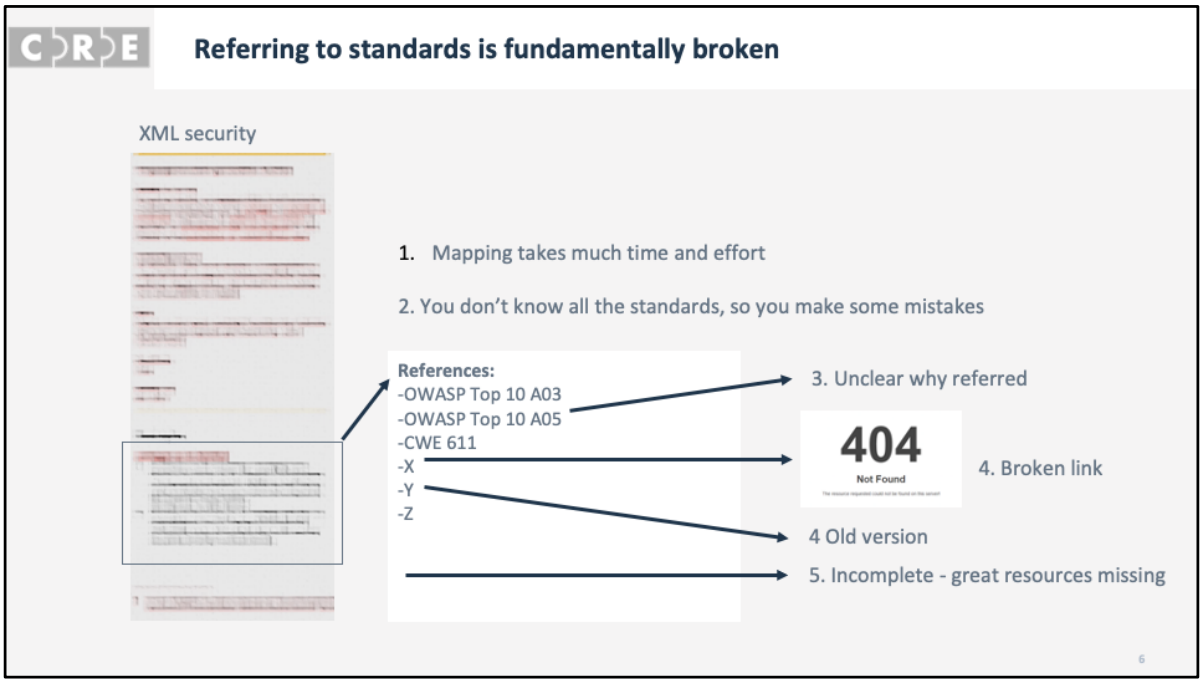
Next to SIG I'm also involved in many initiatives to help grow these fields:
-I for example advise the European Commission on security, and I'm an active contributor to standards at ISO/IEC
-Also I wrote agile secure software guidance, part of OWASP SAMM, I co-lead the Integration project at OWASP and that is where we started the OpenCRE initiative from.
Let me tell you why.



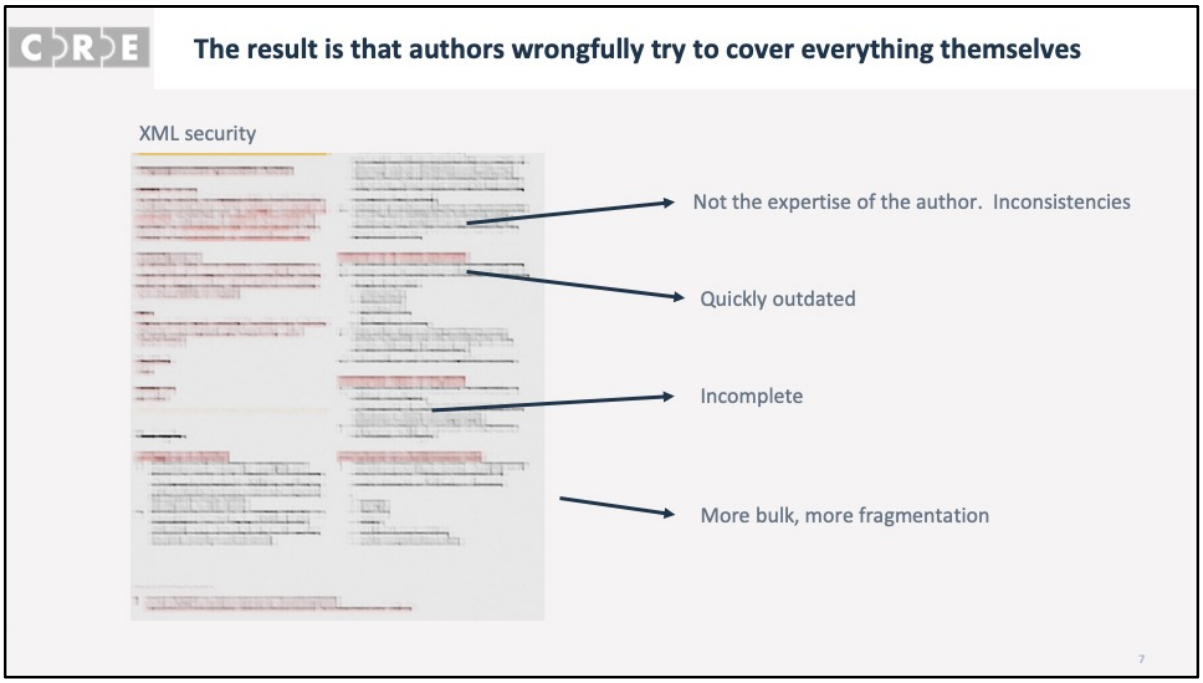
If you write a document on security,
let's say a national standard, for some industry - it can also be a company wiki with security coding guidelines.
Then you want to focus your writing on the specific stuff and refer your readers to the generic material for more details.
Otherwise you'll have to copy and paste all that material, and it will get outdated quickly.
So you add references: several links to related sources. Pretty normal. Good idea. Right?



Well, we see that the world is having a big problem today when it comes to finding relevant information on security:
It's a struggle. And I'm sure you recognize this. The available information is bulky, fragmented, complex, confusing and constantly chainging.
Take a look at this report by the ECSO: it's just a LIST of existing security standards and it's more than 200 pages. Just the list.
..
This is the case NOT because it's necessary to have a lot of standards and complexity. It is not required at all. But there are
historic reasons, psychological reasons, political and commercial reasons that we have to deal with this today.
..
If you're an engineer, a tester, a security officer, if you want to buy software and set requirements: it's hard to select
and find appropriate information on security to do your work.
If you are writing a standard, it is hard to refer your readers to other sources, because it's a bit of a mess.
There are many many standards and for most part they talk about the same thing.



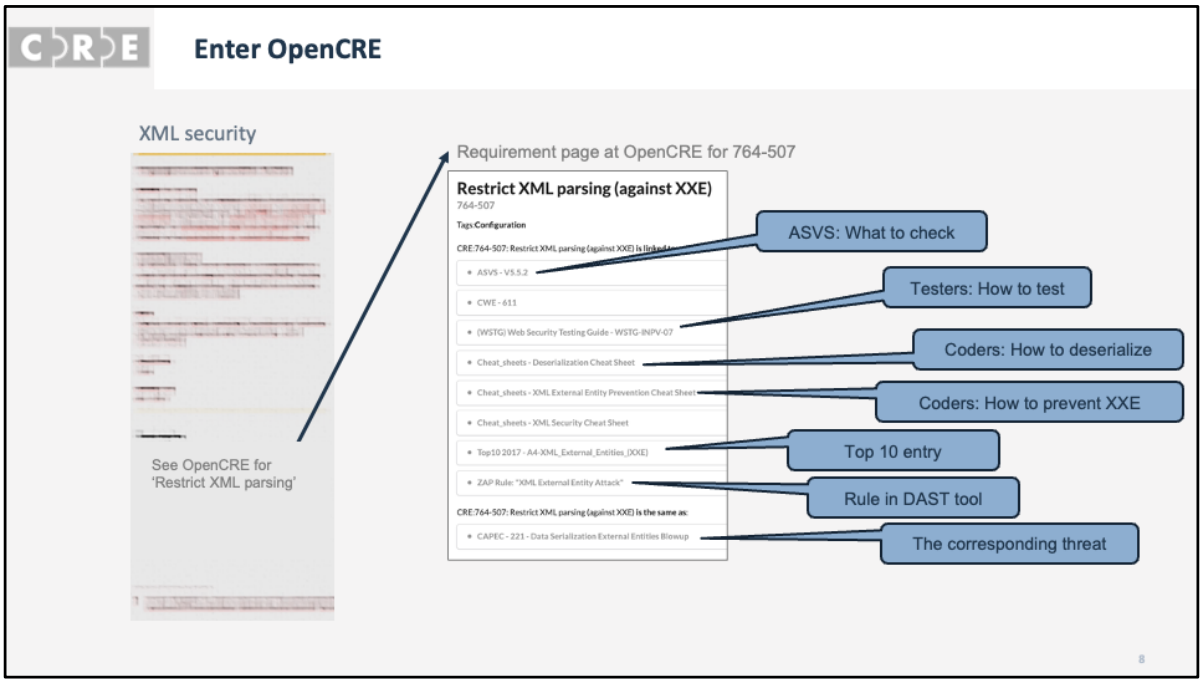
Because of this, refering to standards is fundamentally broken.
First of all it takes a lot of time and tedious work to create mappings between your work and all those other standards.
And because you have better things to do, you are going to make some mistakes, You'll mis things, you'll refer to the wrong sections.
And your references lack structure. They're just a flat list. It's not clear how that top 10 entry is related, or what these different
weaknesses have to do with the topic.
Also, links get outdated. I know many current security standards of which half of the links are not working anymore.
Standards change their structure regularly, and sometimes their location. Then you get broken links. The result is that deeplinks are avoided.
Or you get linked to an old version, while there is a newer version in another location.
And there may be some really good resources that are missing because the author doesn't know them, or chooses not to include because
you can't add everything and then have to maintain a very long list.



So, either you get a list of flawed references OR, what often happens, authors decide to cover the referred information themselves.
Oh dear. Yes, the reference problem is solved, but this typically results in inconsistencies and incompleteness
because it's not the author's expertise per se and the information is not updated automatically.

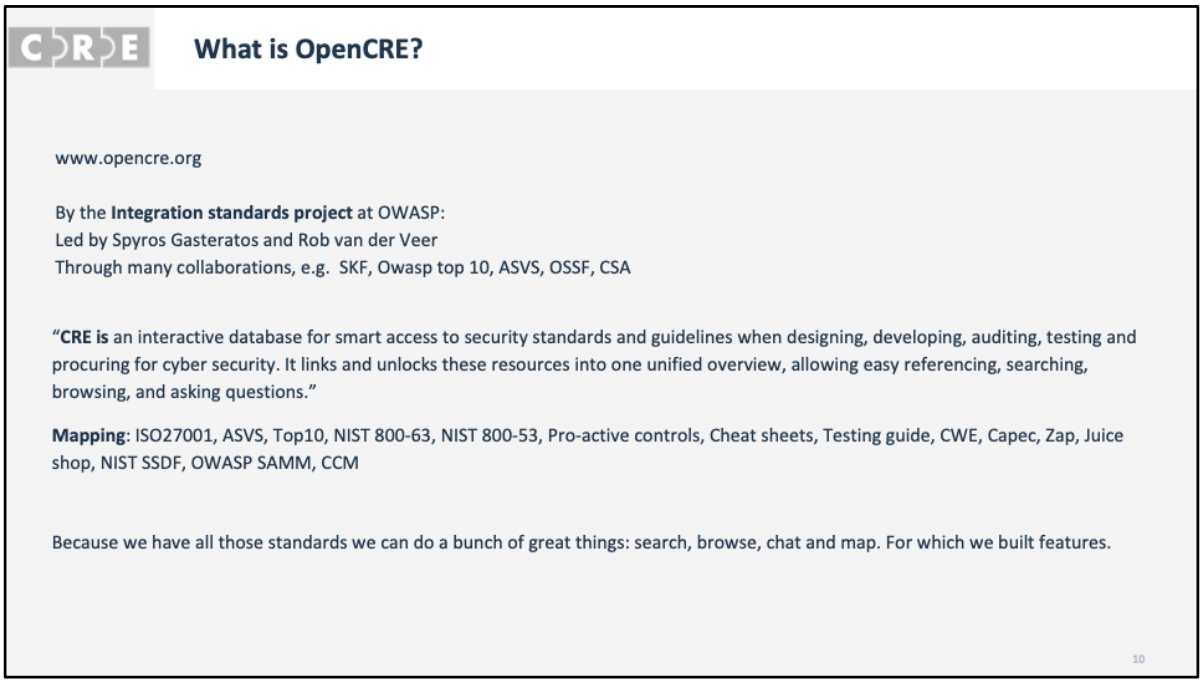
And this is one of the causes for the bulk, the scope creep, the fragmentation and quality issues that standards face today.
The problem that refering to standards is broken, only increases the mess.

If only references could be more complete, have structure, and stay up to date. If only.
Well, that's what OpenCRE is for: it's a repository of references that stay up to date.



And this is the primary use case. This standard has a hyperlink to the OpenCRE website, specifying the ID for the relevant common requirement – in this case 764-507.
And it shows deeplinks to all the standards on the same topic, plus it shows links to related topics, that allow you to explore.
You know what this means?

NO MORE MAPPINGS



So, what is OpenCRE?
We released it about two years ago
after about two years of preparation.
And when I say we, I mean the Integration standards project of the OWASP foundation.
The goal of our project is to create links between security standards at OWASP and beyond, to unlock the standard landscape.
We did this with a lot of help, for example from the OWASP Top 10 team.
So,…what is CRE. Well: <see slide>

Today, OpenCRE maps a wide range of security standards, from ISO, NIST, Mitre, OWASP, the Cloud Security Alliance, etc. etc.

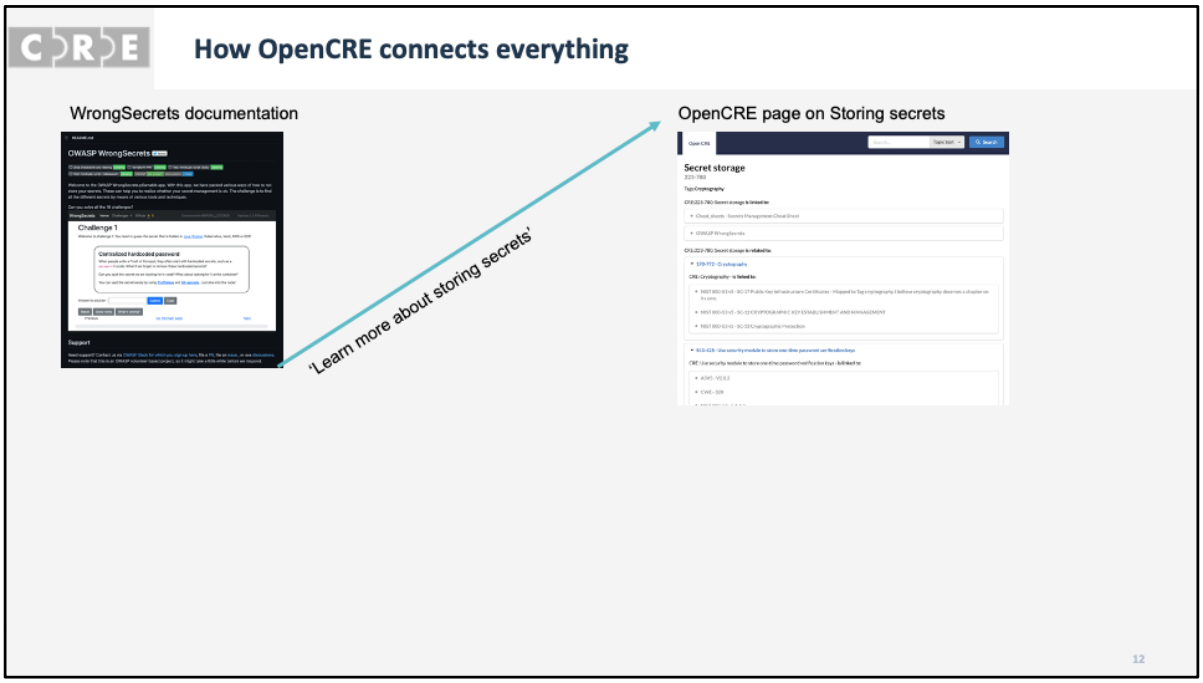
It has been my personal quest for the last 8 years to try create more unity in standards
and I learned that you can't merge initiatives or create super close collaborations between most standard organizations.
Something else needed to happen, and that something else was OpenCRE.

And we’re doing great. We received a grant from OWASP to further develop our system. Standard after standard is connecting with us. And tool after tool. Just recently OWASP SAMM joined, and the Cloud Security Alliance has embraced OpenCRE as their platform to link to other standards. But still, there is more work to be done,

CORE

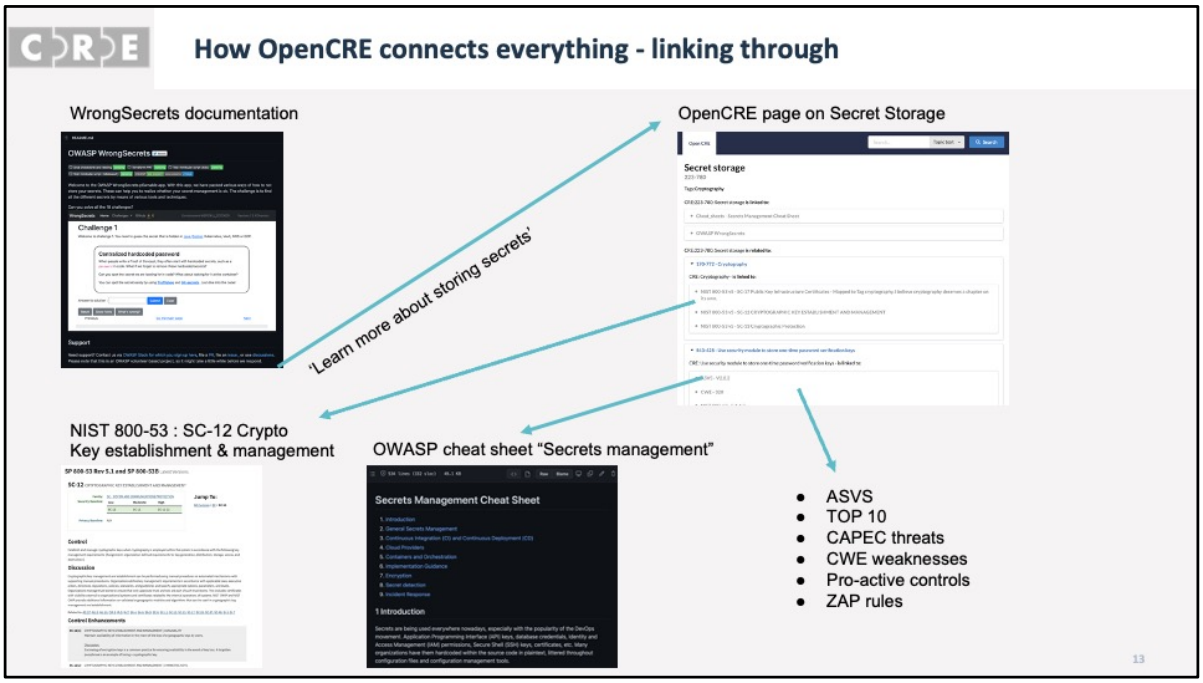
Screenshots instead of live demo

11

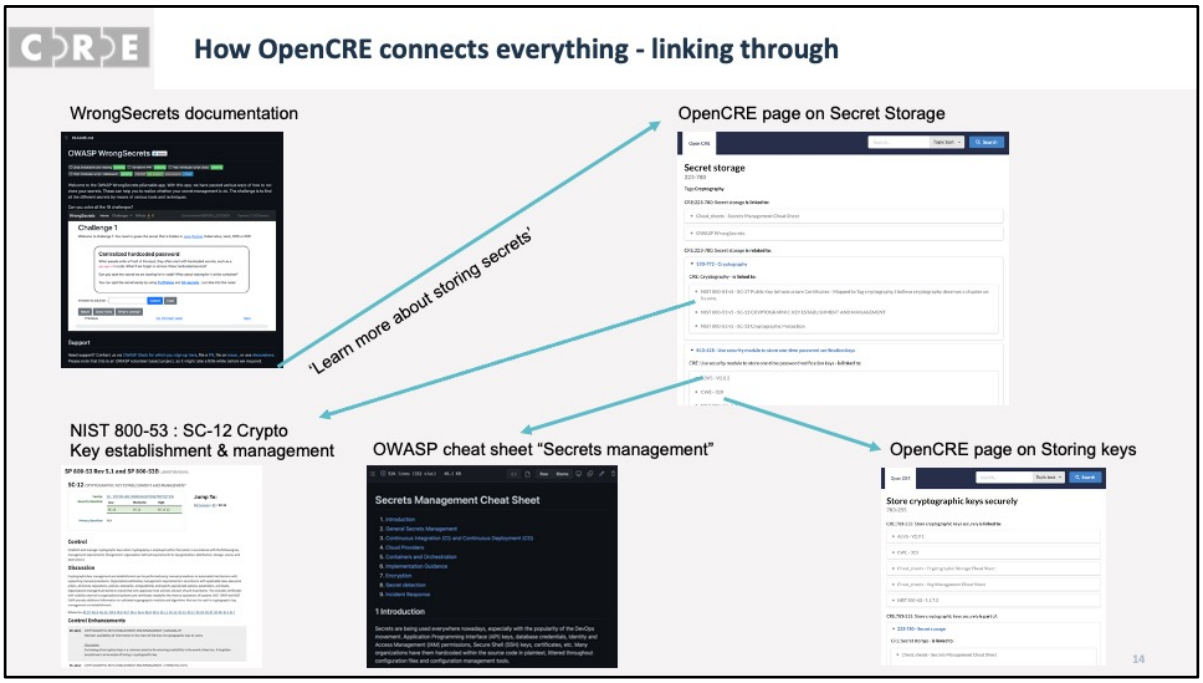


So. How does OpenCRE solve problems? Let's look at an example.
In the top left you see the documentation of the WrongSecrets project. A great tool by Jeroen Willemsen and friends.
It's about secrets management.
They would like to point their readers to more information on the subject.
Typically, a list is made of links to the CWE to the ASVS and to some more relevant resources.
BUT
The idea with OpenCRE is that you simply link to the common requirement 'storing secrets' at opencre.org.
It's a page where you can find everything you need, and it will be up to date.

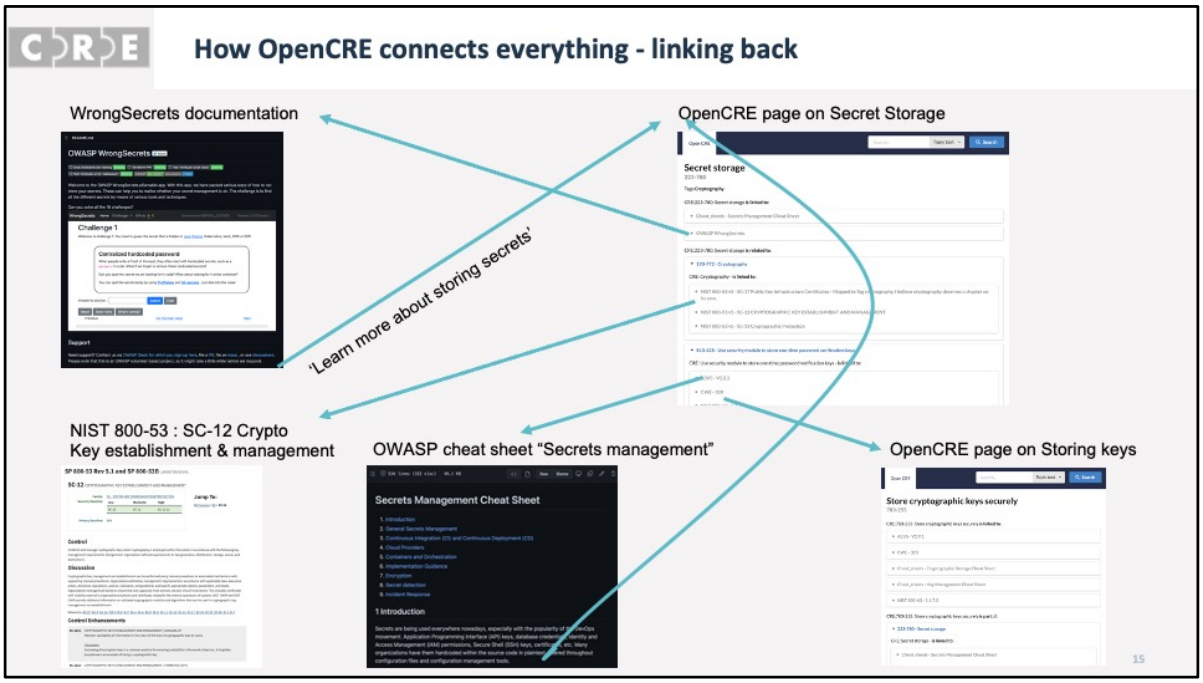
(Cheat sheet on managing secrets:
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Secrets_Management_CheatSheet.md#262-rotation)



You can see here that opencre links to the relevant NIST publication, to the relevant cheat sheet, etc. etc.
Great, everything is there.
And also, when I want to explore related topics. I can go do that. Because…

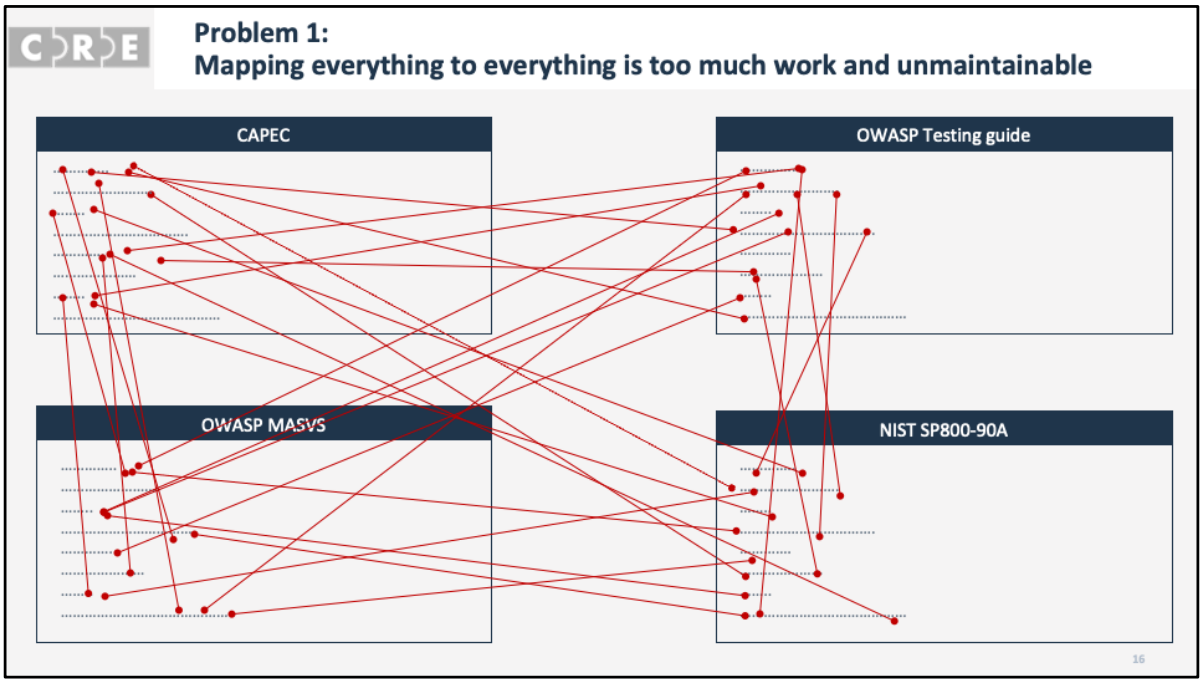


Secret storage also links to other common requirements with related information that I can find from there.
Such as Storing keys safely.
..
And finally, this whole ecosystem also features backlinks.

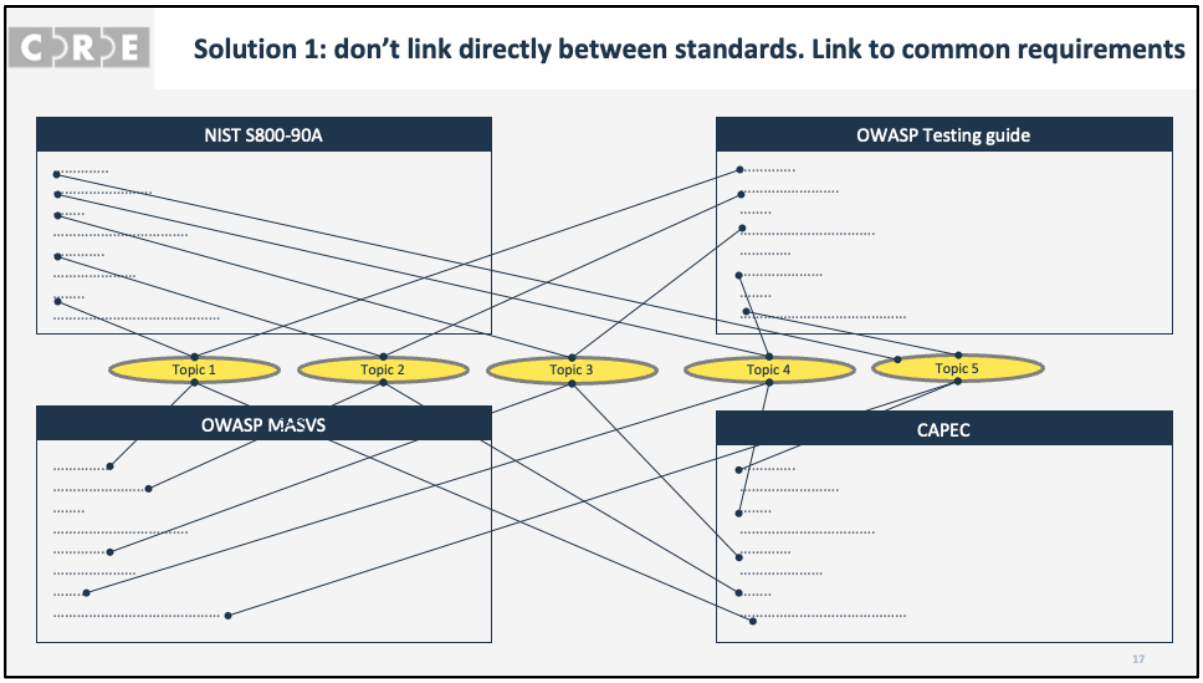


As you can tell there is a link back from opencre to the wrongsecrets documentation. Why?
Well if somebody is looking at the Cheat sheet, and follows the link to OpenCRE, - they may be interested in the WrongSecrets project as well.

So. There you have it. Everything linked with OpenCRE. And we have built it. Opencre.org is operational in beta right now
and open source. It works. And to make it work we first had to overcome a number of hardships and battle a couple of monsters.

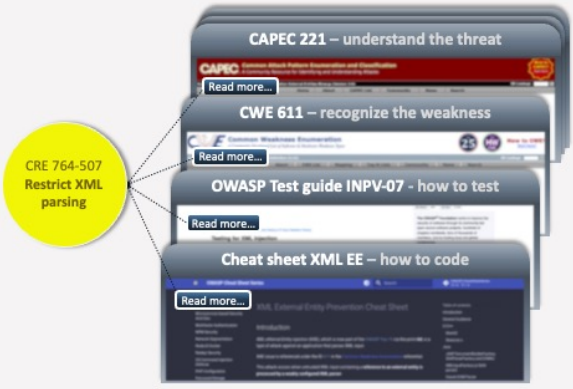


So, what did we do to make this work.
Creating an administration of how everything maps to everything is impossible,
It's what the industry is trying today, but if you want a cover just 1% of what is out there, it's a gigantic amount of work to setup and then maintain.



We solved the mapping problem by introducing what we call "common requirements":
these are generic security topics, and a standard only needs to link a section to ONE of those
instead of all the other standards.
The great result is that if two sections in different standards link to the same common requirements,
they link to each other by definition.
Let me show you

Example of linking standards through a common requirement



ENISA: we need a repository of common security requirements

ENISA report:

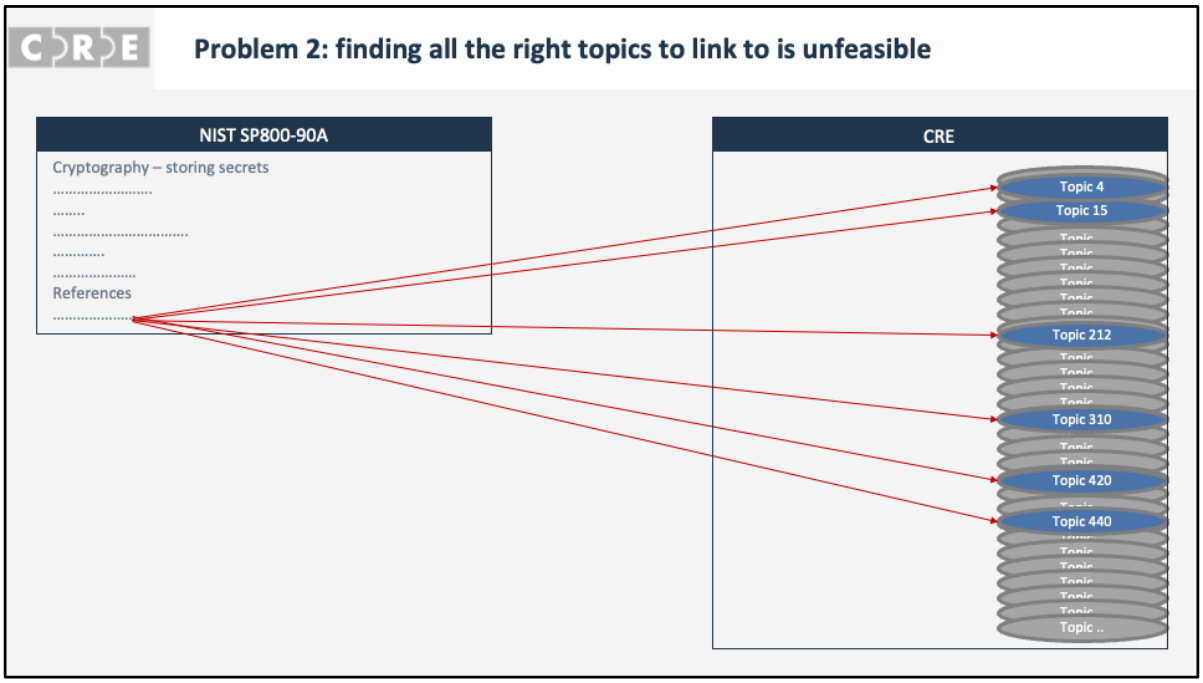
"Requirements largely overlap, demonstrating that software security is mainly a generic problem and both Standards Developing Organizations (SDOs) and European Standards Organizations (ESOs) or good practice producers are often working without proper coordination and effective liaisons "

"DEVELOP A COMMON REPOSITORY FOR SHARED SECURITY MEASURES"

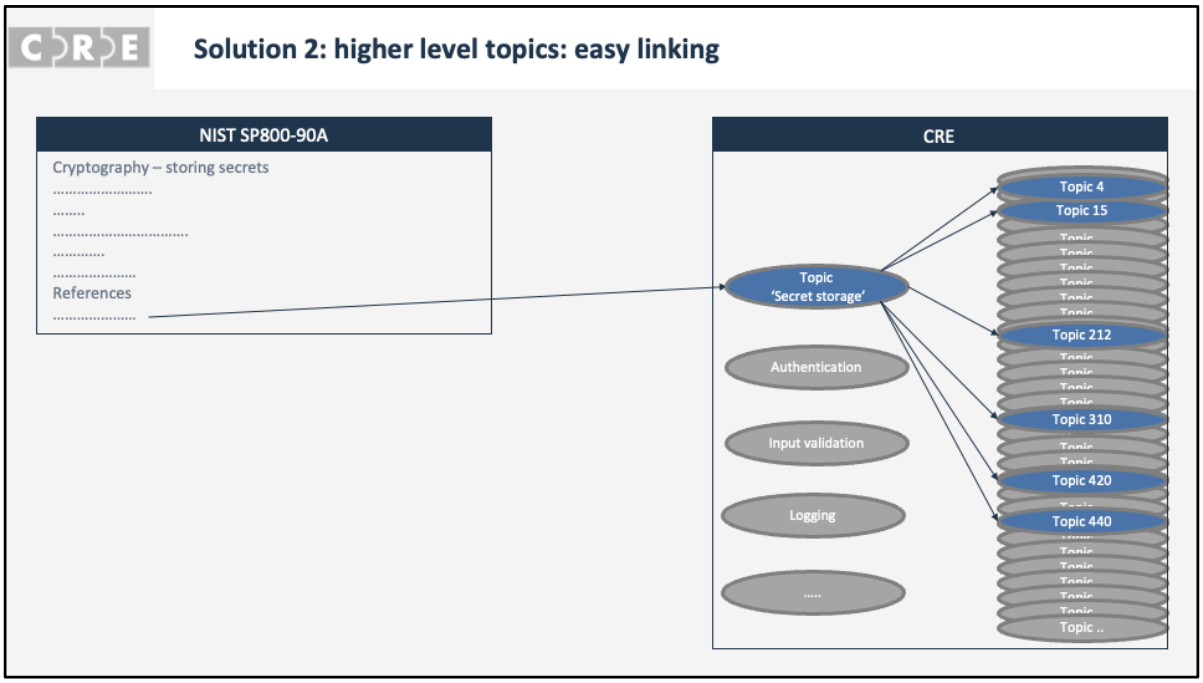
"Aligning on requirement commonalities across different schemes prevents proliferation and fragmentation, while also making drafting and maintaining a scheme more efficient in terms of mitigating the risks."

19

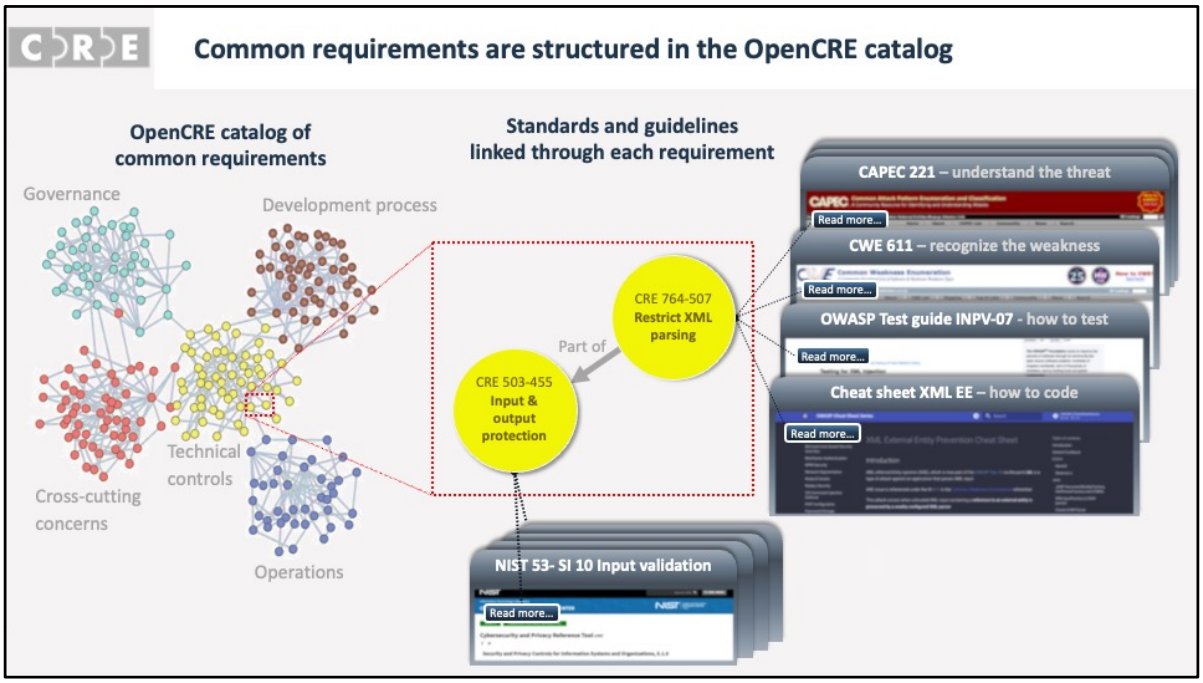
In 2019 ENISA did some research on the security standard landscape and observed the mapping problems I mentioned.
One of the ENISA recommendations is to develop a common repository for requirements.
And this is exactly what we did inwith OpenCRE.

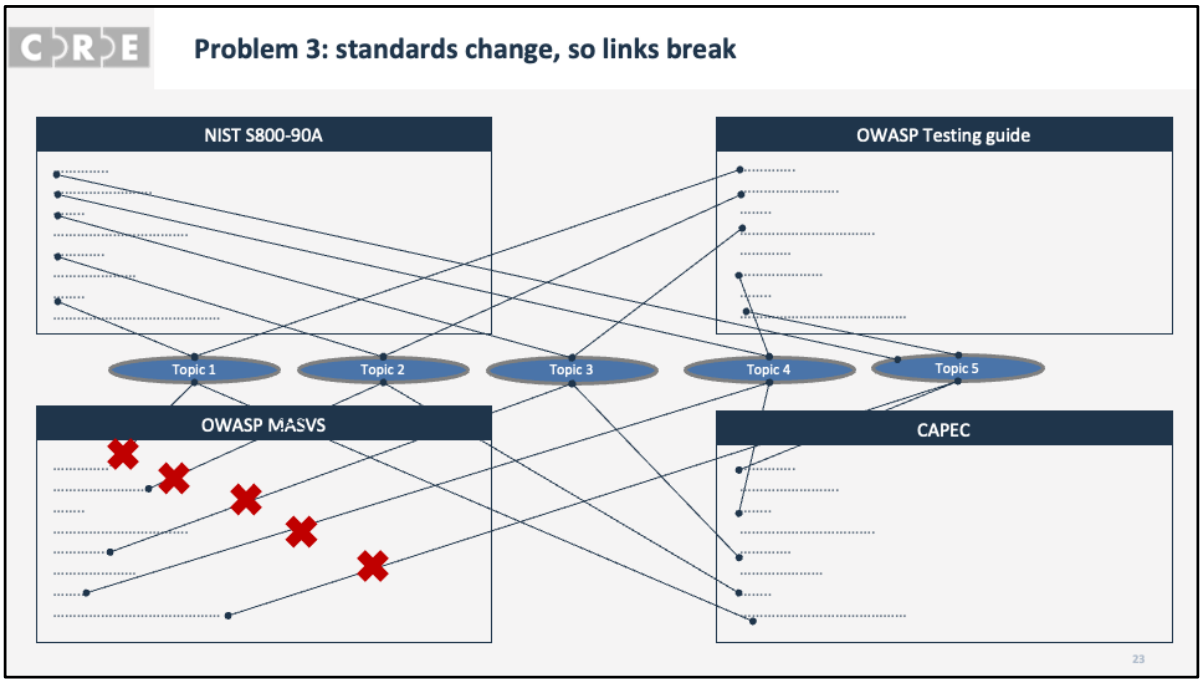


So we started creating all those topics, but then we ran into another problem. There are many topics, so if you are writing
a standard on storing secrets you would have to find all topics at OpenCRE that are relevant to that subject.
This is hard and it's a lot of work.

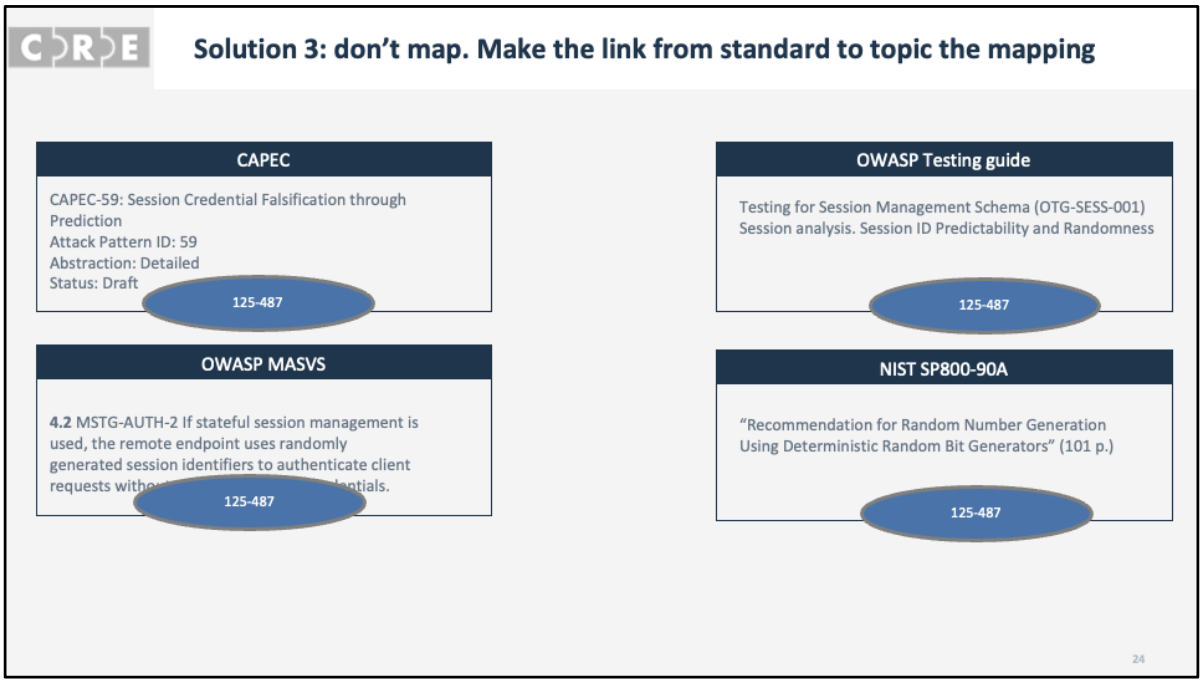


We solved this by introducing higher level topics, for example,,, 'secret storage'. That way you only have to link to that topic,
and you automatically link to all subtopics as well.
By introducing this topic structure, we are in fact building a semantic web of security topics.
We did this by doing a lot of research and workshops and by using existing work on harmonising standards -
for example the security model developed by Software Improvement Group, that they donated to be used as input to the framework.
This has a nice bonus, because users can follow the links between topics to navigate and explore information -
up the tree and down the tree.

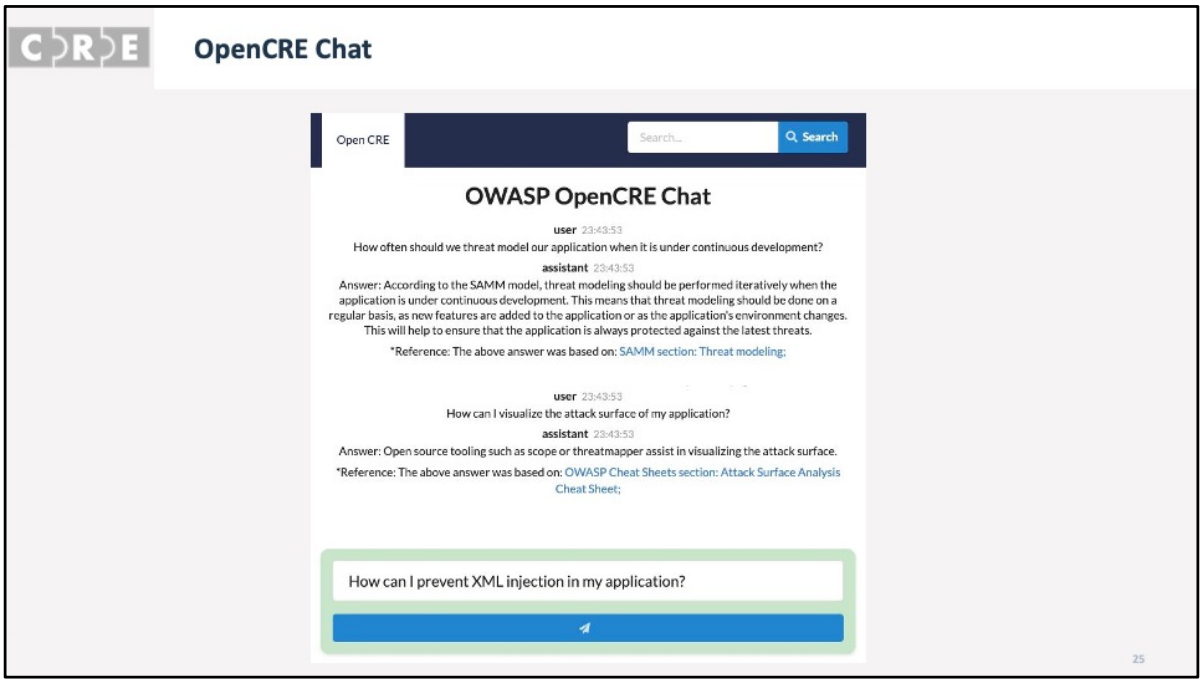

CRE
Common requirements are structured in the OpenCRE catalog
OpenCRE catalog of common requirements
Governance
Development process
Technical controls
Cross-cutting concerns
Operations
Standards and guidelines linked through each requirement
CRE 764-507
Restrict XML parsing
Part of
CRE 503-455
Input & output protection
CAPEC 221 – understand the threat
Read more...
CWE 611 – recognize the weakness
Read more...
OWASP Test guide INPV-07 - how to test
Read more...
Cheat sheet XML EE – how to code
Read more...
NIST 53- SI 10 Input validation
Read more...



Then we ran into another problem. After linking to a standard, the standard changed their structure and the links were broken.
It became clear to us that you can't keep up with the links. Standards constantly change. So links break at some point.



We solved this by making OpenCRE self-maintaining.
If a standard contains a link to OpenCRE in the machine readable source, our parsers can scan that standard and
when it finds the link it sees: okay this is a section of this standard with this name, with this number and it links to this topic in OpenCRE. The information is all there.
So the mapping is not maintained in some separate text file, table or sheet. It is maintained in the standard itself
and automatically moves around with the standard, without requiring any effort by anybody.
Obviously this requires the standard to add links to OpenCRE in their material.
For standards that don't have this, a mapping file needs to be maintained, on github, to which people can contribute.
And we have made that operational.

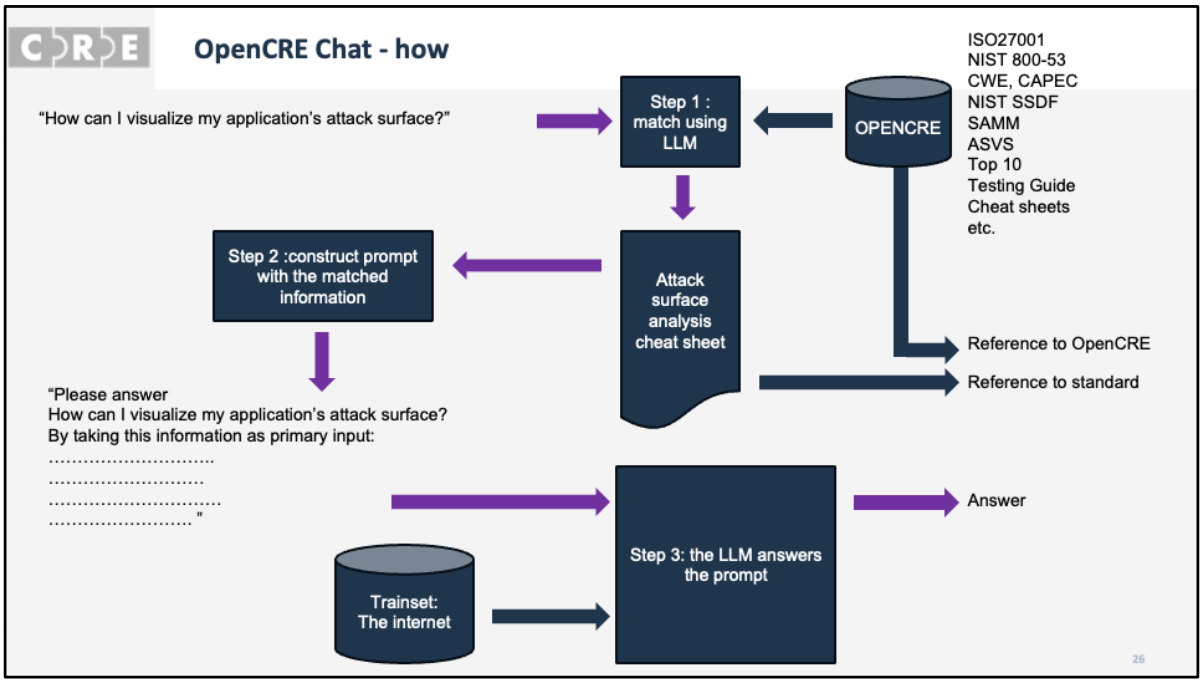


Having all these standards in a catalog opens up so many opportunities!
Perhaps the most exciting thing coming out of this is OpenCRE Chat, which we have developed in collaboration with Google:
It is the world's first security specialized chatbot.

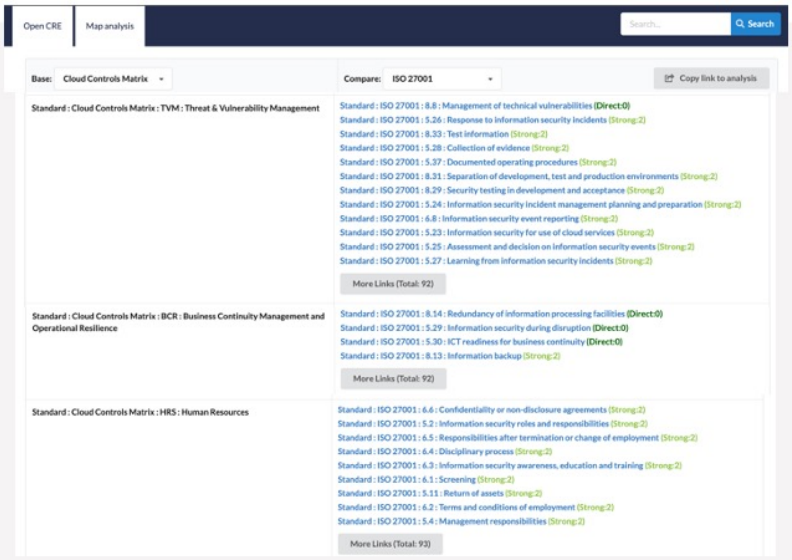
It is a large language model, like for example ChatGPT. And the unique thing is that it uses OpenCRE as a catalog of collected and vetted knowledge from the key security standards. That knowledge serves as the preferred input to answer questions on security for which the chatbot also provides references.

Credit to whom credit is due: The first one with this idea was Sherif Mansour, who started this initiative. And of cours a big shout out to Google for making this happen, and to Software Improvement Group for sponsoring it.

It speaks many languages by the way. The first response we got was from Japan where people are happy they can query security standards now in their own language.


OpenCRE Chat - how
"How can I visualize my application's attack surface?"
Step 1 : match using LLM
OPENCRE
ISO27001
NIST 800-53
CWE, CAPEC
NIST SSDF
SAMM
ASVS
Top 10
Testing Guide
Cheat sheets
etc.
Step 2 :construct prompt with the matched information
Attack surface analysis cheat sheet
Reference to OpenCRE
Reference to standard
"Please answer
How can I visualize my application's attack surface?
By taking this information as primary input:
.....
.....
.....
....."
Trainset: The internet
Step 3: the LLM answers the prompt
Answer
26

Map analysis



Wrapping up - why OpenCRE ?

OpenCRE **democratizes** cyber security :

- Enable engineers, security officers, testers, auditors and procurement to **find security answers**
- Enable **standard makers** to refer their readers - comprehensively, clearly and robust
- Enable **standard makers** to be found

Bonus:

- Attain **shared understanding through a universal translator:** management, compliance, security officers, engineers, testers, auditors, vendors, clients
- Achieve **more consistency and less gaps** between standards

28

Call to action

Use www.opencre.org and spread the word (e.g. social media) – search, browse, chat and getting referred
Join the mailing list: project-cre@owasp.org

Contribute: provide your feedback and ideas: https://github.com/OWASP/OpenCRE

Details: https://github.com/OWASP/OpenCRE/blob/main/CONTRIBUTING.md

Join our team: https://owasp.org/www-project-integration-standards/

Security authors and tool makers unite! And start adding CRE-links to your work:

- Link to CRE to provide your viewers access to a large range of related resources, with advanced browsing, search and chat
- Your benefit:
  - You won't need to write everything yourself
  - Saves you time on finding references and keeping them up to date
  - Links will never break
  - If relevant, your standard becomes instantly findable through OpenCRE – and part of OpenCRE chat: contact us!
- Join our stakeholder group to help steer the CRE direction

29


THIS
IS
THE
WAY


OWASP 2023
GLOBAL
AppSec
WASHINGTON
DC
OCT 30 • NOV 3
THANK YOU