OWASP Common Numbering

CW's feedback, 22nd March 2011

I've put down quite a lot of thoughts here. It's only possible to come up with these now that Dave and Kevin have put the effort into coming up with an example section – that really helps. I have stronger or weaker views on some of my suggestions below, but I hope writing this all down helps the discussion, and improves the final result.

Firstly, a few things to consider as requirements are written.

Longevity

We should try to make sure each requirement (in OCR) is as technology agnostic as possible – to minimise future changes. I haven't anything in particular to point at as an example here, but just something to have in mind.

Generality

We might want to avoid duplicating requirements for particular aspects. So in authentication could "password" also include PIN and token and "device signature"? If so, we might want to scribble a short glossary as we progress. That would also avoid having the various guides having to write out examples every time e.g. "passwords (including PINs, tokens, etc)". Perhaps we could reference the OWASP ASDR for this?

Terminology

Very minor issue.... we should try to come up with agreed terms for the elements of the scheme. This could be considered a very trivial thing to comment on now, but it will help our discussions, and provide more clarity to others and thus aid future adoption. These seem to be some of the important things:

- "requirements area" or "requirements sector"?
- "requirements numbers" or "codes"?
- "requirements" or "common requirements"?
- "numbering system" or "numbering schema"?

I don't have a view about any of these, but I think we need to be consistent.

Requirement text labels

Having seen the example OCR-AUTH area, I wondered if very short, and/or less descriptive/qualitative labels would be better. The full text could be an additional descriptive field, or just somewhere else entirely such as only in the SCP. (I touch on this idea of separating the SCP a little from the OCR taxonomy a few times below, so please read on).

If we were to consider the possibility the SCP will have more detail, then we don't need to edit the OCR text label just because the SCP team come up with some more bright ideas to improve a requirement in the future. This is important because it might alter mappings. OCR-AUTH-13 already shows one requirement where the SCP

has a lot more text than the OCR requirement – and why, not?

For example, here are two current OCR-AUTH requirements:

- OCR-AUTH-17 Brute force protection is provided after a system configurable number of invalid login attempts occur against an account within a configurable period of time (e.g., account is locked, CAPTCHA required, throttling enabled).
- OCR-AUTH-26 Users are notified when a password reset occurs on their account.

Actually the SCP is a little different to this currently. But the OCR text labels could be:

- OCR-AUTH-17 Brute force protection
- OCR-AUTH-26 Password reset notification

Or perhaps something in-between in level of detail would be better:

- OCR-AUTH-17 Brute force protection for user authentication
- OCR-AUTH-26 Password reset notification to users

We still have a one-to-one mapping with the (current) SCP, but the how/why/meaning/intent is no longer in the label text.

Scheme structure

The proposed scheme suggests the major/minor relationships are built into the numbering scheme, as well as by requirement area:

OCR-[AREA CODE]-[PRIMARY REQ NO]-[SECONDARY REQ NO]

Consider OCR-AUTH-11, 22, 23 and 26. These could become something like (ignore the exact text for the moment):

- Password reset
    - Questions
    - Use of email
        - Encrypted communications
        - Destination email address
    - User notification

This might make sense from a classification point of view, but would add complexity to the SCP. Having any form of structure also means decisions have to be made about things like:

- whether ever node is a requirement, or just "leaf nodes"
- how to deal with a child node which could have more than one parent, etc

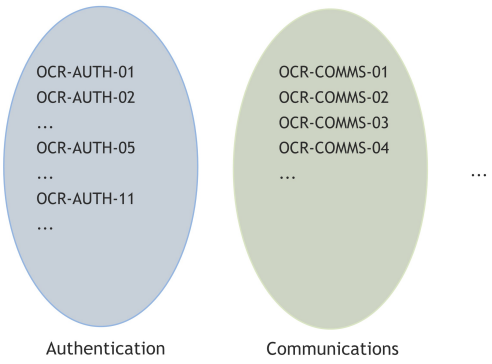
All that can make it more complicated to manage.

So whilst there seems to be some relationships, or groupings, it might be best to keep the structure flat. Relationships (e.g. "is a more specific than...") and mappings (see below) between individual requirements can be used to add detail if required.

Area categorization

Here I'll suggest why I think we might want to consider removing the 2nd element (requirement area) as well.

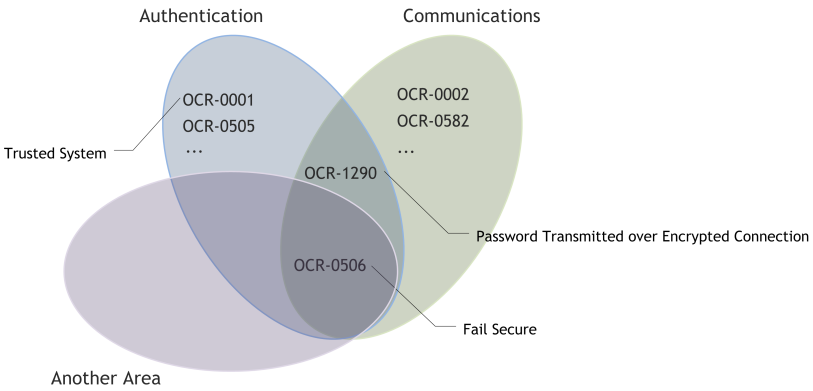
Figure 1: Current Proposal
Each item exists in only one requirements area



It seems that some requirements could site perfectly well in more than one category. An example of this might be encryption of passwords in transit (currently listed as an AUTH requirement). Also, some requirements could apply to many areas (e.g. the "fail secure" item mentioned in the document's comments. As another example, how might a new requirement like "having a list of previous significant events available for the user to view (i.e. not just last logged on date) fit in. That might be AUTH if it focused on just authentication successes and failures, but it could equally be in LOGS if it also highlighted significant events such as password changes, changes of email address, postal address, or payment transfers.

So, a suggestion would be to avoid area categories in the numbering scheme. This would mean requirements only have a number such as OCR-01001, OCR-89505, etc.

Figure 2: Alternative Proposal
Item numbering is area-independent and requirements area are simply one categorization. A consequence is there is no need to duplicate 'identical' items like OCR-AUTH-05 : Fail Securely, and it doesn't matter which area an item is considered to be in, and the actual number has no meaning other than being an identifier.



The number and order is meaningless. Removing the area categorization makes it easier to add requirements. Please read the email from Steven Christey (who I do not know) which raised this issue in my mind:
http://lists.owasp.org/pipermail/owasp-topten/2010-January/000583.html

SCP Guide

I think Keith and Dave have already made some suggested alterations to tie the SCP and OCN together very closely. But why bother? The SCP has a purpose, and audience, in mind, and it should be laid out and written for that – not to match a thesaurus. There are great benefits to keeping the SCP one page per area, but it doesn't make sense forcing a limit on the number of requirements per area in a numbering scheme. Why couldn't one requirement in the SCP link to two in the OCR, or vice versa?

It's true the SCP will be the closest document to the OCR, but I don't think it should be constrained in this way.

Based on all of the above, I think the proposed one-to-one relationship between the OCR and the SCP, will cause difficulties later. Although they are going to be very, very similar, we shouldn't get into the position of one of these forcing a change in the other. So I think the SCP should be somewhat more like the other guides, and choose to structure itself however it wants without having to match the OCR.

The SCP should be free to display/structure/(select) which requirements to highlight, and it shouldn't be forced to include everything in the OCR (but it might!). It is possible the OCR could be more finely grained sometimes, and SCP items reference multiple OCR requirements. This also makes cross-area referencing more natural.

To re-use an example from above, SCP item 26 on authorization, might refer to two (made up) OCR requirements:

- OCR-01234 Password reset
- OCR-24004 Out of band confirmation

Separating the one-to-one relationship also means that other application security requirements could be included in the numbering system. For example, requirements might include aspects mentioned in the example software contract annex, or from SAMM. None of these fit into the SCP, but they may well be included in organization's requirements during procurement or development of software. The scheme already alludes to "non-technical" documentation requirements and verification techniques... so let's not rule out anything else by forcing the SCP to be everything.

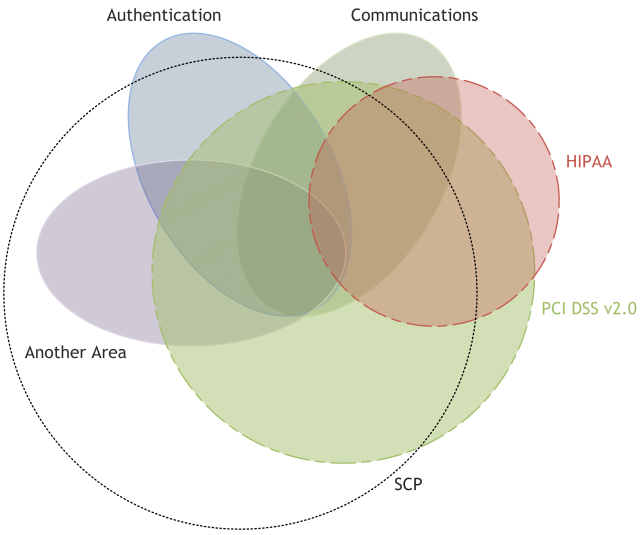
Reserved number spaces

We may want to allocated some codes/sequences for end-users to use for their own additional requirements e.g. OCR-90000+

Mappings

One of the ASVS sections is sensitive data protection which has been identified as OCR-DATAP. It's an interesting one (and a section of ASVS I contributed to), but there are lots of other potential compliance topics, and data protection requirements vary with jurisdiction, the actual data, etc. Some data protection security controls are actually in other requirement areas already.

Figure 3: Mapping Overlays
Compliance and other aspects can be mapped to OCR. Not all requirements might be in the SCP.



Therefore these topics, and other cross-cutting issues, could simply be groups of (unstructured) OCR requirements, where it does not matter if they are AUTH, AUTHZ, etc. So we might have different views of requirements like:

- Data protection:
  - HIPAA
  - EU Data Protection Directive
    - UK
    - Germany
    - etc
  - California Online Privacy Protection Act
- PCI DSS
  - 1.2
  - 2.0
- Someone's guide to secure application change management
- OWASP Top Ten 2010
- etc

These views on the OCR could be created by others (e.g. the OWASP PCI DSS project). Views would link to OCR requirements, and have additional descriptions e.g. a tighter interpretation of password complexity.