CyBOK

New Knowledge Area in Applied Cryptography

The CyBOK project team welcome constructive feedback and comments from the cyber security community on the proposed change to CyBOK version 1.0 as detailed below.

To support this process we would appreciate if all comments could be based around the following points:

- Positive points (what did you like) about the KA?
- What is missing from the KA and why?
- Should anything be removed from the KA and why?
- How could the KA be improved? (with examples and references)
-

Rationale for proposed change:

The current KA on Cryptography provides an excellent introduction to cryptographic primitives, schemes, and protocols. It identifies some core theory and then covers the main cryptographic primitives in a logical way. However, its scope does not extend to the practical application of cryptography, and so it does not discuss many aspects of cryptography in practice. The proposed change is to introduce a new KA, complementary to the Cryptography KA, that covers the practical application of cryptography within cyber security, and area that is not currently covered within CyBOK.

Proposed change:

Introduction of a new KA on Applied Cryptography. This new KA would focus on what cyber-security experts should know about cryptography from a system point of view.

It will of necessity build on many of the topic areas covered in the Cryptography KA (symmetric encryption, public-key encryption, hash functions, message authentication codes, digital signature schemes, standard protocols).

New topics to cover will include:

- Introduction to core security services
- Algorithm/protocol selection, and the context of potential attacks
- Implementation aspects (applying cryptography at different network layers; libraries)
- Attacks on implementations (e.g. on weaknesses in cryptosystems, side-channel, memory attacks, key protection)
- Key management (including key generation, agreement, derivation, certification, transportation)
- Public key Infrastructure
- Randomness (generators, sources, pseudo-randomness)
- Applied case studies (example crypto applications)
- Cryptography policy aspects
- Standards

This KA will not affect the technical content of the KA in Cryptography and will cross-refer back to the primitives in that KA wherever possible. However it may necessitate a change to the introduction of the Cryptography KA, and perhaps a change of title to Foundations of Cryptography,

to reflect the new presence of two KAs focussed on cryptography and to explain the relationship between them.

Depends on KAs:

- Strong dependency: Cryptography,
- Weak dependency: Authentication Authorisation & Accountability, Privacy and Online Rights, Distributed Systems Security, Hardware Security

Depends on External Knowledge: none

How to comment:

The consultation period will be open for a period of 4 weeks until **Friday 28 August 2020** and all comments should be sent to contact@cybok.org. Further details of the CyBOK review and update process can be found on the CyBOK website: https://www.cybok.org/resources/.