New Knowledge Area (KA) in Formal Methods for Security

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:

Formal Methods in Security is a well-established subject area with its own mature research community. It is focused on formal specification, modelling and reasoning about the security of systems and protocols, and covers a wide variety of approaches, techniques and tools. This is a body of knowledge in its own right, and although it cuts across and applies to a number of the existing KAs, it is not collected together in a separate systematic way. Existing KAs that include elements of formal methods should retain these but with the addition of cross references. However existing KAs are self-contained and should not be disrupted by the introduction of a new KA.

Proposed change:

Introduction of a new KA, on Formal Methods for Security.

This KA would encompass: Developing and reasoning about computer systems, components and protocols by means of logical and mathematical descriptions to enable specification and proof of security properties.

This KA is concerned with the approaches, methods and tools that are used to reason mathematically about computer systems with respect to their security properties. Designs can be proven correct with respect to formally expressed security requirements, in the context of particular classes of adversaries. Formal methods is relevant to several other KAs, since it encompasses a general approach to modelling, analysis and verification, which is applicable to many technical aspects of cyber security.

This KA would assume background knowledge of logic, discrete mathematics, theorem proving, formal languages, programming semantics, and would give links to further references covering these background topics.

Modelling and abstraction is a cornerstone of formal methods, and the KA will cover the application of computational modelling and symbolic modelling across security topics, including access control, information flow, security protocols, and program correctness. These can be considered with respect to requirements such as authentication, confidentiality, anonymity and integrity, and in the context of specific attacker models which capture particular classes of threat.

The KA will also cover the variety of approaches to verification, including both computational and symbolic approaches, and covering game-based, simulation-based, universal composability, equivalence, refinement, and semantics based, and will cover logic-based and language-based approaches to specification.

The KA will cover the tool support available for the above approaches to make them practical, including theorem-proving tools and model-checking tools, as well as support for code analysis techniques. The KA will cover the main general purpose formal methods tools that have been applied to security reasoning, and will also cover tools developed specifically for security analysis. Tool support for program development and for reasoning about code will also be covered here.

Depends on KAs: AAA, Distributed Systems Security, OS and Virtualisation Security, Web and Mobile Security, Software Security, Network Security, Hardware Security, Cyber-Physical Systems Security, Cryptography

Depends on External Knowledge: Logic, Discrete Mathematics, Theorem Proving, Formal Languages, Program Semantics

Existing KAs that include elements of formal methods should retain these but with the addition of cross references. However the proposal recognises that existing KAs are self-contained and should not be disrupted by the introduction of a new KA.

How to comment:

The consultation period will be open for a period of 4 weeks until **Friday 20 March 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/.