CyBOK

Extend Network Security Knowledge Area

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 Network Security KA does a good job of covering IP-based networks and the security properties (and vulnerabilities) of various protocols in this context. However, this discussion would benefit from being placed in the broader context of network architectures – and more specifically, security architectures for networks in particular application domains. The rationale is that such architectures vary across domains. The current security mechanisms provide a good coverage of network intrusion detection systems. There is, however, a need for a broader discussion on security mechanisms, such as for network isolation.

Proposed change:

It is proposed that the KA is revised to start with a broader discussion of network security architectures. This should include security considerations in a (representative) range of non-internet network contexts (IP & non-IP), such as private data centre networks; content distribution networks, cloud-based architecture; hybrid network architectures; vehicular networks; operational control systems (SCADA/cyber-physical systems) networks; overlay networks; corporate international networks. Some consideration should be given cross-border regulatory issues in these contexts. These application areas could usefully be linked to other relevant CyBOK KAs.

This should be followed by the current discussion of the protocol stack and the security issues across various layers (current sections 2-7) with this discussion contextualised and update in the light of the new content on network security architectures. Section 4 should include a treatment of the fundamental design changes introduced in TLS 1.3.

Section 8 should then be expanded to include a wider range of network defence mechanisms, e.g., network content separation; VLAN design issues; cross-domain solutions (multi-level security); deep packet inspection; techniques for network security monitoring and traffic analysis data loss prevention techniques; and use of combinations of network defence tools to achieve particular high-level goals.

Move Software Defined Networking into Section 8 as a routinely-deployed technology; remove IoT security and delete Section 9.

How to comment:

The consultation period will be open for a period of 4 weeks until **Friday 31 July 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/.

Date: 29 June 2020