Change request title:

Major revision of Web and Mobile Security Knowledge Area

Change rationale:

CyBOK was originally scoped in 2017 and several Knowledge Areas (KAs) have not seen any significant change requests from the community. This may be a reflection that the KAs continue to represent an up-to-date view of the foundational knowledge in the field. However, it is prudent for the CyBOK editorial team to initiate a proactive review of all five categories to ascertain that this continues to be the case and, if not, identify change requests on which the community may be consulted as part of the normal CyBOK update process.

The CyBOK editorial team, therefore, initiated a pro-active review of the KAs within the Software and Platform Security category. A panel of experts reviewed the KAs within the category and provided input on potential changes. The proposed change request has been distilled from these reviews and panel discussions.

The Web and Mobile Security KA continues to represent a strong and cohesive body of knowledge for the topic. However, over the last few years, there are a number of new developments including on authentication approaches, API security, permission models and how these are communicated to users. The proposed change request is to update the KA to incorporate these elements.

Description of change:

Revision to the KA to incorporate the following key changes.

- Clarify the scope and interaction of apps and web services with IoT and Industrial-IoT devices. The backend services and cloud platforms, together with the apps, form an integrated infrastructure. Web and Mobile security needs to be considered in the context of this integrated infrastructure.
- Include a principled discussion on permissions and authentication with contemporary designs as exemplars and their strengths and limitations. The following changes should be incorporated:
    - Update the discussion on Android permissions as install permissions no longer exist. These can be removed and a clarification added as to why these were abandoned. Furthermore, there are more than two permission levels/classes in Android, and the description should be updated to reflect that.
    - Update the web authentication discussion to include HTTP digest authentication. It should also be clarified that other (form based) authentication mechanisms mostly rely on cookies to pass authentication state in the otherwise stateless HTTPS connections. A discussion on more contemporary approaches such as single sign-on and passkeys should be included as well as more detail on web authentication.
    - For mobile authentication, include a discussion of the role of those biometrics in widespread use in mobile devices. Mobile devices are also commonly used in multi-factor authentication, either through SMS or through an authenticator app. A discussion of the benefits and potential risks should be included. Furthermore, a clarification is needed that, while most Android devices perform the biometric pattern matching in a Trusted Application (TA) running under an ARM TrustZone TEE, this is not the only implementation. If there is a StrongBox dedicated secure element, parts of this comparison might run there instead. On iOS, the comparison supposedly happens inside the Secure Enclave, although I am not aware of all the details. Therefore, they do not

necessarily always rely on ARM TrustZone in particular - that is only one potential implementation.
    - The discussion on passwords needs to be updated to incorporate password managers especially as most browsers now provide built-in support for passwords and passkeys. The various features of password mangers and their implications in terms of functionality vs. complexity and usability should be discussed.
- Include a more detailed discussion on DOM-based XSS and context-sensitive escaping.
- Include a discussion on security and safety mechanisms built into mobile OSs and apps, e.g., to encrypt client-side storage, use of privacy and safety labels for apps. This should also cover the strengths and limitations of such mechanisms.
- There needs to coverage of API security, JSON Web Tokens (JWT) and Single Page Applications (SPA) frameworks.
- Include a discussion on server-side/infrastructural mitigations, e.g., containerisation and WAF/CDN.
- Include a more expanded discussion of CSP.
- Expand the discussion on vulnerabilities to provide a more comprehensive coverage of OWASP Top 10. The mitigations should also be expanded to include approaches based on separation between control and data, and languages/platforms that mitigate against them by design. Suitable cross-references to the Software Security KA should be included.
- Include discussion on client- and server-side timing attacks.

Minor points of detail also need to be addressed, including, that EV certificates are no longer displayed as prominently; discussion of Typescript when JavaScript is described; QUIC and HTTP/2.0; updates to HTTPS indicators; discussion of SameSite cookies; and that many browsers now block third party cookies by default. Furthermore, the discussion on Phishing should be updated to include SMiShing and the effectiveness of FIDO2/WebAuthn as a mitigation against the credential stealing part of phishing.

Depends on KAs:

- Human Factors; Privacy and Online Rights; Malware and Attack Technologies; Adversarial Behaviours; Operating Systems and Virtualisation Security; Authentication, Authorisation and Accountability; Software Security; Network Security; Hardware Security; Physical Layer Security.
- The dependency on Cryptography KA should be updated to Applied Cryptography KA.

Depends on External Knowledge:

- ACM Computer Science Curriculum NC/Network Applications
- ACM Computer Science Curriculum PBD/Web Platforms
- ACM Computer Science Curriculum PBD/Mobile Platforms

References:

(1) René Mayrhofer, Jeffrey Vander Stoep, Chad Brubaker, Dianne Hackborn, Bram Bonné, Güliz Seray Tuncay, Roger Piqueras Jover, Michael A. Specter (2023). **The Android Platform Security Model**, CORR abs/1904.05572. https://arxiv.org/abs/1904.05572

Date: 6 June 2025