6 May 2014 Study · Mobile Security · Privacy & Crypto

Security Analysis of Smartphone Platforms

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/security-analysis-of-current-smartphone-platforms/

Current smartphones have significant data-processing capabilities and are increasingly being used to process critical corporate data. For this reason, common smartphone platforms have been supplemented with many security features in recent years, which were initially not present as the primary sales target was the private user. The current versions of Android, iOS, Windows Mobile and Blackberry support a large number of security features that are suitable for use in enterprise environments and for handling security-critical data. Examples of these features include the integration of encryption systems, management interfaces that allow policies to be defined for these devices, or secure key material and password storage. The aim of the attached A-SIT study is to provide a basis for assessing the suitability of a smartphone platform for use in the enterprise.

Specifically, the following points will be examined in more detail:

- Basic security properties
- Access control
- Encryption
- Software sources
- Update situation
- Mobile device management interfaces
- Bring-your-own-device capabilities

The following presentation is intended to show the differences between the individual platforms. For more detailed explanations and a detailed analysis of the individual platforms, please refer to the full version of the study (available in German) below.

Since the encryption system is an essential component with respect to protecting sensitive data and cryptographic keys, the corresponding components of the platforms iOS and Android have been subjected to a detailed analysis.