20 August 2021 Study · Mobile Security · Web & Cloud

Automatic Detection and Mitigation of Crypto API Misuse in Android Applications

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 This content is no longer updated.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.

Version 2021-08-20
Source https://technology2.a-sit.at/en/publications/automatic-detection-and-mitigation-of-crypto-api-misuse-in-android-applications/

Almost a decade after its first scientific discussion, crypto API misuse remains one of the most common security flaws in Android applications. Due to invalid parametrizations of cryptographic primitives or functionality for establishing TLS connections, malicious parties can frequently gain access to sensitive user data through unsophisticated attacks. Since all efforts by the platform provider Google could not lead to any substantial improvement to the situation, we suggest a novel approach for mitigating the risks of this long-standing issue for end users. Our solution consists of a background daemon that automatically augments all applications installed on an unmodified Android system by a patch for monitoring and correcting any calls to cryptographic APIs. We demonstrate the efficacy of this approach by means of two case studies of popular Android applications from Google Play.