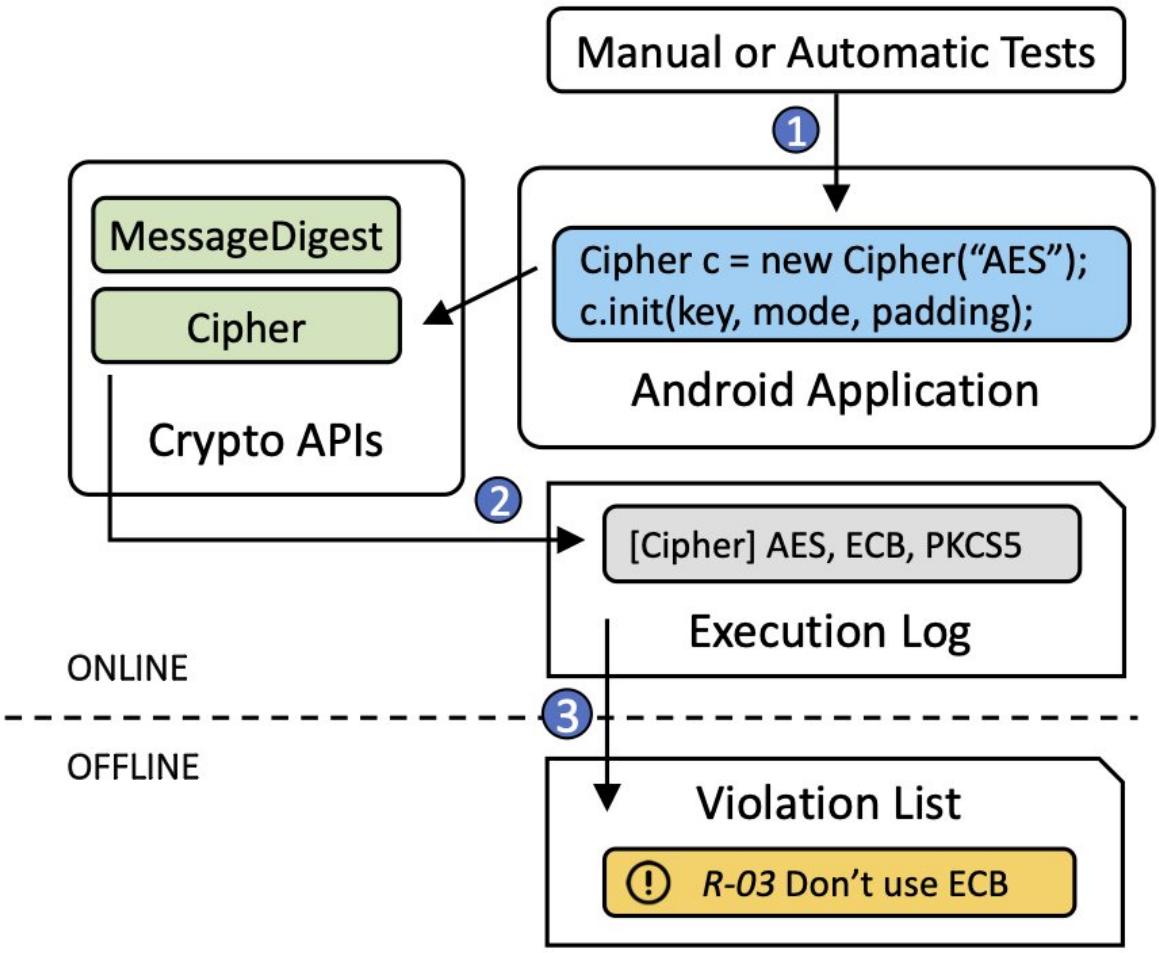
New tool detects unsafe security practices in Android apps

November 9 2020



How Crylogger works: 1. CRYLOGGER runs the application with an instrumented crypto library.2. CRYLOGGER collects a log containing the parameters of the crypto API calls. 3. CRYLOGGER checks the crypto rules and reports all the violations. Credit: Luca Piccolboni/Columbia Engineering

Computer scientists at Columbia Engineering have shown for the first time that it is possible to analyze how thousands of Android apps use cryptography without needing to have the apps' actual codes. The team's new tool, CRYLOGGER, can tell when an Android app uses cryptography incorrectly—it detects the so-called 'cryptographic misuses' in Android apps. When given a list of rules that should be followed for secure cryptography—guidelines developed by expert cryptographers and organizations such as NIST and IETF that define security standards to protect sensitive data—CRYLOGGER detects violations of these rules.

Android apps use cryptographic algorithms to secure users' data, such as credit card numbers, passwords, social security numbers, etc. If used correctly, cryptography protects sensitive data by making them unintelligible. Each cryptographic algorithm is appropriate for a specific scenario and requires the configuration of specific parameters. App and library developers, however, can misuse the application programming interfaces (API) of such algorithms by using constant keys, weak passwords, or by misconfiguring other specific parameters.

"Choosing the correct algorithm and configuring its parameters are critical to keep users' data secure, but it requires an understanding of cryptography," says the study's lead author Luca Piccolboni, a Ph.D. student who is advised by Luca Carloni, professor of computer science. "Wrong choices of the algorithms and/or misconfigurations of their parameters can result in data breaches."

CRYLOGGER is the first tool that detects cryptographic misuses by running the app instead of analyzing its code. This new approach is described in a paper that will be presented May 23-27 at IEEE Symposium on Security and Privacy 2021. In addition to Piccolboni and

Carloni, the paper is authored by Giuseppe Di Guglielmo, associate research scientist in the computer science department, and Simha Sethumadhavan, associate professor of computer science and an expert in cybersecurity.

CRYLOGGER, which is open source, has several key advantages:

- It can analyze closed-source apps, and does not need to modify the code of the app or its binary.
- It analyzes the actual parameters used by the apps instead of doing analysis on their source code and it focuses only on the code that is actually run.
- It can perform inter-application analysis: it can detect when two apps communicate in non-secure ways or when data is shared across multiple apps when it should not.

The researchers ran 1,780 popular Android apps downloaded from the official Google Play Store—the largest case study on cryptographic misuses not based on code analysis—and discovered that almost all the apps contained code or used libraries that did not strictly adhere to security standards. Many of them used broken algorithms and others adopted unsafe cryptographic practices to protect users' data.

Each violation does not necessarily mean that an attack is possible. The rule violations should be treated as warnings to be further investigated. Some violations can be false alarms because it is very hard to precisely discriminate in all situations. The researchers contacted more than 300 developers for confirmation, but only 10 provided useful feedback.

"Many developers do not consider attacks such as privilege escalation and side-channel attacks to be possible on phones, and so they store data locally without sufficient safeguards," notes Sethumadhavan.

The team also manually analyzed the code of 28 Android apps and found that some of the violations reported by CRYLOGGER could potentially be exploited. They see two significant applications of CRYLOGGER. Developers can use it to find cryptographic misuses in their apps as well as in the third-party libraries they use. App stores, such as the Google Play Store, can use CRYLOGGER to screen submitted apps to ensure they meet security standards and are safe for final users to download. Google already uses similar screening technologies to get rid of unsafe or scam apps and these could be extended to consider cryptographic misuses.

The researchers are working on improving the accuracy of CRYLOGGER by defining techniques that will further reduce the number of false alarms. They are also using CRYLOGGER to perform inter-app analysis so that it can analyze how apps exchange data and determine if sensitive data are kept secure. In addition, they are putting rule checking for cryptographic misuses into hardware, rather than software, to force applications to use safe practices in critical contexts.

"While we keep working to improve the accuracy of CRYLOGGER, our approach can be used by app stores to promote better security practices," Carloni adds. "And we believe that CRYLOGGER's technique of analyzing thousands of Android applications by running them and collecting information that can be later analyzed offline could also be used in other security domains."

The study is titled "CRYLOGGER: Detecting Crypto Misuses Dynamically."

More information: "CRYLOGGER: Detecting Crypto Misuses Dynamically." DOI: 10.1109/SP40001.2021.00010 , www.computer.org/csdl/proceedi … 3400a160/1mbmHwIxTb2

Provided by Columbia University School of Engineering and Applied Science