Three Papers Accepted at ACM CCS'17

Dr. Sascha Fahl and his team co-authored three papers accepted at ACM CCS 2017. The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM) and a premier venue for top-notch computer security research.

The papers have co-authors from Google's Chrome Security team and CISPA, Saarland University.

The first paper studies a sample of over 300 million HTTPS warning messages that Google Chrome users encountered in the course of normal browsing. After manually reviewing more than 2,000 error reports, the authors automated rules to classify the top causes of HTTPS error warnings. They were able to automatically diagnose the root causes of two-thirds of error reports. Surprisingly, they found that more than half of errors are caused by client-side (e.g. misconfigured clocks) or network issues (e.g. misconfigured desktop firewalls or anti-virus software) instead of server misconfigurations. Based on these findings, they implemented more actionable warnings and other browser changes to address client-side error causes. The changes are part of the newest Chrome release.

The second paper presents and studies an Android Studio plugin called FixDroid. FixDroid tries to help Android application developers to write more secure code. Frequently, Android developers fail to adhere to security best practices, leaving applications vulnerable to a multitude of attacks. FixDroid points out the advantage of a low-time-cost tool both to teach better secure coding and to improve app security in real-time. The authors show that professional and hobby app developers can work with and learn from an in-environment tool without it impacting their normal work; and by performing a study with students, they demonstrate that code delivered with such a tool by developers previously inexperienced in security contains significantly less security problems.

The last paper investigates root-causes for the presence of outdated and insecure third-party libraries in Android applications. First, the authors conduct a survey with 203 Android app developers from Google Play to retrieve first-hand information about their usage of libraries and requirements for more effective library updates. With a subsequent study of library providers' semantic versioning practices, they uncover that those providers are likely a contributing factor to the app developers' abstinence from library updates in order to avoid ostensible re-integration efforts and version incompatibilities. Further, they conducted a large-scale library updatability analysis of 3 million apps to show that, based on the library API usage, 85.6% of the libraries could be upgraded by at least one version without modifying application code, 48.2% even to the latest version. Particularly alarming are their findings that 95.4% out of 15,346 actively used library versions with a known security vulnerability could be easily fixed.

https://www.sigsac.org/ccs/CCS2017/