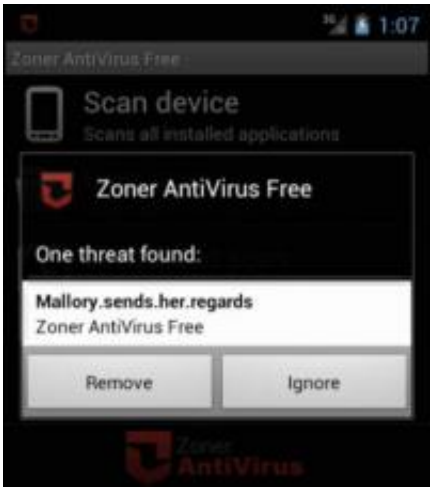
Android apps are full of potential leaks, finds study

October 22 2012, by Nancy Owano



Credit: Sascha Fahl, et al.

(Phys.org)—Many Android apps are capable of falling victim to Man in the Middle (MITM) attacks. How many? Far too many. Thousands of apps in the Google Play mobile market present vulnerabilities because of the way that protocols are implemented—namely, the Secure Sockets Layer (SSL) and Transport Layer Security (TLS). That Android apps are open to malware by now is a yawn-evoking statement if there ever was one, but a new paper provides findings that are making this week's headlines. Computer science researchers from Philipps University of Marburg and Leibniz University of Hannover in Germany showed that Android apps that are used by over 180 million people can expose banking, social networking and email information.

They identified 41 apps available on the Google Play mart that leak sensitive information in traveling between smartphones and servers. The researchers used a smartphone with Android 4.0 Ice Cream Sandwich in their investigations. They installed potentially vulnerable apps on the phone and set up a WiFi access point with a Man in the Middle (MITM) SSL proxy. They equipped the SSL proxy with a self-signed certificate or with one that was signed by a trusted CA, but for an unrelated host name. Of the 100 apps selected for manual audit, 41 apps proved to have exploitable vulnerabilities.

They captured credentials for numerous major services. "Furthermore, Facebook, email and cloud storage credentials and messages were leaked, access to IP cameras was gained and control channels for apps and remote servers could be subverted."

Their paper, testily called "Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security," discovered the apps that have SSL code that either accepts all certificates or all hostnames for a certificate and thus are potentially vulnerable to MITM attacks.

What also troubled the authors was the inability of many people in their survey to even recognize security threats attached to applications. "The results of our online survey with 754 participants showed that there is some confusion among Android users as to which security indicators are indicative of a secure connection, and about half of the participants could not judge the security state of a browser session correctly," they said.

Regarding secure connections, the researchers found that 47.5% of non-IT experts believed to be using a secure connection while the survey was served over HTTP. In addition, 34.7% of participants with prior IT education thought that they were using a secure channel when they were not. Only 58.9% of experts and 44.3% of non-experts correctly

identified that they were using a secure or insecure connection when prompted.

In summing up, the authors pointed to a need for more education and easier tools that can enable the secure development of Android apps. They also called attention to the need for research to identify which countermeasures can ensure the right mix of usability, security benefits and economic incentives for large-scale deployment.

Android by the numbers merits that kind of care. Android is the most used smartphone operating system in the world. Building on the contributions of the open-source Linux community and more than 300 hardware, software, and carrier partners, Android has become the fastest-growing mobile operating system. The numbers keep shifting, but Android's market share currently stays over 50 percent. Android users download more than 1.5 billion apps and games from Google Play each month, and the number is growing.

More information: Research paper: www2.dcsec.uni-hannover.de/fil … android/p50-fahl.pdf

Via Arstechnica