BGU security team says vulnerability found in Samsung Knox

December 26 2013, by Nancy Owano

(Phys.org) —Israeli researchers at Ben-Gurion University of the Negev (BGU) said a security flaw was discovered by a team member, a PhD student, and that this vulnerability could enable interception of data on Samsung mobile devices based on the Knox architecture. The discovery of the alleged security flaw was reported earlier this week in *The Wall Street Journal,*. Fundamentally, the BGU discovery report involves Samsung Knox, which the South Korean giant announced earlier this year as a secure platform solution in mobile architecture for BYOD business environments, providing security hardening from the hardware through to the application layer. Knox is a container solution for separating business and personal use of a mobile device, in step with the Samsung For Enterprise (SAFE) program, to promote the readiness of

Samsung devices for enterprise use.

An alleged vulnerability in the container design is what caught the security researchers' attention. The researchers said they believe the alleged breach "enables easy interception of data communications between the secure container and the external world including file transfers, emails and browser activity." The vulnerability was uncovered by Mordechai Guri, part of a research team at the Cyber Security Labs, discovered during an unrelated research task.

A BGU report posted Tuesday presented details of the findings: "The Knox architecture features a regular phone environment as well as a secure container that is supposed to add security protection to the phone. All data and communications that take place within the secure container are protected and even if a malicious application should attack the non-secure part all the protected data should be inaccessible under all circumstances. However, the newly found breach can be used to bypass all Knox security measures. By simply installing an 'innocent' app on the regular phone (in the non-secure container) all communications from the phone can be captured and exposed."

Guri said, "We are also contacting Samsung in order to provide them with the full technical details of the breach so it can be fixed immediately."

The university's Cyber Security Labs have been conducting research on mobile device security as well as network security for seven years.

Samsung, according to the WSJ report, said it was looking into the allegations, and takes all security vulnerability claims seriously. The WSJ report said that a Samsung spokesperson, however, noted that the BGU lab's breach of the system appeared to have been carried out on a device that was not fully loaded with the extra software that a corporate client

would use in conjunction with Knox.

More information: in.bgu.ac.il/en/Pages/news/samsung_breach.aspx