PHYS.ORG

New technique targets C code to spot, contain malware attacks

March 4 2014, by Matt Shipman

Researchers from North Carolina State University have developed a new tool to detect and contain malware that attempts root exploits in Android devices. The tool improves on previous techniques by targeting code written in the C programming language – which is often used to create root exploit malware, whereas the bulk of Android applications are written in Java.

Root exploits take over the system administration functions of an operating system, such as Android. A successful Android root exploit effectively gives hackers unfettered control of a user's smartphone.

The new security tool is called Practical Root Exploit Containment (PREC). It refines an existing technique called anomaly detection, which compares the behavior of a downloaded smartphone application (or app), such as Angry Birds, with a database of how the application should be expected to behave.

When deviations from normal behavior are detected, PREC analyzes them to determine if they are malware or harmless "false positives." If PREC determines that an app is attempting root exploit, it effectively contains the malicious code and prevents it from being executed.

"Anomaly detection isn't new, and it has a problematic history of reporting a lot of false positives," says Dr. Will Enck, an assistant professor of computer science at NC State and co-author of a paper on the work. "What sets our approach apart is that we are focusing solely on

C code, which is what most – if not all – Android root exploits are written in."

"Taking this approach has significantly driven down the number of false positives," says Dr. Helen Gu, an associate professor of computer science at NC State and co-author of the paper. "This reduces disturbances for users and makes anomaly detection more practical."

The researchers are hoping to work with app vendors, such as Google Play, to establish a database of normal app behavior.

Most app vendors screen their products for malware, but malware programmers have developed techniques for avoiding detection – hiding the malware until users have downloaded the app and run it on their smartphones.

The NC State research team wants to take advantage of established vendor screening efforts to create a database of each app's normal behavior. This could be done by having vendors incorporate PREC software into their app assessment processes. The software would take the app behavior data and create an external database, but would not otherwise affect the screening process.

"We have already implemented the PREC system and tested it on real Android devices," Gu says. "We are now looking for industry partners to deploy PREC, so that we can protect Android users from root exploits."

More information: The paper, "PREC: Practical Root Exploit Containment for Android Devices," will be presented at the Fourth ACM Conference on Data and Application Security and Privacy being held March 3-5 in San Antonio, Texas. Lead author of the paper is former NC State graduate student Tsung-Hsuan Ho. The paper was co-authored by Daniel Dean, a Ph.D. student in Gu's lab at NC State.

Abstract

Application markets such as the Google Play Store and the Apple App Store have become the de facto method of distributing software to mobile devices. While official markets dedicate significant resources to detecting malware, state-of-the-art malware detection can be easily circumvented using logic bombs or checks for an emulated environment. We present a Practical Root Exploit Containment (PREC) framework that protects users from such conditional malicious behavior. PREC can dynamically identify system calls from high-risk components (e.g., third-party native libraries) and execute those system calls within isolated threads. Hence, PREC can detect and stop root exploits with high accuracy while imposing low interference to benign applications. We have implemented PREC and evaluated our methodology on 140 most popular benign applications and 10 root exploit malicious applications. Our results show that PREC can successfully detect and stop all the tested malware while reducing the false alarm rates by more than one order of magnitude over traditional malware detection algorithms. PREC is light-weight, which makes it practical for runtime on-device root exploit detection and containment.

Provided by North Carolina State University

Citation: New technique targets C code to spot, contain malware attacks (2014, March 4) retrieved 24 April 2024 from https://phys.org/news/2014-03-technique-code-malware.html