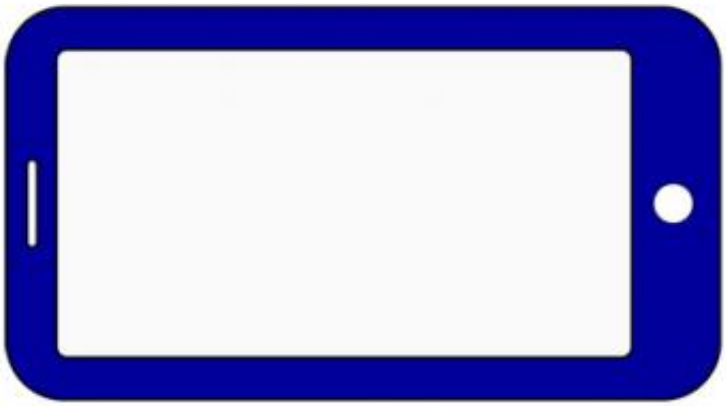
Many Android vulnerabilities can be traced to manufacturer modifications

November 5 2013, by Matt Shipman



(Phys.org) —Computer security researchers have found that Android smartphone manufacturers are inadvertently incorporating new vulnerabilities into their products when they customize the phones before sale, according to a recent study. On average, the researchers found that 60 percent of the vulnerabilities found in the smartphone models they evaluated were due to such "vendor customizations."

A paper describing the study is being presented Nov. 6 at the ACM Conference on Computer and Communications Security in Berlin, Germany.

Although Google creates the base Android platform that all Android smartphones use to operate, vendors – such as Samsung, Sony, and HTC – customize that platform to integrate their hardware. These vendors also incorporate applications they or their partners have developed.

A team led by NC State computer security researcher Xuxian Jiang sought to determine whether these customizations posed a security threat. Jiang is senior author of a paper describing the study.

The researchers looked at 10 representative Android smartphone models. They looked at an older model (version 2.x) and a newer model (version 4.x) from each of five manufacturers: Samsung, HTC, LG, Sony and Google. For those 10 models, vendor customizations were responsible for an average of 80 percent of the apps that came preloaded onto the phones.

"All 10 devices were vulnerable, based purely on the preloaded apps," Jiang says. "The older versions had an average of 22.4 vulnerabilities per device, while the newer versions had an average of 18.4 vulnerabilities per device. And the newer versions weren't always more secure. Some of the more recent models were actually less secure than their predecessors." Of the 10 models evaluated, the most recent Google device they looked at, the Nexus 4, had the fewest vulnerabilities.

Jiang's team discovered vulnerabilities including the ability to record audio without the user's permission, the ability to make phone calls without the user's permission, and the ability to wipe out the user's data.

"We also found that 85 percent of the preloaded apps were overprivileged," Jiang says. An app is considered "overprivileged" if it requires users to give it permissions that the app does not actually use. "Seeing this many overprivileged apps indicates that the programmers developing the vendors' apps are violating a well-known security

principle, i.e., the 'least privilege principle.'"

Lei Wu, a Ph.D. student at NC State, is lead author of the paper, "The Impact of Vendor Customizations on Android Security." Co-authors are NC State Ph.D. students Michael Grace, Yajin Zhou, and Chiachih Wu.

Provided by North Carolina State University