SU professor uncovers potential issues with apps built for Android systems

October 13 2011

Wenliang Du, professor of computer science in the L.C. Smith College of Engineering and Computer Science (LCS), has had his paper accepted to be presented at the 27th Annual Computer Security Applications Conference, on potential issues with mobile applications (commonly referred to as apps) written for the Android system using the WebView platform.

Currently, in the Android market, 86 percent of the top 20 most-downloaded apps in 10 diverse categories use WebView. With the goal of creating dynamic apps, WebView has enabled developers to embed browsers in their apps allowing users to have a more customized experience that provides opportunities to interact with social media, personal email and other app users. However, Du has discovered that the use of WebView opens app developers and users to potential risks.

There are two major issues addressed in his paper:

1. Which apps to trust. There are a limited number of web browsers on the Internet (i.e. Firefox, Explorer, Safari, etc.). As a result, users of these browsers can be reasonably assured that they are protected from malicious content. However, WebView allows developers to embed browsers in their apps, creating thousands of browser applications on mobile platforms and there is no way to determine which apps are trustworthy. Malicious app developers could create apps that steal or modify users'

information in their online accounts, such as Facebook.

2. Dealing with losing the protection of the sandbox. Internet browsers on computers have safeguards, known as the sandbox, that protect user information and prevent personal information from unknowingly being shared throughout the web. As apps have become more dynamic, those safeguards can often impede some of the desired functionality a developer wishes to create. As a result, app developers have slowly begun opening up holes in the protective sandbox to provide a better user experience, but as a result user information is no longer as secure.

"In industry, developers are usually carried away by the fancy features they create for their products; they often forget about or underestimate the security problems caused by those features," says Du. "This has happened many times in the history of computing. The design of WebView in Android is just another example of this."

Du has submitted a proposal to Google to explore whether there are ways to preserve the nice features of WebView and at the same time make it secure. He and his graduate students are also planning on exploring whether this issue may also affect other smartphone and tablet platforms.

A Ph.D. student, Tongbo Luo, who is currently working with Du on a National Science Foundation cybersecurity research grant, had the initial idea to explore weaknesses in the Android system. Luo had taken Du's courses in computer security and Internet security where students explored both how to identify weaknesses in operating systems and applications as well as how hackers might take advantage of these weaknesses.

Du is passionate about preparing his students to apply the right amount of skepticism to new product introductions. "The goal of both of my

security courses is for students to learn take a look at a system or new technology and ask themselves: 'Is this risky?'"

Provided by Syracuse University