'Open port' backdoors are widespread smartphone security hole

May 2 2017, by Nicole Casal Moore

Credit: University of Michigan

A sweeping study of an internet communication mechanism common in mobile devices has revealed that so-called 'open ports' are much more vulnerable to security breaches than previously thought.

The vulnerability the University of Michigan researchers highlighted is most pronounced in Android apps that let users share data across devices and connect to their phones from their computers. One app, called Wifi File Transfer, has been downloaded more than 10 million times.

Open port backdoors could be exploited to steal private information such as contacts, security credentials and photos; to remotely control a device; to perform a denial of service attack; or to inject malicious code that could jumpstart widespread, virus-like attacks, the researchers say.

How to protect yourself

They have some advice for Android users: Update AirDroid to the latest patched version (AirDroid is pre-installed on some devices). Don't use the default passcodes. Only launch vulnerable open port apps when you need them, and after using them, be sure to exit them fully through the task manager.

"When choosing an app whose functionality is data sharing across devices, proxy/VPN, or enabling the user to control a phone remotely—without physically accessing it—we recommend being extra careful. Consider using only those created by developers with good reputations," said Yunhan Jia, a doctoral student in computer science and engineering who is involved in the research.

The team identified 410 apps with dangerous insecurities, and 956 different individual ways those insecurities could be exploited. Beyond

these figures, they manually confirmed vulnerabilities in 57 applications, including popular file transfer mobile apps with 10-to-50 million downloads. Overall, the number of mobile devices at risk could turn out to be higher, as the researchers continue to investigate how open ports are used in mobile devices.

Open ports and their history

Open ports are integral pieces of internet infrastructure that allow computer programs to accept packets of information from remote servers. These communication mechanisms are routinely used in traditional computers, where they're secure in part because computers' Internet Protocol addresses don't change. An IP address identifies a connected device.

Smartphones also rely on open ports to receive certain types of information. But because of the way mobile networks are structured, phones' IP addresses can change as they move through the world. This and other factors relating to mobile architecture lead to these vulnerabilities, the researchers say.

The U-M team isn't the first to identify that open ports on mobile devices could be susceptible to hacking. But their systematic study has shown how widespread the problem is.

Open ports were implicated in the November 2015 "wormhole" vulnerability in a software development kit made by Baidu, a Chinese internet services company. The issue affected thousands of Android apps and at least 100 million devices. While the number of devices affected was high, the U-M researchers say this represents just one usage of open ports.

"Even though the security community has been aware of that specific

instance in which an open port served as a backdoor, it remained unclear how general the problem is—and what the fundamental causes are," said Z. Morley Mao, U-M professor of computer science and engineering and the Morris Wellman Faculty Development Professor.

"We are the first to show that this is actually a widespread problem for mobile apps using open ports. We systematically detected a large number of such threats in the wild."

How they did it

To arrive at their findings, they designed and implemented a tool called OPAnalyzer that can identify and characterize vulnerable open port usage in Android apps. They analyzed 24,000 popular mobiles apps.

The researchers found that more than half of the usage of open ports in the apps they studied is unprotected. While not all of those instances could be exploited to do harm, the researchers say their unprotected nature demonstrates a general lack of awareness of the problem.

The researchers also investigated the fundamental causes behind this general vulnerability, and they found that it is exposed by popular ways open ports are used in the smartphone ecosystem, rather than poor implementation of apps.

The researchers identified certain steps app developers can take to mitigate the vulnerability. More information can be found on their Mobile Open Port Security website.

The team has reported vulnerabilities to affected app developers. Their website includes videos of threat model demos, defense demos, and app manufacturer responses.

More information: Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications: eecs.umich.edu/eecs/about/arti … 2017/open_euro17.pdf

Provided by University of Michigan