Sandia builds Android-based network to study cyber disruptions

EurekAlert!

Sandia's David Fritz holds two Android smartphones, representing the virtual network of 300,000 such devices that he and other researchers are using to advance understanding of malicious computer networks on the Internet.

LIVERMORE, Calif. — As part of ongoing research to help prevent and mitigate disruptions to computer networks on the Internet, researchers at Sandia National Laboratories in California have turned their attention to smartphones and other hand-held computing devices.

Sandia cyber researchers linked together 300,000 virtual hand-held computing devices running the Android operating system so they can study large networks of smartphones and find ways to make them more reliable and secure. Android dominates the smartphone industry and runs on a range of computing gadgets.

The work is expected to result in a software tool that will allow others in the cyber research community to model similar environments and study the behaviors of smartphone networks. Ultimately, the tool will enable the computing industry to better protect hand-held devices from malicious intent.

The project builds on the success of earlier work in which Sandia focused on virtual Linux and Windows desktop systems.

"Smartphones are now ubiquitous and used as general-purpose computing devices

as much as desktop or laptop computers," said Sandia's David Fritz. "But even though they are easy targets, no one appears to be studying them at the scale we're attempting."

The Android project, dubbed MegaDroid, is expected to help researchers at Sandia and elsewhere who struggle to understand large scale networks. Soon, Sandia expects to complete a sophisticated demonstration of the MegaDroid project that could be presented to potential industry or government collaborators.

The virtual Android network at Sandia, said computer scientist John Floren, is carefully insulated from other networks at the Labs and the outside world, but can be built up into a realistic computing environment. That environment might include a full domain name service (DNS), an Internet relay chat (IRC) server, a web server and multiple subnets.

A key element of the Android project, Floren said, is a "spoof" Global Positioning System (GPS). He and his colleagues created simulated GPS data of a smartphone user in an urban environment, an important experiment since smartphones and such key features as Bluetooth and Wi-Fi capabilities are highly location-dependent and thus could easily be controlled and manipulated by rogue actors.

The researchers then fed that data into the GPS input of an Android virtual machine. Software on the virtual machine treats the location data as indistinguishable from real GPS data, which offers researchers a much richer and more accurate emulation environment from which to analyze and study what hackers can do to smartphone networks, Floren said.

This latest development by Sandia cyber researchers represents a significant steppingstone for those hoping to understand and limit the damage from network disruptions due to glitches in software or protocols, natural disasters, acts of terrorism, or other causes. These disruptions can cause significant economic and other losses for individual consumers, companies and governments.

"You can't defend against something you don't understand," Floren said. The larger the scale the better, he said, since more computer nodes offer more data for researchers to observe and study.

The research builds upon the Megatux project that started in 2009, in which Sandia scientists ran a million virtual Linux machines, and on a later project that focused on the Windows operating system, called MegaWin. Sandia researchers created those virtual networks at large scale using real Linux and Windows instances in virtual machines.

The main challenge in studying Android-based machines, the researchers say, is the sheer complexity of the software. Google, which developed the Android operating system, wrote some 14 million lines of code into the software, and the system runs on top of a Linux kernel, which more than doubles the amount of code.

"It's possible for something to go wrong on the scale of a big wireless network

because of a coding mistake in an operating system or an application, and it's very hard to diagnose and fix," said Fritz. "You can't possibly read through 15 million lines of code and understand every possible interaction between all these devices and the network."

Much of Sandia's work on virtual computing environments will soon be available for other cyber researchers via open source. Floren and Fritz believe Sandia should continue to work on tools that industry leaders and developers can use to better diagnose and fix problems in computer networks.

"Tools are only useful if they're used," said Fritz.

MegaDroid primarily will be useful as a tool to ferret out problems that would manifest themselves when large numbers of smartphones interact, said Keith Vanderveen, manager of Sandia's Scalable and Secure Systems Research department.

"You could also extend the technology to other platforms besides Android," said Vanderveen. "Apple's iOS, for instance, could take advantage of our body of knowledge and the toolkit we're developing." He said Sandia also plans to use MegaDroid to explore issues of data protection and data leakage, which he said concern government agencies such as the departments of Defense and Homeland Security.

Original release:
http://www.eurekalert.org/pub_releases/2012-10/dnl-sba092712.php [1]

Source URL (retrieved on *12/20/2014 - 2:27pm*):
http://www.ecnmag.com/news/2012/10/sandia-builds-android-based-network-study-cyber-disruptions?qt-recent_content=0

Links:
[1] http://www.eurekalert.org/pub_releases/2012-10/dnl-sba092712.php