PHYS.ORG

Cell network security holes revealed, with an app to test your carrier

May 21 2012

Popular firewall technology designed to boost security on cellular networks can backfire, unwittingly revealing data that could help a hacker break into Facebook and Twitter accounts, a new study from the University of Michigan shows.

The researchers also developed an Android app that tells phone users when they're on a vulnerable network. They will present their work May 22 at the IEEE Symposium on Security and Privacy in San Francisco.

Using Android smartphones, computer science associate professor Z. Morley Mao and doctoral student Zhiyun Qian revealed how an attacker could hijack a TCP Internet connection by taking advantage of publicly available information on smartphones; users' willingness to download untrusted apps; and network firewall middleboxes, which block data bundles that don't appear to be part of the flow of information traffic.

The researchers detected these middleboxes on 32 percent of the nearly 150 networks they tested worldwide.

"Firewall middleboxes are supposed to protect against this kind of attack, but it turns out they do the opposite," Qian said. "Most vendors and carriers that deploy such firewall middleboxes still believe they are safe and we want them to be aware of this design flaw."

Middleboxes monitor the "sequence numbers" of data packets on their way to mobile devices. When you snap and share a photo with a friend, for example, it gets chopped into numerous packets before it's sent across the network. Your friend's smartphone looks to the sequence numbers to put the picture back together. Middleboxes could help hackers use the process of elimination to home in on a number in the right range.

"An attacker can try to guess at sequence numbers. It's usually hard to get feedback on whether a guessed number is correct, but the firewall middlebox makes this possible," Qian said. "The attacker can try a range of sequence numbers. The firewall will only allow one through if it is in the valid range."

In their test, the researchers used a binary search process that can rule out half of the possible numbers at a time. In 32 rounds, which take just seconds to complete, this process guarantees that they'll arrive at a valid number and get a packet through.

How does the attacker know he has succeeded? That's where the Android spyware comes in (smartphone malware is already very popular, the researchers say, and it wouldn't be hard for an attacker to add this capability into an existing program). The intelligence the spyware needs is not privileged information. It doesn't need special administrator or root access. It would just read a couple of the phone's publicly available incoming packet counters and let the attacker know when the counters advanced.

Armed with a valid sequence number, the hacker could spoof Facebook or Twitter's HTTP (as opposed to the more secure HTTPS) web login page and gain the user's passwords.

The attack Qian and Mao propose illustrates a susceptibility in the so-called sandboxing safety mechanism that smartphone platforms utilize. Sandboxing isolates an app to a certain piece of memory, with the intention of protecting the rest of the phone from any tampering.

"What's surprising here is that this shows how malware can, in a sense, reach out of its sandbox and tamper with other legitimate apps such as your browser," Qian said.

More information: Qian's app, Firewall Middlebox Detection, is available free of charge at play.google.com/store/apps/det … .umich.eecs.firewall

The paper is called "Off-Path TCP Sequence Number Inference Attack, How Firewall Middleboxes Reduce Security."

Project website: web.eecs.umich.edu/~zhiyunq/tc … ce_number_inference/

Provided by University of Michigan

Citation: Cell network security holes revealed, with an app to test your carrier (2012, May 21) retrieved 26 April 2024 from https://phys.org/news/2012-05-cell-network-holes-revealed-app.html