Researchers Demonstrate Android 'Cloak And Dagger' Attacks

Security researchers have detailed a new class of attacks affecting Android devices, which they say make use of "design shortcomings" to carry out a variety of attacks, including silently stealing security credentials.

In tests, researchers found they could carry out the "Cloak and Dagger" attacks to steal a user's test Facebook credentials without the user suspecting anything was wrong.

Design flaws

In their paper, Chenxiong Qian, Simon P. and Chung, Wenke Lee of Georgia Tech and Yanick Fratantonio of UC Santa Barbara demonstrated that the SYSTEM_ALERT_WINDOW ("draw on top") Android permission, which allows an app to draw overlays on top of any other app, could be misused to carry out a clickjacking attack.

That could be used to cause a user to unknowingly activate another, more powerful permission called BIND_ACCESSIBILITY_SERVICE ("a11y"), which is intended to aid users with disabilities and can notify an app of any event that affects the device.

The researchers demonstrated that design flaws with the two permissions meant they could be abused by a malicious application to effectively take over a device by tricking the user into installing a “God-mode” app with all permissions enabled.

They found that in tests with 20 subjects, which involved asking the user to interact with the proof-of-concept app and then log into Facebook with a set of test credentials, none of the subjects suspected anything was wrong.

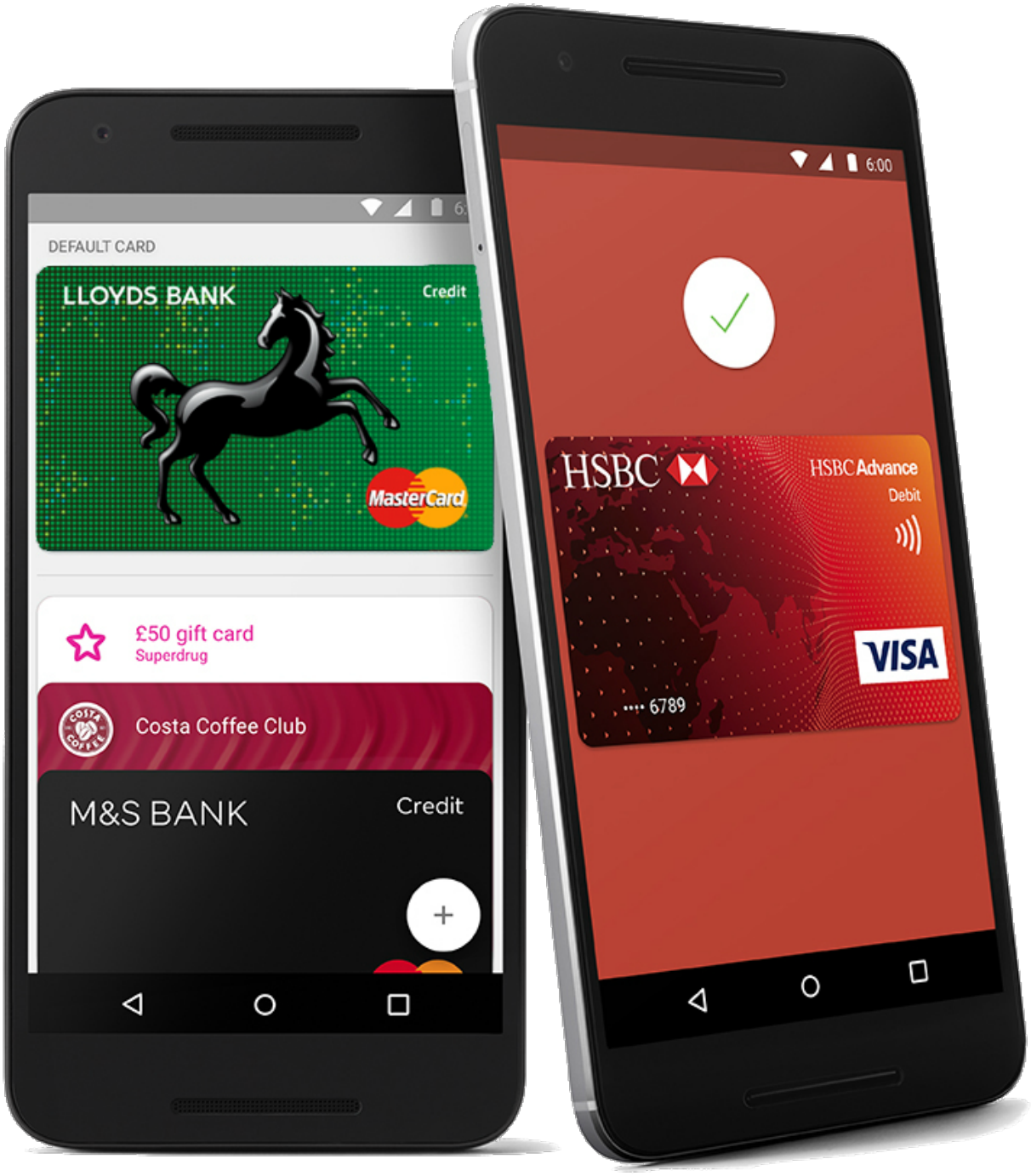
Invisible attack

“The results of our study are worrisome: even if the malicious app actually performed clickjacking to lure the user to enable the BIND_ACCESSIBILITY_SERVICE permission, silently installed a God-mode app with all permissions enabled, and stole the user’s Facebook (test) credentials, none of the 20 human subjects even suspected they have been attacked,” they wrote. “Even more worrisome is that none of the subjects were able to identify anything unusual even when we told them the app they interacted with was malicious and their devices had been compromised.”

Google said it was aware of the issues and had updated the Google Play Protect security service to prevent the installation of such apps, as well as building new protections into the upcoming version of Android, code-named “O”, to further protect from the problems identified.

“We’ve been in close touch with the researchers and, as always, we appreciate their efforts to help

keep our users safer," the company stated.



Security firms have warned, however, that such protections don't necessarily reach Android users, many of whom rarely or never receive software updates.

‘Judy’ malware campagin

Users can’t rely on the security of Google Play, either, since malware is regularly discovered on Google’s official app store, with Check Point last week disclosing what it called “possibly the largest malware campaign” found on the store to date.

The campaign, called “Judy”, was developed by a South Korean company and has affected up to 36.5 million users, Check Point said.

The malware code is designed to generate fraudulent web advert clicks for its developers and was found in 41 apps developed by the company, with 4.5 to 18.5 million downloads.

Some of the apps involved had been on Google Play for several years without being detected, and many received positive reviews from users, Check Point said.

“Judy” got around Google Play’s security by deploying a seemingly benign bridgehead app on the store, which retrieves a malicious payload from a remote server after installation.

“Users cannot rely on the official app stores for their safety, and should implement advanced security protections capable of detecting and blocking zero-day mobile malware,” Check Point wrote in an advisory.