Researchers found a security flaw that had 10 million banking app users at risk

6 December 2017

Credit: CC0 Public Domain

Researchers from the University of Birmingham have developed a tool to perform semi-automated security testing of mobile phone apps. After running the tool on a sample of 400 security critical apps, they were able to identify a critical vulnerability in banking apps; including apps from HSBC, NatWest, Co-op and Bank of America Health.

This vulnerability allowed an attacker, who is connected to the same network as the victim (e.g., public WiFi or corporate), to perform a so called "Man in the Middle Attack" and retrieve the user's credentials such as username and password/pin code.

The researchers found that the banks had put a lot of effort into the security of their apps, however one particular technology used - so called "certificate pinning" - which normally improves security, had meant that standard tests failed to detect a serious vulnerability that could let attackers take control of a victim's online banking.

The tests found that apps from some of the largest banks in the world contain this flaw, which if exploited, could have enabled an attacker to decrypt, view and modify network traffic from users of the app. An attacker with this capability could thereby perform any operation which is normally possible on the app.

Other attacks were also found, including "in app phishing attacks" against Santander and Allied Irish bank. These attacks would have let an attacker take over part of the screen while the app is running and use this to phish for the victim's login credentials.

The researchers worked with the banks involved, and the UK government's National Cyber Security Centre to fix all the vulnerabilities, and the current versions of all the apps affected by this pinning vulnerability are now secure.

The researchers recommend that all users of banking apps ensure that they are always using the most recent version of the app, and that they always install upgrades as soon as they are offered.

The research was carried out by Dr Tom Chothia, Dr Flavio Garcia and PhD candidate Chris McMahon Stone, who are all members of the Security and Privacy Group at the University of Birmingham

Dr Tom Chothia said, "In general the security of the apps we examined was very good, the vulnerabilities we found were hard to detect, and we could only find so many weaknesses due to the new tool we developed" he added "It's impossible to tell if these vulnerabilities were exploited but if they were attackers could have got access to the banking app of anyone connected to a compromised network".

Dr Flavio Garcia said, "Certificate Pinning is a good technique to improve the security of a connection,

but in this case, it made it difficult for penetration testers to identify the more serious issue of having no proper hostname verification"

Chris McMahon Stone said, "As this flaw is generally difficult to detect from normal analysis techniques, we have developed a detection tool that is semi-automated and easy to operate. This will help developers and penetration testers ensure their apps are secure against this attack."

Some initial results were given in the paper "A Security Analysis of TLS in Leading UK Banking Apps" presented at the Conference on Financial Cryptography and Data Security, in January, and full results will be given in the paper "Spinner: Semi-Automatic Detection of Pinning without Hostname Verification" which will be presented Wednesday at the 33rd Annual Computer Security Applications Conference in Orlando.

More information: Chris McMahon Stone et al, Spinner, *Proceedings of the 33rd Annual Computer Security Applications Conference on - ACSAC 2017* (2017). DOI: 10.1145/3134600.3134628

Provided by University of Birmingham