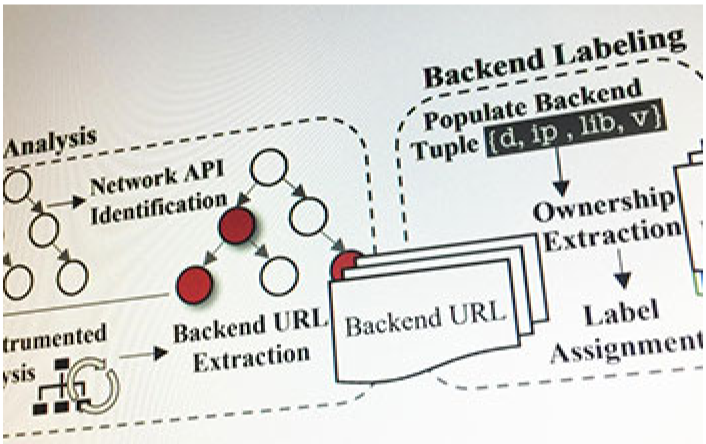
National Science Foundation
WHERE DISCOVERIES BEGIN

Research News

Smartphone apps may connect to vulnerable backend cloud servers

Most users likely unaware of vulnerabilities in smartphone apps



A portion of the process used by SkyWalker to vet backend systems that support mobile apps.

Credit and Larger Version (/discoveries/disc_images.jsp?cntn_id=299054&org=NSF)

August 15, 2019

Cybersecurity researchers have discovered vulnerabilities in the backend systems that feed content and advertising to smartphone applications, potentially exposing users' personal information.

In results reported at this week's USENIX Security Symposium, researchers from the Georgia Institute of Technology (/cgi-bin/good-bye?https://www.eurekalert.org/pub_releases/2019-08/giot-sam081119.php) and The Ohio State University identified more than 1,600 vulnerabilities in the support ecosystem behind the top 5,000 free apps available in the Google Play Store. The vulnerabilities, affecting multiple app categories, could allow hackers to break into databases that include personal information -- and perhaps into users' mobile devices.

To help developers improve the security of their mobile apps, the researchers have created an automated system called SkyWalker to vet cloud servers and software library systems. SkyWalker can examine the security of the servers supporting mobile applications, which are often operated by cloud hosting services rather than individual app developers.

"A lot of people might be surprised to learn that their phone apps are communicating with not just one, but likely tens or even hundreds of servers in the cloud," said Brendan Saltaformaggio of Georgia Tech's School of Electrical and Computer Engineering. "Users don't know they are communicating with these servers because only the apps interact with them and they do so in the background. Until now, that has been a blind spot where nobody was looking for vulnerabilities."

The researchers discovered 983 instances of known vulnerabilities. They are still investigating whether attackers could get into individual mobile devices connected to vulnerable servers.

"Security should not be an afterthought, it should be considered as a first-class citizen when designing systems – this is something we have advocated through the CNS Core Program <https://nsf.gov/funding/pgm_summ.jsp?pims_id=505671> ," says Samee Khan, a program director in NSF's Directorate for Computer and Information Science and Engineering <https://www.nsf.gov/awardsearch/showAward?AWD_ID=1834216&HistoricalAwards=false> , which funded the research.

-- NSF Public Affairs, (703) 292-7090 media@nsf.gov (mailto:media@nsf.gov)