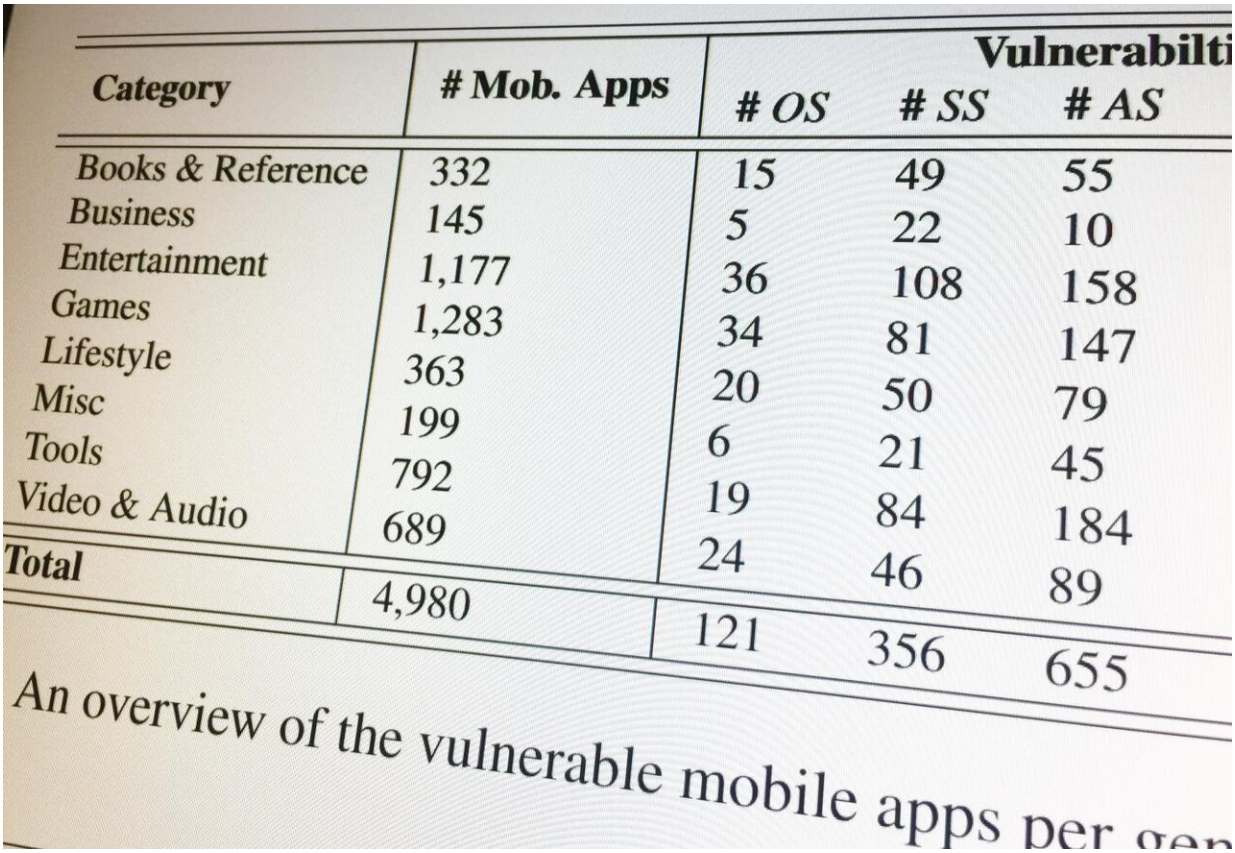
Smartphone apps may connect to vulnerable backend cloud servers

August 12 2019



Category	# Mob. Apps	Vulnerabilti		
		# OS	# SS	# AS
Books & Reference	332	15	49	55
Business	145	5	22	10
Entertainment	1,177	36	108	158
Games	1,283	34	81	147
Lifestyle	363	20	50	79
Misc	199	6	21	45
Tools	792	19	84	184
Video & Audio	689	24	46	89
Total	4,980	121	356	655

An overview of the vulnerable mobile apps per gen

A portion of the chart created to provide an overview of vulnerable mobile apps by genre. Credit: Georgia Tech

Cybersecurity researchers have discovered vulnerabilities in the backend systems that feed content and advertising to smartphone applications

through a network of cloud-based servers that most users probably don't even know exists.

In research to be reported August 15 at the 2019 USENIX Security Symposium, researchers from the Georgia Institute of Technology 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 the 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, an assistant professor in 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 Air Force Office of Scientific Research and the National Science Foundation supported the research.

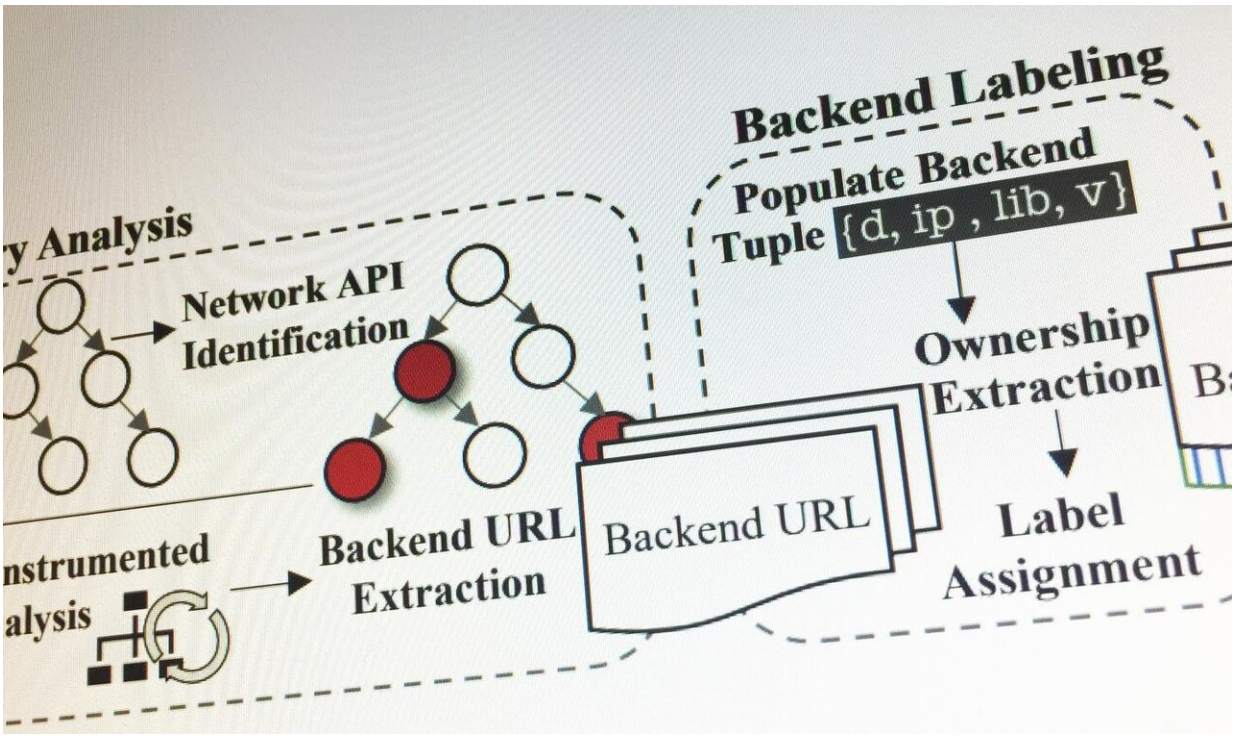
In their study, the researchers discovered 983 instances of known vulnerabilities and another 655 instances of zero-day vulnerabilities spanning across the software layers—operating systems, software

services, communications modules and web apps—of the cloud-based systems supporting the apps. The researchers are still investigating whether attackers could get into individual mobile devices connected to vulnerable servers.

"These vulnerabilities affect the servers that are in the cloud, and once an attacker gets on the server, there are many ways they can attack," Saltaformaggio said. "It's a whole new question whether or not they can jump from the server to a user's device, but our preliminary research on that is very concerning."

The researchers identified three types of attack that could be made on the backend servers: SQL injection, XML external entity and cross-site scripting, explained Omar Alrawi, a Georgia Tech graduate research assistant and co-first author with Chaoshun Zuo at Ohio State. By taking control of these machines in the cloud, attackers could gain access to personal data, delete or alter information or even redirect financial transactions to deposit funds in their own accounts.

To study the system, Alrawi and Zuo ran applications in a controlled environment on a mobile device that connected to backend servers. They then watched the communications between the device and servers, and repeated the process for all of the applications studied.



A portion of the four-phase process used by SkyWalker to vet backend systems used to support mobile apps. Credit: Georgia Tech

"We found that a lot of applications don't encrypt the communications between the mobile app and the cloud service, so an attacker that is between the two points or on the same network as the mobile could get information about the user—their location and user name—and potentially execute password resets," Alrawi said.

The vulnerabilities were not easy to spot. "You have to understand the context through which the app communicates with the cloud server," he said. "These are very deep bugs that cannot be identified by simply scanning and using traditional tools that are used for web application security."

The operators of vulnerable systems were notified of the findings. Concerns about who is responsible for securing those backend servers is one of the issues to come out of the study.

"It's actually a significant problem because of how many different software developers may have their hands in building these cloud servers," Saltaformaggio said. "It's not always clear who is responsible for doing the patching and who is responsible for the vulnerabilities. It's tough to track down these vulnerabilities, but it's also tough to get them patched."

To save app developers from having to do the security research they did, the researchers are offering SkyWalker, an analysis pipeline to study mobile backends.

"SkyWalker will watch how the application communicates with those cloud servers, and then it will try to communicate with the servers to find vulnerabilities," said Alrawi. "This information can give an app developer a heads-up about potential problems before they make their application public."

The researchers studied only applications in the Google Play Store. But applications designed for iOS may share the same backend systems.

"These servers provide backend services for mobile apps that any device could use," Alrawi said. "These cloud services are essential components of modern mobile apps. They are part of the always-connected world."

For the future, the researchers hope to study how the vulnerabilities could affect smartphone users, and to check on whether the problems they identified have been addressed.

"We are going to keep doing these sorts of studies and will revisit them

later to see how the attack landscape has improved," said Saltaformaggio. "We will keep looking for more blind spots that need to be studied. In the new world of smartphones and mobile applications, there are unique problems that need to be rooted out."

More information: Developers will be able to submit their apps to SkyWalker at (https://mobilebackend.vet) and get a report on what it finds.

Provided by Georgia Institute of Technology