CERTIFIABLE —

Dozens of popular iOS apps vulnerable to intercept of TLS-protected data

76 apps in Apple’s App Store still don’t use best practices to protect user data.

SEAN GALLAGHER - 2/6/2017, 3:38 PM

25

While developing a tool for evaluating mobile application security, researchers at Sudo Security Group Inc. found out something unexpected. Seventy-six popular applications in Apple's iOS App Store, they discovered, had implemented encrypted communications with their back-end services in such a way that user information could be intercepted by a man-in-the-middle attack. The applications could be fooled by a forged certificate sent back by a proxy, allowing their Transport Layer Security to be unencrypted and examined as it is passed over the Internet.

The discovery was initially the result of bulk analysis done by Sudo's verify.ly, a service that performs bulk static analysis of application binaries from Apple's App Store. Will Strafach, president of Sudo, verified the applications discovered by the system were vulnerable in the lab, using a network proxy configured with its own Secure Socket Layer certificate.

In the post about his findings being published today, Strafach wrote:

> During the testing process, I was able to confirm 76 popular iOS applications allow a silent man-in-the-middle attack to be performed on connections which should be protected by TLS (HTTPS), allowing interception and/or manipulation of data in motion. According to Apptopia estimates, there has been a combined total of more than **18,000,000 (Eighteen Million) downloads** of app versions which are confirmed to be affected by this vulnerability.

Ars independently verified that several applications discovered by Strafach were vulnerable. These sorts of vulnerabilities are nothing new; thousands of applications have had incorporated bugs that caused TLS to become vulnerable to attack, both on iOS and Android. But the fact that they persist even as Apple tries to push developers toward greater security is disconcerting, to say the least—especially in applications that could expose financial or health data along with user credentials.

FURTHER READING
Android apps *still* suffer game-over HTTPS defects 7 months later

The data exposed by the vulnerability in each of the applications varied in sensitivity. For just less than half—33 of the applications—the risk was relatively low, as most of the data was "partially sensitive analytics data," Strafach said. These apps included a number of third-party "uploader" apps for Snapchat (which exposed Snapchat usernames and passwords) and the Vice News app, among others.

In 24 cases, the exposed data included login credentials or session tokens that would allow an attacker to hijack the account associated with the application, though those accounts were not tied to highly sensitive data. However, the remaining 19 applications left sensitive data exposed to attack. In these cases, Strafach "confirmed ability to intercept financial or medical service login credentials and/or session authentication tokens for logged in users."

The names of these apps are not currently being published. "Currently, this list is only available to limited parties due to sensitivity," Strafach wrote. "I have been in touch with MITRE and will follow up later with a listing of the CVE IDs for affected iOS applications of which data interception would be considered medium risk or high risk."

The same old story

Until recently, many mobile applications didn't protect much of the data sent to their back-end interfaces. When we looked at passive monitoring of mobile applications in 2014, we discovered many applications that were passing session tokens and other sensitive data in the clear. And for some developers that have moved to secure connections, poor verification of TLS certificates has continued to be problem.

Even security-focused applications have run into trouble with TLS validation, including the two-factor authentication provider Duo. In 2015, Duo issued a security advisory warning that one version of their iOS application had left open a TLS vulnerability. Many secure applications avoid the issue by using "pinned" certificates hard-coded into applications, which allows them to avoid interception of the certificate hand-shake at the beginning of a TLS session. But that may not be practical for other applications.

FURTHER READING
Critical HTTPS bug may open 25,000 iOS apps to eavesdropping attacks

Apple has been pushing iOS developers to use App Transport Security (ATS) to secure data transmitted by applications sold through the App Store. In December, Apple extended the deadline for application developers to implement ATS. ATS uses TLS v. 1.2 and requires stronger cryptography (AES and SHA-2), as well as "forward secrecy" to protect past transactions if a certificate is compromised. But ATS doesn't ensure that applications properly verify the certificate—just that the developer uses TLS to begin with.

ATS does allow for use of Certificate Transparency—a public "log" of verified certificates. Google is also pushing the service and is planning to use Certificate Transparency to enforce validation of trusted web sites by October 2017. But not all certificate authorities (let alone site and app operators) have signed off on implementing CT, so its adoption by app developer is still in its infancy. And if Apple tries to enforce Certificate Transparency now, it could actually cause some applications to become less secure, Strafach said. Developers "would not be able to utilize certificate pinning for their connections, and they could not trust otherwise untrusted certificates which may be required for intranet connections within an enterprise using an in-house PKI."

The one ray of sunshine for end-users is that man-in-the-middle attacks (other than those by state actors) are possible only when connected to the Internet via an untrusted Wi-Fi connection. If you're connected using cellular broadband or a trusted wireless network, man-in-the-middle attacks are highly unlikely—though attackers can use Wi-Fi network spoofing to fool a device into connecting to a malicious network, as Ars has demonstrated in the lab in the past.

SEAN GALLAGHER
Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean.gallagher@arstechnica.com // **TWITTER** @thepacketrat

READER COMMENTS 25

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

1,500 iOS apps have HTTPS-crippling bug. Is one of them on your device?

Heartbleed vulnerability may have been exploited months before patch [Updated]

HTTPS-crippling FREAK exploit affects thousands of Android and iOS apps

Today on Ars

Dealmaster: Get a Dell Inspiron 15 with a Core i7 CPU for just $549

Your office equipment can reveal the identity of your special someone

World of Warcraft gold can now be used to buy other Blizzard items

Jawbone may stop making consumer wearables and instead make medical devices

A black hole has been devouring a star for a decade

Three decades after Challenger, a soccer ball finally reaches space

Google Brain super-resolution image tech makes “zoom, enhance!” real

Kangaroo care—why keeping baby close is better for everyone

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS