TechTarget | SearchMobile Computing

E-guide

PRO+ Content

iOS vs. Android: Compare the Mobile OSes

In this e-guide

In this e-guide:

Apple and Google have long been rivals. The competition continues between Android and iOS and both mobile operating systems are security contenders. With cyberattacks becoming more prevalent and advanced, new security capabilities from these OSes are more significant than ever. In this e-guide compare the two mobile OSes and the security features of each.

In this e-guide

Android vs. iOS security: Compare the two mobile OSes

Kevin Beaver,

http://searchmobilecomputing.techtarget.com/tip/Android-vs-iOS-security-Compare-the-two-mobile-OSes

Apple and Google have a rivalry for the ages, not unlike Windows vs. Linux, and the competition continues with Android vs. iOS security. The top two mobile operating systems are both security contenders.

In a world where it's hard enough to convince executives, even CIOs, about the importance of security, the average mobile user may not be all that concerned. However, if IT is looking to deploy corporate-issued devices or support multiple mobile platforms via a BYOD policy, both Android and iOS mobile security features are worth knowing.

Check out these OS security highlights, which can affect IT and information security programs, as Android and iOS step into the ring.

In this corner: Android

Google pushes out Android security patches every month. Only Nexus and Pixel users get the update immediately, and other manufacturers might delay or skip the update all together. Having owned a Nexus phone as well as others from Samsung and LG (both locked and unlocked), I can say that

In this e-guide

it's really nice getting the monthly updates for stock Android directly from Google. Having to wait on third-party manufacturers and the layered complexity/bureaucracy of the carriers on top, I have found it pretty rare to get any consistent security updates on the Android platform.

Google has a built-in "guard" against apps that users install manually if Google deems them to be unsafe. There can be false positives, though, and there's no way for users to know for sure. There are also numerous ways to lock or unlock an Android phone such as pattern, voice and facial recognition.

Starting with Android Marshmallow, boot verification has become a standard feature that checks for anything wrong with the operating system. It will give errors if the user is running a custom ROM on the device or if someone has rooted it.

To increase security, users are required to enter app permissions upon app launch, if the app is updated. Older apps will not ask for permissions, but users can manually disable this feature in the settings -- a step that further boosts mobile security and privacy. After all, who wants to share their calendar and address book with random app developers if they don't want to?

Encryption is also standard, starting with the Nexus 6. It initially made the devices slower, but Google has since fixed any lagging issues.

In this e-guide

In this corner: iOS

Apple's most well-known security feature is its App Store, where any app passing through must not only meet Apple's security requirements, but also pass the tests. This security has been shown to be at risk with hot patching, or remote software updating, but Apple's new policy may keep things under control.

Apple device users have control over many different security features, including encryption, which they can enable in the device settings. Apple introduced device encryption starting with iOS 8 in 2014. Users can disable features such as Siri on the lock screen to prevent anyone trying to send messages without the device being unlocked. Like Android, iOS also lets users disable permissions for certain apps in the settings.

The latest iOS has upped its user passcode requirements. Now, the default PIN length is six characters rather than four, which provides for better security than previous versions of iOS. In addition, the fingerprint reader grants users direct access into apps in lieu of having to enter a password every time.

Android vs. iOS security

A common question that arises with both iOS and Android is whether or not users need to run antivirus software. Given the architectures and default configurations of these operating systems, running antivirus software is

likely unnecessary, although such controls certainly wouldn't hurt if maximum security is the ultimate goal.

So, when it comes to Android vs. iOS security, which OS is the winner? It's up to IT shops to decide; only they know exactly what the organization requires in terms of mobile security features. The latest versions of Android and iOS are both pretty solid; the question is whether users have the latest version and, if not, when they'll be able to get it.

There are a lot of moving parts with mobile, whether it's outdated app vulnerabilities or numerous source code and runtime flaws that can equally affect both iOS and Android. IT shops might have additional mobile device management controls in place to ensure that they're locked down. Then again, they may not. The important thing is to understand the organization's mobile security gaps and do due diligence to minimize any identified risks moving forward.

Test your mobile device security know-how

Do you know what it takes to provide mobile security? Take this quiz that covers differences in mobile OSes, containerization, data encryption and more

Next article

In this e-guide

A look at the official iOS and Android security reports

Jack Madden, Analyst and blogger

http://www.brianmadden.com/opinion/A-look-at-the-official-iOS-and-Android-security-reports

Recently I've been spending a lot of time talking to people about mobile threat detection it's getting a higher profile in the EMM space, largely because of increasing enterprise mobile maturity.

As part of the conversation around mobile threat detection (or for any EMM conversation), one of the informative things anyone can do is read Apple's iOS Security Guide and Google's Annual Android Security Year in Review, both of which were updated recently. Of course, Apple and Google being the way that they are, the focus of each report is a bit different.

Apple iOS Security

The Apple iOS Security Guide doesn't discuss the rate of any types of security incidents or malware, rather it's a close look at all the security mechanisms that are in place. This includes: device and OS integrity assurance; the update model; how Touch ID works; encryption; app security; services like Apple ID, iMessage/FaceTime, iCloud Keychain, and Apple Pay;

privacy controls; and of special interest to the enterprise, device controls and MDM.

For actual incidents, we'll have to look at the security content of iOS updates as well as third-party metrics, but in the meantime the Apple iOS Security Guide is still quite educational.

Google Android Security

Android, being the broad and diverse ecosystem that it is... well, let's just say it's the one that's more likely to be associated with security concernts, so Google's report takes a different approach.

It does a pretty deep dive into PHAs (potentially harmful applications) and MUwS (mobile unwanted software), revealing their definitions, methodology for finding them, the tools they use, the types they see, and the broader ecosystem trends. The headline statistic is this:

- *By Q4 2016, fewer than 0.71% of devices had Potentially Harmful Applications (PHAs) installed and for devices that exclusively download apps from Google Play, that number was even smaller at 0.05%.* (p. 4)

An important part of Android security is Verify Apps, which essentially acts as Google's own anti-malware service. Available on any device that uses Google Play (which is probably almost all devices in the enterprise, save for some fringe BYOD devices or specialized embedded devices), it can prevent

users from installing PHAs or prompt them to remove ones already on their device.

A triumph of 2016 was the spread of regular Android security patches. Both users and enterprises can easily look up a given device's patch level, and there's more good news:

- *In the United States, over 78% of active flagship Android devices on the four major mobile network operators reported a security patch level from the last three months.* (p. 31)
- *In Europe over 73% of active flagship Android devices on the major mobile network operators reported a security patch level from the last three months.* (p. 32)

The report doesn't spend too much time on the Android OS security model for that you'll have to head to source.android.com/security. It does highlight the improvements in Android 7.0, which according to the developer dashboard, along with 7.1 accounts, for 4.9% of Android devices right now:

- There are improvements to how encryption is implemented, and encryption rates are around 80% in Android 7.x, versus around 20% for 6.0 and 10% for 5.1 and earlier (the report didn't give exact values). (p. 24)
- Among all devices, 48.9% have some type of lock screen enabled. (p. 17)

There's also a discussion of device rooting:

- *Google's SafetyNet security service provides a feature called Attestation that can check for signs of rooting.* [...] *Worldwide 94.4% of all Android devices report passing the basic system integrity check, from which we conclude that these devices are not rooted. The remainder includes devices that were rooted by the user, sold as a rooted device, were unintentionally rooted by a PHA, or that do not match expected characteristics of an intact security model. Verify Apps tracks the ratio of all app installs to user-intended rooting. In 2016, user-intended rooting installs comprise 0.3461% of all installs, with fewer than 0.0001% of installs coming from Google Play. Apps that root devices without disclosure to and permission from the user are significantly more rare. In 2016, malicious rooting apps accounted for 0.00233% of all installs. Most devices are either rooted by the user or the manufacturer.* (p. 40)

Final thoughts

Clearly, we can say that the conventional wisdom is true: Keeping your devices patched (which is actually possible for a lot more devices now) and sticking to the official app stores can go a long way.

As I mentioned, the mobile threat detection space (i.e. third-party security products other than mobile device management, mobile app management, and built in device security features) is going through some interesting changes right now. For a bit more on what this space is about, you can read this overview that I wrote for TechTarget's Access Magazine. Keep an eye out for more throughout the next two months, and if you've installed it at

In this e-guide

your company or are considering it now, I'd love to chat informally (and of course confidentially many customers still aren't very public about their mobile threat detection experiences).

Next article

In this e-guide

Get up to speed on iOS 10 security

Kelly Stewart, Assistant Site Editor

http://searchmobilecomputing.techtarget.com/feature/Get-up-to-speed-on-iOS-10-security

As Apple's iPhone and iPad capabilities continue to grow and develop, so does iOS security.

Online and mobile threats have also developed and grown quickly. With iOS 10 came new features that pose risks themselves, as well as iOS security measures that can combat other risks. It is imperative to double-check current privacy settings as well as know what to manage in order to best protect user data.

What are the biggest iOS 10 security features?

With iOS 10, the passcode options expanded to include alphanumeric, meaning any combination of numbers and letters. This is in addition to the Touch ID biometric authentication method for iPhones generation 5s and newer. Another one of the new iOS 10 security features is auto-lock, which users can now set for as quickly as 30 seconds. If an iPhone is unlocked but set down, this feature will automatically lock the device within the amount selected.

Not only does iOS 10 give more options regarding when location services can be shared with an app, but it also creates a list of applications requesting to access certain data. This allows IT to better manage and control the sharing of data. In addition, the Advertising button under privacy settings gives the choice to limit ad tracking, so that an individual's search data is more guarded.

How does iOS 10 approach user privacy?

The biggest privacy update with iOS 10 is differential privacy. This new way of coding personal data is as complex as its name suggests. Apple is able to collect, analyze and encrypt personal data from an iPhone without specifically connecting that collected data to a specific user. For instance, with predictive texting in messaging, the system will analyze what words and emojis a user most commonly uses, but it does not identify the user. For the Spotlight search, users will see suggestions of frequently used items of the keyword within a search, but it stores the analyzed data locally, protecting the individual's privacy.

With the introduction of differential privacy comes benefits and risks, however. The benefits are higher protection on data and better aggregated information to make devices more customized to individual use. But for Apple to get this type of insight, it must collect much more data than it previously did. The more data that is gathered, the more vulnerable the data is to interception.

In this e-guide

What are security risks with iOS 10?

With employee mobility comes the risk of personal and professional data being attacked and exposed. It is vital for businesses to expand their mobile protection strategy, as iOS 10 security is not always enough. In September 2016, a huge hole in iOS password-verification threatened the whole operating system, allowing a firm to gain access to password-protected local backups faster than on previous versions. Apple solved the problem by altering the algorithm in follow-up security updates 10.1 and 10.2; however, these types of attacks are a major concern in terms of iOS security strength.

Apple has introduced more and more iOS management and security features for IT. Do you know how to use them? Take this quiz to find out.

How can IT keep iOS device security top notch?

IT must enforce company-wide mobile device management and employee best practices to best protect against threats. IT should also encourage employees to never connect to public or insecure Wi-Fi, turn on Touch ID and two-factor authentication for devices and iCloud, and not allow employees to jailbreak iOS devices.

IT should also ensure that users keep their devices up to date with the latest OS and apps, require a complex six-digit passcode and enable remote wipe.

In this e-guide

Just by going from a four-digit to six-digit passcode, the number of possible combinations increases from 10,000 to 1 million.

Next article

In this e-guide

Users are biggest impediment to Apple iOS security

Ramin Edmond, News Writer

http://searchmobilecomputing.techtarget.com/news/450423643/Users-are-biggest-impediment-to-Apple-iOS-security

Apple's iOS has the trust of enterprise IT, but users can still pose a security threat.

No software is completely secure, but iOS has a strong reputation because Apple regularly updates the operating system and strictly vets apps that developers submit to the App Store. Still, the behavior-based security risks that threaten every operating system -- such as when people click suspicious links in emails or don't set device passcodes -- should have IT's attention. As a result, the most important Apple iOS security measure organizations should take is to educate their users.

"You can make all the security advancements you want in hardware and software, but if a user just gives their password away, that's all for naught," said Erik Lightbody, assistant director of technical services at Saint Michael's College in Colchester, Vt. "Your security precautions go out the window just by someone clicking a link."

A strength of Apple iOS is its users update the OS more frequently than those of other mobile OSes, which allows users to have the latest security features and patches. Nearly 80% of iOS devices were updated to the

newest version, iOS 10, in February, while 16% still needed to upgrade from iOS 9, according to Statista. In comparison, just 6.6% of Android users updated to the latest version of the OS, Android 7, in May, while 31.2% were still on Android 6, and 23.3% were still on version 5.1, according to Statista.

While iOS users are typically more up to date than Android users, there are still many mistakes users make that can affect Apple iOS security.

Phishing attacks

The most common Apple iOS security issue that IT experts see today is the threat of phishing attacks, which send deceptive links to websites that install malware or trick users into giving up their personal information. To avoid these, IT can whitelist or blacklist websites or install software that detects suspicious sites before users visit them. The most effective way to address phishing, however, is to make users aware of the threat and how to identify suspicious links.

"Educating people is more effective than any security software you can purchase," Lightbody said. "If people know what they're doing, they won't do things they shouldn't be doing."

In this e-guide

Lack of passcodes

Another behavior that threatens Apple iOS security is users turning off passcode protection on their devices. Without a passcode, if a device is lost or stolen, any data on it is readily accessible.

"Training and education is hugely important," said Eric Klein, director of mobile software at VDC Research Group Inc. in Natick, Mass. "Organizations need to communicate with users and employees and go over issues on a regular basis to be proactive about security."

Saint Michael's College had problems with students and faculty not putting passcodes on their devices, for instance. But the school recently switched to Microsoft Exchange, which by default requires all mobile devices that access the server to have a passcode.

It's a good policy because it's safe to assume users have sensitive data in their email, Lightbody said.

Organizations can also adopt enterprise mobility management tools to enforce the use of passcodes and remotely wipe devices in the event they are lost or stolen.

In this e-guide

Malicious apps

A less common but still serious issue is the threat of compromised apps in Apple's App Store.

"One of the biggest things iOS has going for it is the rigidity in the App Store," Lightbody said. "Apple signs off on everything. It's a lot harder to get malicious malware on there."

This doesn't mean that every app is safe. There have been highly publicized security problems deriving from malware in the App Store, such as the XcodeGhost attack in 2015 that infected 4,000 apps.

"Anyone who tells you they're 100% secure because they have an Apple device is living in la la land," said Jack Gold, founder and principal analyst of J. Gold Associates, a mobile analyst firm in Northborough, Mass.

Downloading a malicious app from the App Store isn't the user's fault, but there are some steps they can take to recognize suspicious apps. Because Apple containerizes all apps on iOS, these apps can't communicate with each other unless the user grants permission. If a single-purpose app, such as a flashlight app, asks for access to contacts or location services, the user should recognize that as an odd request.

Users should also be aware of alerts from Apple or their IT departments warning of malicious apps. When Saint Michael's College discovers a security issue with an iOS app, IT alerts users by email and social media.

In this e-guide

Next article

In this e-guide

Google plays a strong hand with new Android security features

Alyssa Provazza, Senior Managing Editor

http://searchmobilecomputing.techtarget.com/blog/Modern-Mobility/Google-plays-a-strong-hand-with-new-Android-security-features

Google announced Android security features that continue to heighten the company's enterprise mobility game.

Enterprise security features from the big mobile operating systems, Google Android and Apple iOS, have been a hot topic for years. Now, with BlackBerry down for the count and cyberattacks becoming more advanced, new security capabilities from these OSes are more significant than ever.

Due to fragmentation and issues with malware, experts often saw Google's OS as sub-par compared to Apple's when it came to enterprise security. Not so much anymore. Android 7.0 Nougat added support for seamless updates, allowing the OS and apps to be patched in the background making users less likely to avoid installing important security updates. The company in December even dropped the Android for Work brand name, given that most Android devices now ship with the enterprise security features built in.

In this e-guide

All work and all Play

Google took further security steps at its I/O developer conference last week, with Play Protect and new features in the upcoming Android O.

Google Play Protect will be built into devices that have the Google Play store. The service continuously scans all apps on the device for vulnerabilities or other issues, and through machine learning, gathers information over time that allows it to intelligently find threats. Play Protect can also let users know if an app is dangerous and prevent them from downloading it or remove it from their device. The Verify Apps service did this previously, but the new service steps up the machine learning element and makes the scans more visible in the Play Protect app.

For employees, Google Play Protect [...] allows them to work confidently and productively without worrying about harmful apps, said Travis McCoy, senior product manager at Google, in a blog post. And using our Android enterprise management features, IT managers can enforce this protection by policy.

Also in Android O, the code name for the next OS version, is improved IT control over file-based encryption, greater controls over Wi-Fi and Bluetooth restrictions, additional management capabilities around work profiles, and more. In a stand against ransomware, the OS will now close off permissions that previously would allow an attacker to take control of an infected device. Plus, developers can now build the ability for pop-up notifications to time out, or disappear after a certain amount of time on screen, providing more security for sensitive information that may appear.

In this e-guide

Android O is now in public beta, so users, developers and IT admins will have plenty of chance to check out those and other new enterprise security features to see how Google is keeping up.

Next article

In this e-guide

Android is getting a key new enterprise provisioning tool

Jack Madden, Analyst and blogger

http://www.brianmadden.com/opinion/Android-is-getting-a-key-new-enterprise-provisioning-tool

Today, Google is announcing that Android enterprise, the mobile device management feature set formerly known as Android for Work, is getting a new zero-touch enrollment process for enterprise-owned devices.

When a company buys a device, it can be flagged so that when it turns on and is connected for the very first time, it will automatically enroll itself in MDM, as well as configure settings and provision apps. This means that you can hand new devices directly to users, and you don't have to worry about the device ever being used in an unmanaged state. This is the the out of box experience.

Devices in this program will almost certainly get enrolled into what's known as Device Owner Mode, which gives the associated MDM server extensive controls that you would want for a corporate device. Previously, enrolling in Device Owner Mode required a few more steps, like entering settings manually or scanning a QR code. (These will still be an option, of course.) You can dig into more Android enterprise details in their help page and the Android EMM Developers site.

In this e-guide

Support for this type of enrollment process is a key feature, as it has a big potential for time savings, as well as important security implications. We learned this from the Los Angeles Unified School District when they deployed thousands of iPads back in 2013 with, well, mixed success.

Android enterprise zero-touch enrollment is similar to what Samsung provides with Knox Mobile Enrollment, as well as Apple's Device Enrollment Program and Windows AutoPilot. Apple DEP is already quite popular, and Knox Mobile Enrollment is becoming common, too.

By adding zero-touch, Google will be joining this trend and taking another step in making it easier for OEMs to have standard EMM features. It also means that enterprises can use the same process with devices from multiple OEMs.

Not every carrier and Android device will support zero-touch enrollment, but since we're talking enterprise-owned devices, that's okay. Companies aren't worried about supporting anything that comes in the door, rather, they'll look for support in the specific devices they choose for their fleet. There's a full list of OEM, carrier, and EMM partners at the Android enterprise site, and it looks pretty broad.

Overall, vendors across the spectrum have been making a lot of progress on enterprise-owned device management features, and Google's announcement today will certainly open up even more new use cases.