The Economist Intelligence Unit

A report from the Economist Intelligence Unit

The personalisation challenge

Business culture and mobile security

The mobile security patch problem

Sponsored by

The mobile security patch problem

Most smartphones are not receiving available security fixes, and the risk of malware infections and data loss are mounting for businesses and consumers.

Both Apple and Google regularly update their mobile software to close security gaps that are discovered. But while Apple regularly pushes out iOS software updates to its devices, many Android devices never get Google's "patches", leaving them vulnerable to attacks and putting the corporate networks they connect to at risk.

Apple's patching task is easier because it controls both the operating system and the hardware. The company regularly pushes software updates to iPhones and iPads, and most users are quick to install them, says Dan Guido, chief executive of Trail of Bits, a US information security company. "Within about seven days, 50% of all iOS users in the wild across the world have applied [a new] patch," he says. "It's a very quick turnaround."

Most Android phones, on the other hand, are manufactured by an original equipment manufacturer (OEM) and loaded with a customised version of Android. Conflicting priorities among handset manufacturers, software makers and wireless carriers combine to create an ecosystem in which regular software updates for most Android smartphones are complicated and rare. While Google usually creates a patch in one day, more than 200 days pass before half of all Androids have that patch installed, according to Lookout, a US mobile security software firm.

"There are a lot of interests that are fighting here," says Mr Guido. "You have carriers and OEMs that both have to support their own software and their own devices on their network, and then you have the actual [software] vendors like Google and Apple that are pushing out patches very quickly."

Google says that OEMs and carriers are beginning to more proactively update devices—at least the more popular smartphones. "If you look at the major devices now, many are running Android version 4.2 or 4.3, so they are within a couple of months to being up to date," says Adrian Ludwig, Google's lead Android security engineer. (Version 4.3 is the most current version of the OS.) "It's increasingly common that a carrier will review the security updates and put pressure on the OEM to push out the patches."

Most Android devices do not run a pure version of the operating system created by Google, however. Handset manufacturers and wireless carriers tweak the OS for each device, sometimes to support specific hardware and apps or to disable functionality—or simply to add the carrier's logo to the phone's splash screen. Accordingly, each version of Android effectively becomes a customised operating system, one that cannot be updated with a universal patch. Instead, each patch requires testing and approval from the wireless carrier, which may have other priorities.

"Carriers don't care about their customers' security—what they really care about is getting you to sign a two-year contract," argues Christopher Soghoian, principal technologist for the American Civil Liberties Union (ACLU), a nonprofit advocacy group that has filed a complaint with the US Federal Trade Commission (FTC) against US wireless carriers. "Wireless carriers have only a certain amount of engineering resources, and they prefer to use engineering to focus on the next new phones."

"Carriers don't care about their customers' security—what they really care about is getting you to sign a two-year contract."

Christopher Soghoian, principal technologist for the American Civil Liberties Union (ACLU)

Consequently, Android updates are a long time coming. According to a study by technology news site Ars Technica, Android users routinely wait up to 15 months after launch of an Android phone before they receive the first software patch.

Mr Ludwig counters that even if Android phones are not updated, Google provides defensive mechanisms to protect devices. All Android smartphones, for instance, have a built-in service called Verify Apps that will warn users who try to install apps with malicious content, whether from Google Play or another source. "The warnings have about an 80% effective rate," he says. "The vast majority of users have never encountered any type of harmful application."

For those in the market for new Android smartphones, security experts recommend the Nexus, manufactured and serviced by Google, which can frequently and seamlessly push updates to users.

Not every Nexus is created equal, however. Mr Soghoian says Nexus phones sold by Verizon and Sprint are modified by the carriers and, as a result, cannot receive automatic updates from Google. He recommends that businesses and consumers opt for the Nexus-branded phones from AT&T and T-Mobile.

Mobile malware is still relatively rare, but attacks are growing rapidly and **99%** target the Android operating system.

Too much opportunity for hackers, too little recourse for device owners

The dominance of the Android platform and the slow delivery of security updates offer ample opportunity for hackers. Of smartphones shipped worldwide in the second quarter of 2013, 79% were Android devices, according to the US research firm International Data Corporation (IDC). Mobile malware is still relatively rare, but attacks are growing rapidly and 99% target the Android operating system, according to Kaspersky Lab, a Russian security software maker.

The growing risk for personal users centres on the security and privacy of sensitive personal information—think contact lists, e-mails and photos. For businesses, the stakes are much higher. "Malicious applications that get installed onto your phones are able to take it over very easily," Mr Guido says. Intruders "can read any kind of sensitive application data or sensitive business data that's on those devices."

Employees could also unknowingly connect Android devices infected with sophisticated malware to the corporate network, thus allowing hackers to burrow in and extract sensitive business data from the network itself.

These risks make many security executives reluctant to support Android, says Mr Guido. They "are pushing iOS as the lesser of two evils." A security director at a financial services firm recently told him that "users want Android so we have to find some way to support it regardless. We are between a rock and hard place."

Other than selecting a Google-serviced Android phone, IT managers and consumers alike lack compelling options. They cannot, for instance, download and install Android updates directly from Google.

"You're really at the mercy of the vendor or the OEM or the carrier here," Mr Guido says. "It's very important to make your concerns known so that this situation can change in the future."

The ACLU is trying to force change with its FTC complaint. The watchdog group asked the commission to investigate AT&T, Verizon, Sprint and T-Mobile for engaging in "unfair and deceptive business practices" by failing to warn customers about known, unpatched security flaws in products they sell. The complaint, filed in April 2013, claims that the carriers are aware of security vulnerabilities for which fixes exist, but typically have not taken action to update the software.

"The industry has failed to regulate itself," says Mr Soghoian, who submitted the complaint on behalf of the ACLU. "There is a clear issue here that isn't getting fixed."

The ACLU argues that carriers should allow consumers to return for full refund or exchange any carrier-supplied Android smartphone that is less than two years old and has not received "prompt, regular security updates."

That seems unlikely; Mr Soghoian says he has not received an indication of what action, if any, the FTC might take. But he says that the complaint has already met one key goal: shining a spotlight on the Android security-patch problem. ■

London
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

New York
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

Hong Kong
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

Geneva
Boulevard des
Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com

Cover: Shutterstock