New Smartphones and the Risk Picture

Mobile phone platforms are susceptible to malicious attacks, both from the network and upon physical compromise. Understanding the vectors of such attacks, level of expertise required to carry them out, available mitigations, and impact of compromise provides a background for certain risk decisions. In general, comparing risks introduced by the new generation of mobile devices to those of traditional, widely-deployed desktop systems provides insight into how the risks to DoD networks are changing. Due to the larger cultural and technological shift to mobile devices, this may be more relevant than comparison of different smartphone brands.

Attack Vectors

User-initiated installation of malicious software is strongly addressed by the new mobile phone platforms. The ability for enterprises to confine software installation to trusted software repositories ("app stores") addresses the software provenance problem by providing strong technical mechanisms that restrict the sources of software. Such mechanisms were never available on desktop operating systems, which instead relied heavily on adherence to policy to control software installation. Through the use of cryptography and built-in, OS-enforced restrictions on software sources, the mobile platforms can ensure software deployment occurs in a way that is more accountable and more efficient than general-purpose desktops. The level of expertise necessary to deploy a malicious app onto a public app store remains low, because some app stores perform no vetting and others – as with any software analysis – must make a speed versus accuracy tradeoff. However, targeting individuals with malicious apps can be effectively mitigated by only allowing access to trusted app repositories.

Smartphones use a separate "baseband" processor to carry out communications with the cellular network, with which they are constantly connected. Attacks which take advantage of bugs in the firmware executed by this processor have been publicized over the previous year. Some of these require an attacker to spoof a cell tower, which is now inexpensive and supported by open source software such as OpenBTS; others can be launched via globally remote communication such as text message. This attack vector is obviously absent from wired systems, and the ability to monitor or disrupt such attacks is also diminished when compared to wired networks with established points of ingress/egress. The baseband (and WiFi) firmware, as with other software on the device, can be patched regularly to address these bugs as they are discovered. The level of technical skill and motivation required for such attacks remains high, but has been decreasing due to public attention. Further into the future, however, such vulnerabilities could be expected to diminish due to the stable nature of the functionality provided by such software.

Lost or stolen mobile devices can place DoD data at risk of exposure. Policy compliant DoD laptops, as well as the established DoD smartphone platform, include capabilities that can credibly be described as full disk encryption and which are extremely difficult to defeat. The newer generation of smartphones do not yet include such comprehensive capabilities in COTS form. Nevertheless, they do support encryption of enterprise data on the device, if the user opts to store such data in certain areas. The level of technical skill required to access data stored outside such protected areas on the device is low. However, data-at-rest protection is considered a fundamental platform feature, and vendors continue to advance in this area by making such features more comprehensive. It also remains important to note that encryption or "secure containers" are not a countermeasure against either remote attacks (such as some "jailbreaks" or "roots"). Also note that encryption is not generally intended to protect against attacks that involve re-use of a device after a loss of physical control.

Malicious email or web-based attacks, called "spear phishing" when tailored for particular targets, remain the most likely front door to DoD networks for globally remote attackers. To combat this threat, most modern smartphone platforms include features (such as process sandboxing, Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and verified boot) which make it more difficult for attackers to successfully exploit vulnerabilities. Only the very latest desktop operating systems and web browsers contain many of these anti exploitation features. Although such attacks against smartphones remain possible, their resistance to attacks compares favorably to the typical DoD desktop. Adversaries targeting DoD networks can attack substantial numbers of outdated and nearly unsupported desktop operating systems such as Windows XP, and obsolete and insecure browsers such as Internet Explorer 6. Mobile devices, on the other hand, compare more closely to modern desktop operating systems such as Windows 7, and security-hardened browsers such as Internet Explorer 9 or Google Chrome.

The level of technical skill required to exploit systems via malicious email or web page varies considerably, from very low to very high. The level of difficulty corresponds directly to the age of the operating system, whether desktop or mobile. Judgments about a particular mobile device's resistance to such attacks are further complicated by researchers' interest in making very sophisticated attacks publicly available. Such sophisticated techniques are not even necessary on older desktops.

Impact of Compromise

An attacker who has fully compromised a device which remains in use (whether a smartphone or a PC) can effectively impersonate the user of that device. This includes access to all data and network resources available to the user. This is because a sophisticated attacker can elevate privileges to that of the device's operating system, and carry out any activity from the device that the user would (and without the user knowing). This includes making use of any credentials stored directly on the device, or those which are accessible from it. Storing credentials on hardware tokens provides a mitigation, as the attacker is then required to connect to the compromised device in order to make use of these credentials. This requires an attacker to expend more effort and engage in more-visible network activities. Any credentials stored directly on the device's main storage, however, can be collected by an attacker during the initial compromise and then used to impersonate the user and access resources from another location at the attacker's leisure.

As malicious email or web pages can be used by an adversary to make a successful initial intrusion into either a smartphone or desktop, little stands in the way of an attacker making further use of such techniques to compromise other systems (and gather privileged credentials) once inside an enclave. This can be enabled by using contacts listed in the address book of the user's device. For outdated desktop systems which are most vulnerable to this kind of attack, it is notable that applying the limited configuration guidance available for browsers, email clients, or PDF readers is a very weak mitigation when compared to updating to newer software.

Although modern smartphones are more resistant to fully remote compromise when compared to outdated desktop systems, their array of hardware features provides an attacker with much greater capabilities for information gathering and remote communications. This includes a microphone for listening to conversations, GPS for location tracking, cameras for visual surveillance, and cellular or WiFi radio for non-enterprise controlled or monitored network communications. Such capabilities may be of little consequence on a compromised device that belongs to a rank and file soldier or civilian, but may betray significant sensitive information from a senior leader.

Effective detection of compromise remains a high priority, and this is dependent on platform vendor cooperation. On some platforms, detection is currently hindered by security features themselves. App sandboxing, for example, limits the capabilities of any security-enhancing software that is not provided by the platform vendor as part of the device's operating system. Even mobile devices with a "trusted" or "secure" boot process – a valuable feature – often prevent independent access of the device's main storage area for verification purposes. Should vendors choose to provide it, low level hardware support for integrity checking could address this problem. Such a design permits confidence that a compromised operating system is not providing false integrity information.

Conclusion

The new generation of smartphones is more resistant to some types of cyber attacks that have proven extremely damaging to DoD, such as spearphishing and user-installed malicious software. At the same time, their use involves acceptance of other risks such as attacks via the cellular network, and a greater likelihood of data loss due to lost or stolen devices. Overall, vast numbers of obsolete desktops are likely to continue to be attackers' front door to DoD networks, although smartphones do permit highly motivated adversaries to carry out highly-targeted attacks against senior leaders. NSA continues to partner with industry to develop technological enhancements that prevent and detect such attacks.

Table 1. Attack Categories Against Mobile Devices

Attack Vector	Impact	Sophistication/Level of Effort Required	Mitigation
Malicious App	Total compromise of device	Low - but difficult to target	Enterprise-controlled App Store
Cellular Network	Varies; up to total compromise of device	High - but falling	Applying software patches
Physical Access: Lost/Stolen Device	Loss of data stored outside encrypted storage areas	Low - but increasing	Store data only inside apps or partitions that provide encryption
Physical Access: Reuse After Loss of Control	Total compromise of device	High	User training
Malicious Email/Web Page	Total compromise of device	Medium to High - depends on device	Applying software patches

A Product of the
Network Components
and Applications Division

The Mitigations Group
9800 Savage Rd.
Ft. Meade, MD 20755-6704
410-854-6632 DSN: 244-6632