How to secure a smartphone for the tweeter-in-chief

January 25 2017, by Anupam Joshi

As President Donald Trump takes office, he has also taken up a new, digital symbol of the presidency. Before, during and since the campaign, he used an Android smartphone to conduct his business and tweet prolifically, directly reaching millions of followers. But when he was inaugurated, Trump surrendered that device and accepted in its place a smartphone that has somehow been made more secure.

It is a key move for a man who might now be not only the 45th commander-in-chief but also America's first president with such devotion to Twitter. Many private companies deal with issues like this, in which employees joining the ranks already have a mobile phone they use for their personal life. Should that device be connected to company systems? Or should workers be issued a cumbersome second phone for work-only purposes? There are federal recommendations about that, but few firms are handling data as sensitive as the president's phone might be.

A presidential smartphone is probably the most attractive target imaginable for foreign governments' hackers. Attacking the phone could provide access to the highest secrets of national security, and near-constant real-time information about exactly where the president is, raising the potential for physical threats. Securing a phone like that requires several layers of protection.

Exactly what has been done to protect the president's phone is intentionally left unclear to the public. But as a scholar of mobile

security, I know that beyond overall network security measures, there are several technological approaches to securing a smartphone for special use. The most secure, however, is also among the least practical and least likely: ensuring the phone cannot connect to the internet at all. So how might have government cybersecurity specialists locked down Trump's new phone?

Hiding key information

One level of protection is what is called "security by obscurity." Many people presumably had Trump's pre-presidential phone number. Now, relatively few people will have his new number. Similarly, his old phone's internal device identifiers, such as its unique 15-digit International Mobile Equipment Identity number, or IMEI, may not have been as carefully guarded as those for his new phone. Keeping that information secret means the first hurdle for potential attackers involves figuring out which phone to attack in the first place.

Another layer of security involves ensuring the device was made by a trusted manufacturer, using trusted components, reducing the risk that the hardware would have any vulnerabilities that an attacker could exploit. Similarly, anyone who worked with or handled the phone at any step would have to be prevented from tampering with it to introduce any weaknesses.

Adding even more security in the physical device itself would be a specialized computer chip to add significant encryption capability for data stored on the phone or transmitted to or from it. Called a "Trusted Platform Module," this hardware element is required by the Defense Department in all new devices handling military information. In addition, it could be used to ensure that any attempts to tamper with the phone, its settings or the operating system installed would be identified immediately.

Custom configuration

The phone also might be configured to connect only with certain predetermined phone and data networks that are regularly screened against intrusions. Limiting its contact with the internet would, of course, be key – though that would also significantly limit the phone's usefulness to a president whose routine involves constant connection.

To handle that middle ground – finding a compromise between a full, unrestricted internet connection and a completely disconnected device – Trump's phone likely has some degree of customization. This could include a custom operating system, such as the Android variants the Department of Defense has developed. These would contain security features not typically found in commercial systems, such as special restrictions on logging in and unlocking the phone, as well as specialized encryption settings.

A more limited app store

The apps allowed on the president's phone should be few and limited only to those verified in advance. There should be little, if any, ability to automatically download and install apps, which could carry with them security-breaching code. For similar reasons, automatic updates to apps or the operating system might be restricted.

What happens inside a phone's processor and memory when it's running an app is already fairly secure even on commercial smartphones. Parts of the memory storing data and other parts handling the software instructions for working with those data are typically separated and identified. For smartphones such as those used by the president, this memory tagging should be done in hardware. This can prevent a number of different types of attacks that try to trick the device into running

software code from areas of memory set aside to handle data.

Also important is determining which data an app can use. Most operating systems allow users to make that decision. To improve security even more, the phone could be programmed with mandatory limits provided by, say, the secret service. To some degree, this ability is present on many smartphones, preventing users or attackers from corrupting key elements of the system.

But it could be stepped up – even enforcing that a particular file could be shared only with people or apps holding a certain level of security clearance, and having the system prevent sharing it elsewhere. For example, even if the president inadvertently told the Twitter app (if it's installed on his phone) to share a piece of classified information, the phone's software could step in and prevent that from happening.

Additional steps

Separately encrypting the memory spaces used by each app can boost security further. That would ensure that even if a malicious app makes its way onto the phone, it cannot see what other apps are doing, nor read the data they are working with.

Academic researchers have developed other ways that could be incorporated into a more secure presidential smartphone. The concept of "data tagging" can ensure that data that have been accessed by a certain app are accessed only in restricted ways. For example, the phone could be instructed that information that has passed through the White House's secure wireless networks should not be accessible to the Twitter app.

Additionally, context-dependent settings could monitor the phone's location and take note of surrounding devices. Perhaps the phone's microphone and camera could be shut off, and any active Twitter link

disconnected, if the phone itself is in the Oval Office, and whenever the president is meeting with members of his national security team.

How exactly the president's phone is protected is vitally important to our national security. Trump's agreement to stop using his previous, commercial-grade phone in favor of a government-secured one is a good step toward keeping the president informed and engaged while he and the nation also stay safe.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How to secure a smartphone for the tweeter-in-chief (2017, January 25) retrieved 25 April 2024 from https://phys.org/news/2017-01-smartphone-tweeter-in-chief.html