Ten years ago, the Operating System workhorses for US Government IT networks were Windows for unclassified And Solaris for classified traffic. There were sprinklings of Novell (due to its unique messaging system) and Mac OSx But there was no way a Systems Administrator was going to be allowed to put Linux on any government operational network.

However work was ongoing within one of the groups belonging to the keepers of the cryptographic gateway to Utilize the versatility of the Linux operating system to create an acceptable and capable version of Linux. The National Security Agency presented the scalable Security Enhanced Linux, which did not initially catch on with the Academics (due to its heavy reliance on compartmentalization) but it has evolved and withstood the test of time for The security administrators.

Government Mobile Problem (Background)

The governments mobile platform has been RIM's BlackBerry. This past decade they have provided a stable environment with security measures to prevent outsiders from easily tapping into communications; however; RIM couldn't do much because they don't have direct access to the encrypted network their customers use. However, it has since come to Light that while Blackberry may encrypt their network the first layer of encryption happens to use the same key every-where meaning that should it be broken once (by a government or authorities) it can be broken for any Blackberry. This has limited the Blackberry's clearance level. This is the reason the android devices (with the new kernel) can be secured at a higher clearance level than Blackberry devices. They have Many characteristics that allow them to be groomed like SELinux.

Since the White House Communications Office decided to move the executive branch from Blackberry Devices to Android-based phones, the boys at NSA have now teamed up with Google, NIS and members of The academic community to certify the android. The Department of Defense has decided that Once the AndroidKernel is sufficiently hardened and certified by the agencies required, each member (from General to Private) will Soon be issued an android phone as part of the standard equipment.

The androids sandboxed Java environment has similarities with what has already been created with SELinux. Each individual having the same system will make it simpler to manage and track. The ability to remotely locate And zero the systems will also eliminate the debacles that have resulted in the past two decades of lost Laptops By everyone from FBI Agents to VA officials.

Google Security Benefit

Google will benefit from the security research relationship they now have with NSA, NIST and the subject Matter experts working on this project from academia because the net is a virtual battlefield and the Agency Has been fighting this battle for many years. As a work in progress, the Linux based OS of the Android will also integrate mandatory access controls to enforce the separation of information based on Confidentiality and integrity requirements.

This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables The confinement of damage (and compromise) that can be caused by malicious or flawed applications. Using the System's type enforcement and role-based access control abstractions, it is possible to configure the android to Meet a wide range of security needs which will be passed on to commercial users.

Locating a flawed application or process is the first step in trying to exploit it. Once you've found a flaw, the Next step is to try to exploit it or connect to it. While bad apps do occasionally show up in the Market, Google Removes them swiftly and they have the ability to remotely kill bad apps on the customer phones. The expertise Of the Intelligence community (NSA. GCHQ, etc) will shore up Google's proficiency. The security Relationships they now have will enhance user protection against data sniffing and exploitation tools.

Android Market

Critics and experts claim free antivirus apps from the market miss nine out of ten potential threats. The free apps guide users Through the capabilities of the apps detection abilities but, many users don't examine the potential they are getting. The paid apps Are able to scan and detect about half of all installed threats but they are limited by the sandboxed environment.

On installation blocking, the Zoner app blocked 80% of malware, while free apps typically failed to detect any infiltration. The Zoner app springs into action (as intended) to stop most infection processes. The paid apps (AVG, Kaspersky, etc) blocked All malware from being installed, even those not spotted with manual scans.

Zoner is a great app but (with the best outcome for the free apps), with Zoner AV scanning in real-time as apps are installed, 20% of known threats slipped right through. These free apps are used by millions of people who have absolute confidence in The Android Market. Users should be careful not to become complacent with proper security practices (avoid downloading Apps from the seedier side of the net).

The paid solutions will stop all of the current threats from being installed. This is good for an Android phone right out of the box. If a user has a unit that has been in use with no antivirus, many previously-installed malware apps will be missed. Basically the user (Paying for the app) is not going to be able to sweep their phones clear of malware.

Android User Security

The typical android user does not have the security research resources of the NSA available for their personal Protection on the networks (with the communication protocols used by most smart phones and tablets). Many users Are quick to adopt android antivirus (paid and free) apps assuming they are receiving the same expertise available In the desktop market. They lack the kind of low-level system access onmobile that desktop antivirus apps have had for years.

A new phone (should be backed up immediately for recovery operations) is better with a free antivirus app than it is with none at all, but an infected Android (or smart phone) is not going to benefit from a free security app (because most android malware will not be swept out) and will probably be in trouble even with a paid security app (20% of malware gets through). Most of these have trouble cleaning a phone which is already full of malware.

Users Getting That New Droid

The best way to stay safe on Android is to back up your android and just stick to established apps from the official Android Market, Amazon Appstore or go straight to the paid security vendor sight (such as AVG, Bulldog, Kaspersky. Etc) to avoid the most Serious Android Malware threats in the wild.

The user's should stick to the official Android Market repositories, verified security vendor sights, leave the ‘unknown Sources' option disabled (in the ‘Android Settings)' and always scrutinize the security permissions and app requests.

Remember, when an app is installed, the system will always display the permissions requested. "SMS Trojans" Usually come in the form of a single app (like a website add-on) that asks for permission to send and receive SMS messages. When the infected app is given permission to access background processes, it also allows the Trojan to do the same. The Trojan then works unrestricted behind the scenes to send messages.

The Trojans typically are software apps the user installs willingly not knowing it is infected (from third party sites With porno, pirated music, games, etc). When they are installed, initially the user will be informed the app was not compatible, leading the user to believe the app did not install… then it goes after the country code to retrieve the phone Number… they then text premium rate numbers to rack up Charges for the unsuspecting user. They also employ this Tactic for apps that include phone calling permissions; that could call premium rate numbers without the users knowledge.

The most dangerous threats have been detected on forums and third party sights pretending to be well known apps. Users should proceed with caution on third party sights. By leaving the ‘Unknown Sources" option disabled in the ‘Android Settings" apps can not be side loaded effectively, blocking malicious vendors.