# Global Information Assurance Certification Paper

# Android Security: Web Browsers and Email Applications

*GIAC (GCCC) Gold Certification*

Author: Marsha Miller, mmiller@mastersprogram.sans.edu
Advisor: Mohammed Haron
Accepted: August 29th, 2016

Template Version September 2014

Abstract

Mobile devices are popular communication tools that allow people to stay connected in most places at all times. Despite the varied proliferation of applications that can be installed on smartphones and tablets, web browsers and email applications are default applications that remain highly vulnerable if not properly addressed. This paper will compare several different mobile versions of these applications and use the E-mail and Web Browser Protections critical control to suggest ways to secure these end points.

# 1. Introduction

Computers are now smaller and more efficient. They have become a staple used every day by many people. It is hard to imagine life without using a smartphone to keep in touch with varying events. However, with that ease of use, there is an increased risk to security. Email and web browsing remain high profile targets that produce results for attackers with little effort required.

Mobile devices most often connect to networks and other devices via wireless and Bluetooth protocols. They also have different operating systems than standard personal computers, and patches and upgrades for Android usually come at a much slower pace. The length of time increases due to the number of levels involved in the patching. After Google releases the update, both the manufacturer and the cellular provider may each add a code modification before final delivery to the device.

Devices usually provide a default email application and web browser; however, the user may download additional applications to augment or replace these. Despite the fact that application updates are enabled to install automatically by default, users may turn this feature off. In that case, the user must initiate the update process manually. Vulnerabilities addressed in a new update may not be applied to all devices immediately, leaving those devices open to additional risk.

Also, consider the human factor. Social engineering is a tactic that preys on a victim's false sense of safety. Users tend to ignore the warnings of the security community to use caution when opening email from unknown sources, clicking links, and in general, being alert when viewing websites. Attackers capitalize on this by enticing the user with various methods.

In the past, developers designed web browsers with function as the prime focus. Mobile versions today are no different. Although added over time, privacy features are usually disabled by default and must be enabled by the user. The user must be security-conscious enough to protect their personal data and willing to make security a priority.

Author Name, email@address

Authors of a 2012 study on mobile web browser security point out that security features are not standardized across various browser applications (Amrutkar, Singh, Verma, & Traynor, 2012). Even worse, there is a vast difference between the desktop and the mobile versions. The developers did not port security features offered on the desktop platform to the mobile one, increasing risk to the mobile browsers. The paper also proposes possible attacks that can be used to exploit the vulnerabilities.

To fill an increasing cyber security gap, the Center for Internet Security (CIS) maintains the CIS Critical Controls. These controls are "a prioritized, highly focused set of actions that have a community support network to make the implementable, usable, scalable, and compliant with all industry or government security requirements" ("Center for Internet Security," 2016). Together with industry experts, CIS updates the prioritized list which evolves as the threat landscape changes over time. Email and web browsing are currently addressed in one control.

# 2. E-mail and Web Browser Protections Control

## 2.1. How This Control Applies

The E-mail and Web Browser Protections control provides security guidance for these two applications. While some of the critical controls address post-breach actions, this particular control focuses on proactive measures of prevention.

Recommendations for this control that can be applied to mobile devices are:

- Enforce only fully supported and up-to-date web browsers and email clients
- Restrict add-ons to only those that are necessary
- Limit scripts
- Use URL filters to manage website access
- Where possible, use separate browsers: one configured with script prevention and a second with minimal configurations
- Block malicious email attachments

Applying patches automatically or as soon as possible after testing is one way to reduce vulnerability of the device. Maintaining both the OS and the applications in this manner helps secure the device as a whole.

Security features should be enabled where available, and reserve the default web browser for instances where functionality is inhibited by properly configuring a secure browser. However, in some cases, security experts recommend not using the default browser for any reason. If the application is end-of-life with no new updates, such as those systems with an operating system older than Android 4.4, install and use a different browser. These systems are vulnerable to URL spoofing, and there is no mitigation for the applications (Constantin, 2015). Metasploit also offers a module that targets these susceptible versions.

In general, updating the web browser and email application to the most current version is a good start for improving the security of the mobile device. Once a vulnerability has been announced, it increases the likelihood of exploitation. Malware developers know that a percentage of the devices still in use contain outdated software, making it worth the effort to try an exploit. By enabling software updates to occur automatically, it will reduce the risk of exposing the device unnecessarily.

Add-ons and scripts provide many different types of functionality; however, they should be reviewed and used cautiously. While they provide benefits to the user, they may also introduce undesirable vulnerabilities to the application.

Whitelisting and blacklisting can be beneficial in reducing the risk of visiting a website hosting malware. These URL filters can be maintained utilizing several techniques.

In addition to harmful website URL links, email attachments may contain malicious code. Opening the attachment will execute the script and infect the device. If possible, block or quarantine the email to prevent an accidental infection.

And last, identify the websites needed or most often visited, and configure a web browser with the highest security standards possible to access these sites. Any sites not properly displayed with the features enabled should use a secondary browser with lower

security settings. However, it is important to use this web browser only when necessary and to enforce restrictions where possible. Otherwise, it nullifies the risks mitigated by employing this setup.

### 2.2. Malware

With so many infections delivered utilizing SMS or alternate application stores, Towelroot is a good example of why this control is important and still relevant. Discovered in April of 2016 by Blue Coat Labs, the Ransomware is posted to a website using an advertisement and delivered as a drive-by (Brandt, 2016). The malware code initiates as the browser loads the web page and the user's device becomes infected.

However, malware can easily be delivered to an unsuspecting user via email utilizing a phishing campaign. Phishing relies on the user to fall victim to social engineering practices. A common phishing technique provides an unknown URL disguised in such a way that the user mistakes it as valid. Trojans such as Triada can spoof URL's, sending a user to a different site than the one intended (Kivva, 2016). Most often, the default web browser changes, but it also possesses potential for more damaging results.

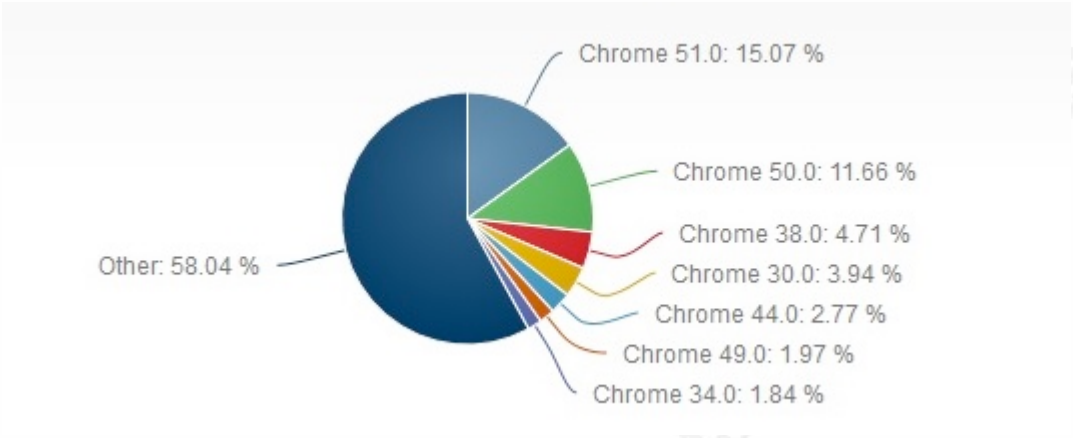
Stagefright 2.0 caused a stir in October of 2015 when it revealed a vulnerability inherent in all Android devices. While the first version targeted the messaging system for delivery, the second caused concern for web browsers and phishing attacks. Hanan Be'er of NorthBit posted a proof of concept outlining the attack vectors on GitHub (Be'er, 2016).

While malware developers use various delivery methods, web browsers and email are both frequently targeted due to the human factor. It is important to educate others and practice good security habits.

## 3. Web Browsers

Although updates to web browsers are released to fix vulnerabilities, users often do not update the applications regularly. This graph shows the various versions of

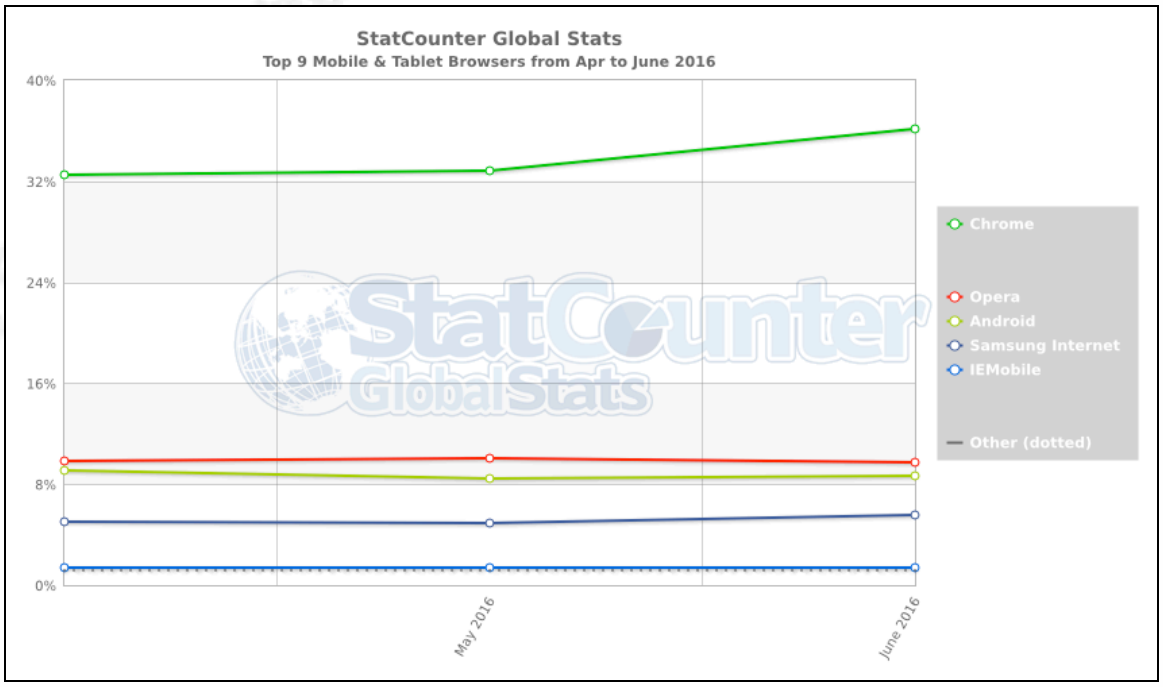
Chrome in use during June 2016. With updates released every one to two months, nearly half of the installations are a previous version.




*(NetMarketShare, 2016)*

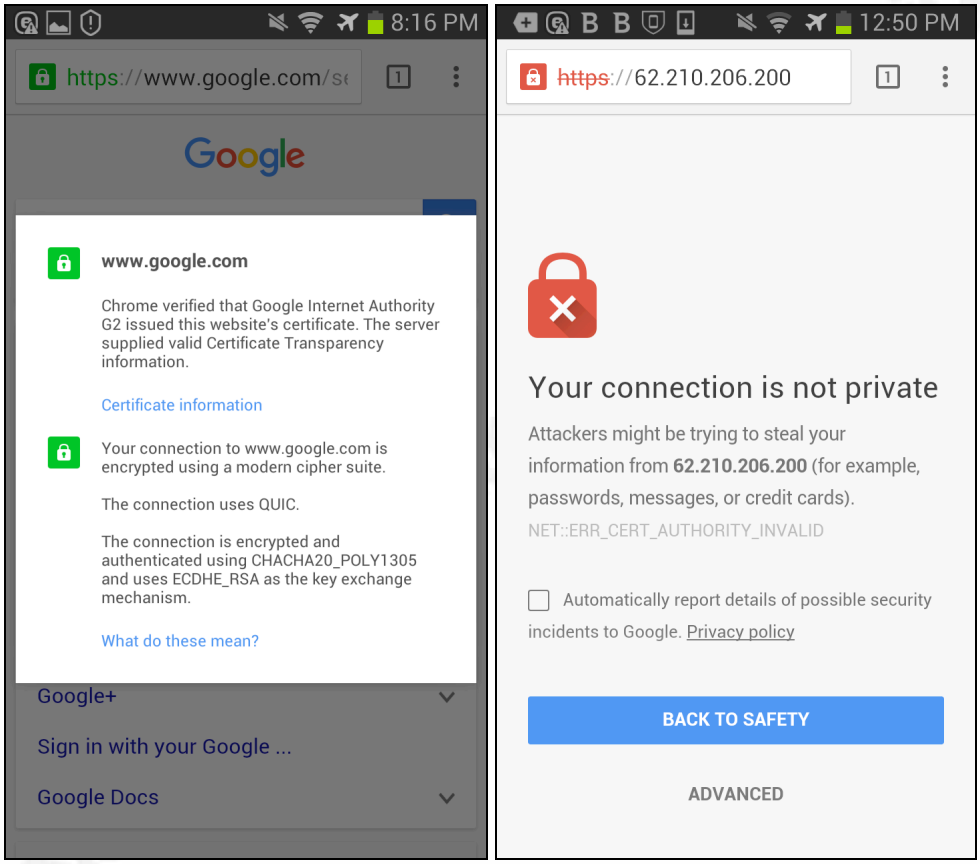
## 3.1. Chrome

Created as an alternative to Internet Explorer and Firefox, Chrome was designed from the ground up to accommodate the changing landscape of web browsing (Levy, 2008). According to StatCounter in June of 2016, Chrome is the leading mobile device web browser regardless of the operating system platform.




*(StatCounter, 2016)*

To make users more aware of secure websites, browser designers added a padlock, typically to the left of the URL, to signify when a web page uses a type of encryption. Chrome displays this icon in green indicating a site using HTTPS and providing information about the certificate. Unfortunately, it requires the user to tap three times to access the significant information such as the cipher strength.




Users can fine tune the application by modifying separate settings. For instance, device location information and JavaScript are available options. For privacy concerns, enable "Do Not Track", and Clear browsing data should be performed on occasion to clear the cache. Also, the user can uniquely customize individual settings per website under Site Settings. Additional settings are available by typing "chrome://flags" into the address bar; however, the availability of these settings may change at any time. Although useful in providing additional functionality, Chrome extensions are not available on the Android platform.

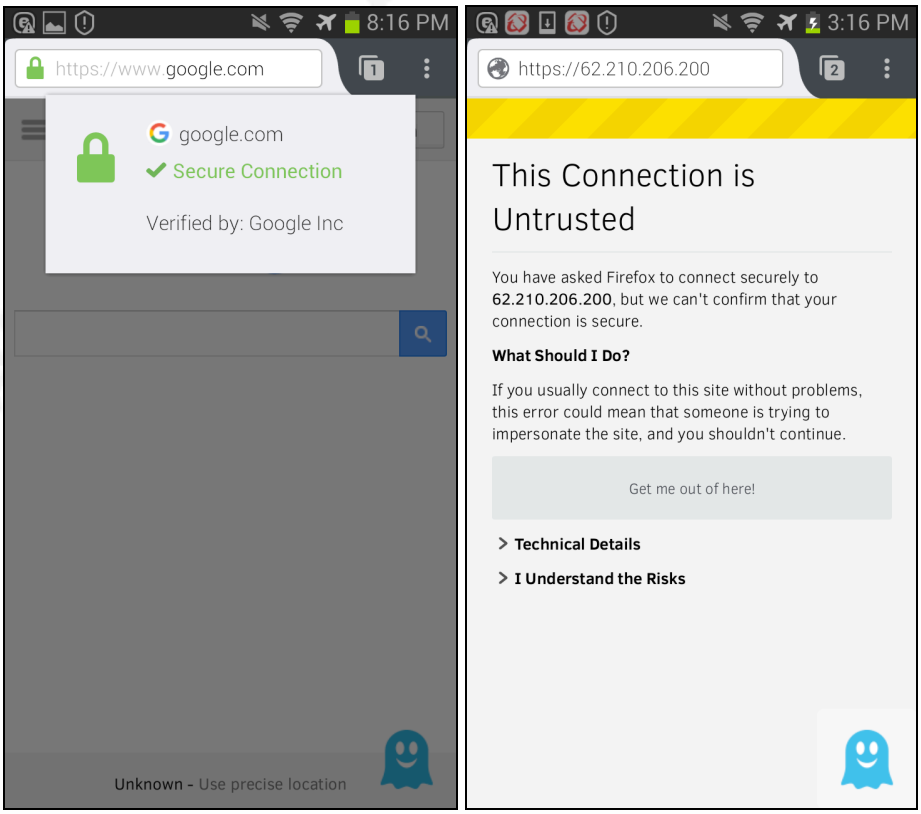
Author Name, email@address

Every day, Google reviews web pages to provide internet users a measure of protection from unsafe sites ("Safe Browsing – Transparency Report – Google," 2016). Compromises occur daily and present an opportunity for malware to distribute under the pretense of a known good site. Web pages are continuously reviewed for changes to their security posture and webmasters are notified. To take full advantage of this protection on mobile devices, turn on Safe Browsing under Privacy settings to provide various warning messages about sites.

## 3.2. Firefox

Firefox is a web browser supported by Mozilla and has been popular with desktop users for many years as an alternative to Microsoft's Internet Explorer. Add-ons allow the user to customize the experience.

Firefox displays a green padlock when indicating the web page is encrypted which helps the user identify a more secure connection. However, the Firefox mobile application does not display information about the certificate for the user to view easily.



Firefox also provides a warning for unsafe websites. To make this determination, it checks lists of sites tagged as malware, phishing, or containing undesirable software. It also sends metadata of downloads to the Safe Browsing Service at Google to verify content, which continuously improves detection capability across the board. This feature comes standard with the application.

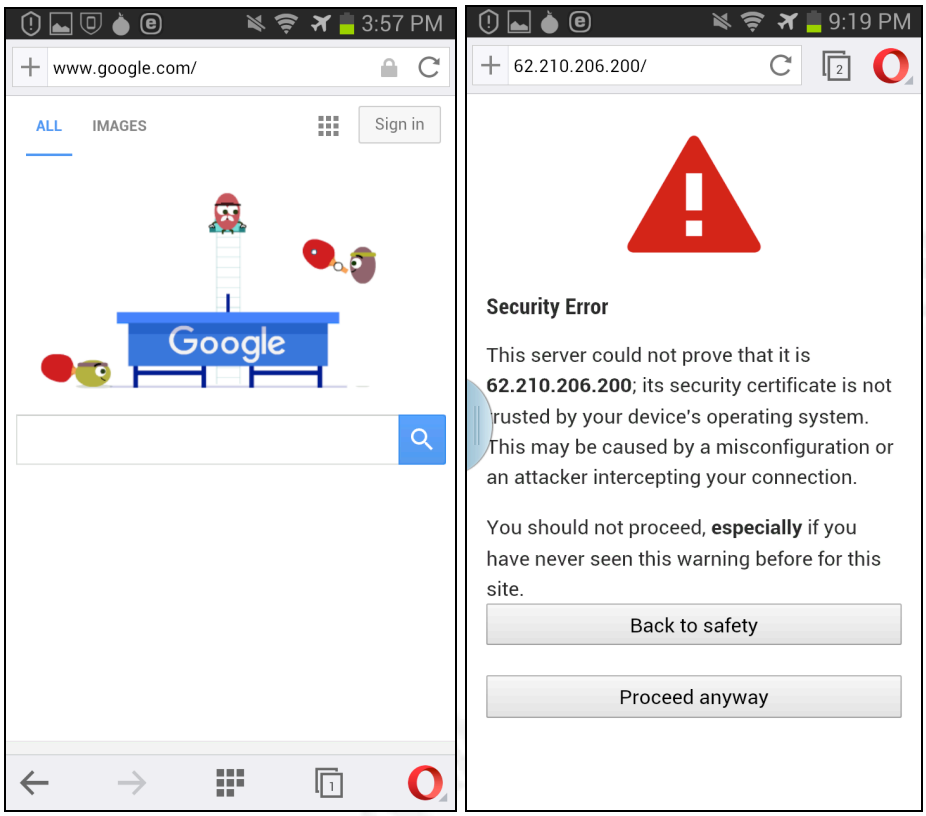
Configure additional settings to enable or disable features. For instance, JavaScript can be allowed or prevented. To make this adjustment, open a new tab in the mobile browser and type "about:config" in the address bar. Scroll through the available features and adjust them as necessary.

NeeURLFilter, ProCon Latte, and other whitelisting add-ons may help limit the URL's accessed on a device. They offer both blacklisting and whitelisting options. For instance, the ProCon Latte add-on can be set to restrict viewing of pornography and gambling sites, or it can be configured to allow only approved websites.

## 3.3. Opera

Opera focuses on increased speed when loading web pages. To achieve quicker loading, it caches the content. It also offers add-ons, extensions, and a built-in VPN free-of-charge, although none of these options are currently available on the mobile version.

There are two applications available for Android: Opera Mini and Opera Browser. Opera Mini displays a green padlock to indicate a secure connection while Opera Browser shows a gray icon that is easy to overlook. Neither provides access to the security certificate to verify the encryption strength; however, an insecure site will produce a noticeable warning.

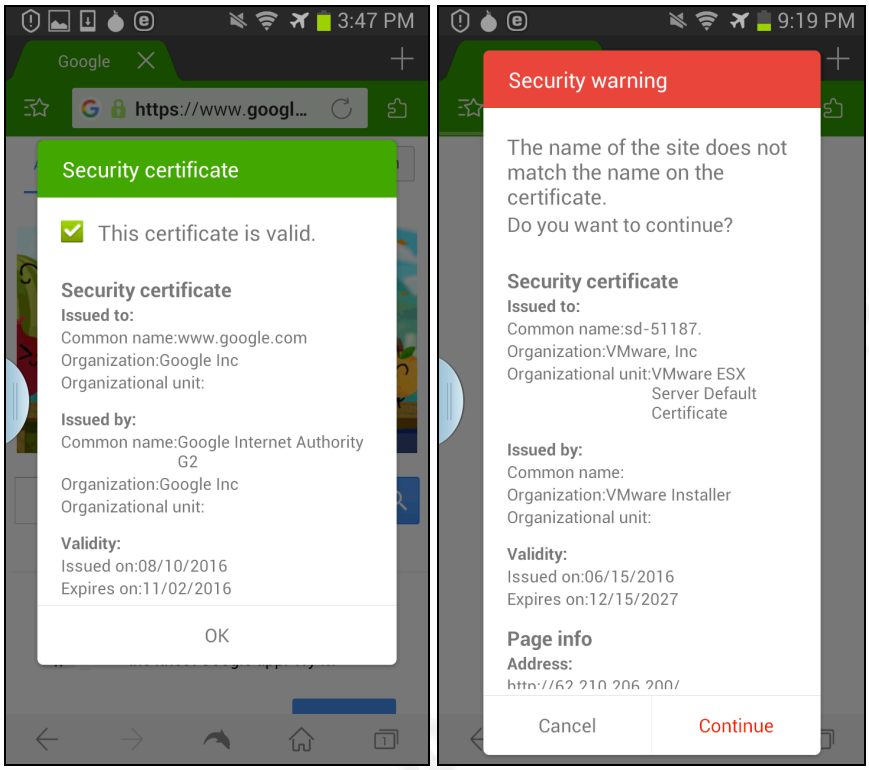



The available list of settings in Opera for Android is limited. For security, set the option to block pop-up windows and occasionally clear the cache. Typing "opera:flags" in the address bar allows access to additional security settings. The list of configurations is short and presented as experimental features, similar to Chrome.

### 3.4. Dolphin

Dolphin is a feature-rich browser. In addition to a private mode, it provides additional features such as the ability to use voice command and hand movements to control the interface.

Dolphin offers a green padlock to indicate a secure site, and the user views the security certificate information when tapped. However, the information displayed is limited.




Configuration settings include options for checking server certificate revocation, caching web pages, enabling JavaScript, accepting cookies, and blocking pop-up windows. The user can set options to clear select types of data automatically when exiting the application. Add-ons are also available for installation as separate applications.

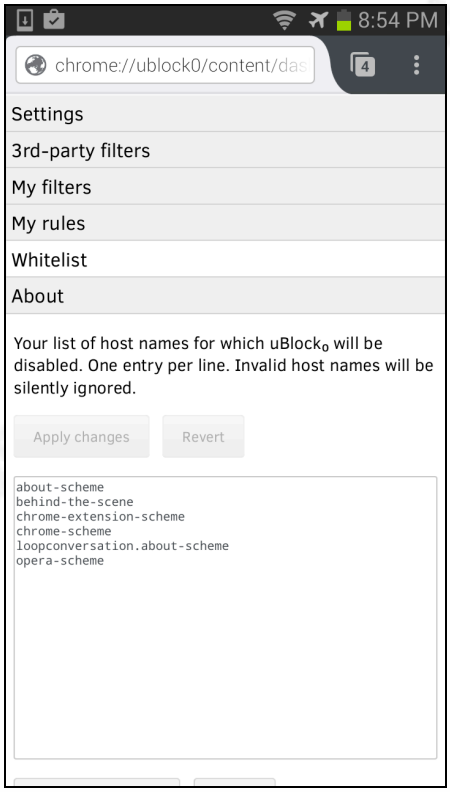
## 3.5. General Protections

To help mitigate possible issues, use a vetted download source such as Google Play and a trusted network (such as a business or home; not an open unsecured Wireless Access Point (WAP)) when performing these operations. As stated in a vulnerability involving the Dolphin web browser, someone with elevated privileges on a network can take advantage of vulnerabilities and alter files (Rotlogix, 2015).

The user should disable JavaScript in browsers that support this configuration setting. Several vulnerabilities, including Stagefright, are associated with this feature, and it should be enabled only when necessary.

While trackers are often used in legitimate ways, they also may have unintended negative consequences such as those that impact privacy and data leakage ("What are

Cookies & Trackers? | GHOSTERY," 2016). However, the potential to use trackers to distribute malware is also a concern. Various add-ons and extensions are available on multiple platforms and provide additional protection. Firefox and Chrome both support the use of Ghostery and uBlock Origin. Ghostery blocks trackers and gives the user control over which ones to allow. During the initial setup, click on Categories and select options to block such as advertisers, site analytics, customer interaction, social media, essentials (including tag managers), audio/video player, adult advertising, and comments. It also provides the ability to whitelist a trusted site. uBlock Origin is configured to block ads, trackers, and malware sites by default. It can also be configured to filter websites.




HTTPS Everywhere, supported by Electronic Frontier Foundation and The Tor Project, will force all web browsing traffic to be encrypted for websites that support HTTPS. In doing so, it provides a measure of security so that encrypted traffic is the default when available. If the page is not displayed properly due to an issue, the rule can be temporarily disabled and reported to the support team.

OpenDNS offers URL filtering for both business and personal needs. For personal use, configure it by adding two IP addresses to the WiFi settings. The website

contains instructions for configuring home routers and mobile devices; however, this will not prevent access while on the cellular network, and the setup must be changed for each SSID stored in the WiFi settings.

A Virtual Private Network (VPN) encapsulates all device traffic, providing security beyond the web browser. Some businesses already employ this technique on the mobile platform. For those that do not want to manage or maintain VPN equipment, personal and professional services are available for purchase.

# 4. Email Clients

Android mobile devices come with preinstalled email applications such as Gmail and a default email client; however, the user may also choose to download others. One reason for using a different client is functionality. For instance, when tested, the default email client on the Samsung S5 device was unable to support three separate types of email accounts simultaneously. Another reason to choose a different application is security. The ability to send an encrypted email may be hampered or unavailable on some applications.

APG and OpenKeychain create a key pair (public and private) for the use of encrypting email. Using the established keys, two users achieve a more secure communication. In his article, Ring mentions that OpenKeychain was vulnerable to data leaking along with Gmail and K-9 (Ring, 2016). However, OpenKeychain resolved the issue several months prior (Schürmann, 2015). Although not mainstream with the average user, this method is popular among privacy advocates and easily configured.

## 4.1. Gmail

The Gmail application usually comes standard on Android devices; however, it is not considered the default email client. It can be configured for multiple accounts and is popular among many Android users ("Email Client Market Share and Popularity - June 2016," 2016). A potential disadvantage is that it does not provide many options to allow a customizable interface.

OAuth, an authentication method that provides additional security, is supported by the Gmail client. After the account is configured, a random key is generated for use and applied in the email application in place of the account password. This prevents the client from having access to the true account credentials.

The Gmail application does not support utilization of AGP or OpenKeychain for email encryption; however, the use of an additional application such as Virtru gives the user the ability to send encrypted email via Gmail. This statement directly addresses the Gmail application itself and not the use of Gmail utilizing Chrome with an encryption extension.

Gmail blocks some file attachments viewed as a security risk. Attachments with extensions frequently used to deliver malware, such as .exe and .vbs, are blocked.

```
This message was created automatically by the mail system (ecelerity).

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

                    (reading confirmation): 552-5.7.0 This message was blocked because its
 content presents a potential
552-5.7.0 security issue. Please visit
552-5.7.0  https://support.google.com/mail/answer/6590 to review our message
552 5.7.0 content and attachment content guidelines. u123si12432342qkh.321 - gsmtp
```

## 4.2. K-9

K-9 is a community-supported email client that was developed to provide more functionality to the user. It contains many options which allow users to customize the application. For example, a user can change the number of lines viewed in the inbox or create a custom signature.

The main security advantage of using K-9 is that it supports the use of OpenPGP for encrypting email. APG and OpenKeychain are available options. K-9 also supports client-side SSL for authentication and plans to support S/MIME in future editions ("Security | K-9 Mail," 2016).

## 4.3. TypeApp

TypeApp focuses on organization using a feature known as clusters. It also boasts multi-device support including Android Wear. It supports configurations that allow

customization of the interface, such as the action performed when the user swipes left versus right. The application has features that allow the creation of groups and the ability to treat an email as a task with a notification function.

Despite the customization options available for the user to make changes to the appearance and menus, security settings are limited. It supports the use of two-factor authentication; however, there are no additional security settings that integrate with the use of email encryption.

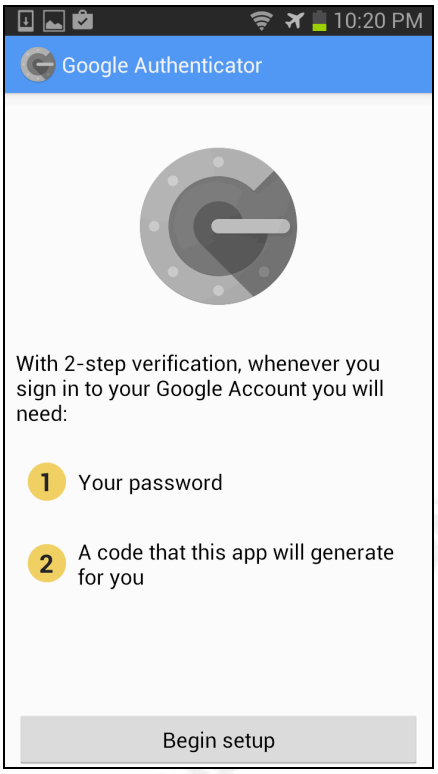
## 4.4. Microsoft Outlook

Extending its reach into the mobile market, Microsoft created Outlook for Android after buying Accompli. The interface is customizable and provides synchronization with the account calendar. While in the Inbox, it lets the user set a different action when swiping to the left versus to the right.

Although the Outlook application supports OAuth for security in regards to authentication credentials, it does not include additional settings for PGP use to support encrypting email messages. In June of 2015, Microsoft added authentication updates including multi-factor support for Office 365.

## 4.5. General Protections

When offered by the service provider, utilizing two-factor authentication with email accounts increases the security. Services hosted online, such as Gmail and Microsoft Live, provide this option which adds additional protection for both accessing the account on the server and the email applications on mobile devices. Requiring additional information for authentication beyond username and password decreases the likelihood that stolen user credentials are effective after a breach situation. Options available to the user for the second code include receiving an SMS text message or accessing an application, such as Google Authenticator or the Authenticator in Sophos Mobile Security, which provides a random set of numbers that change every thirty seconds.



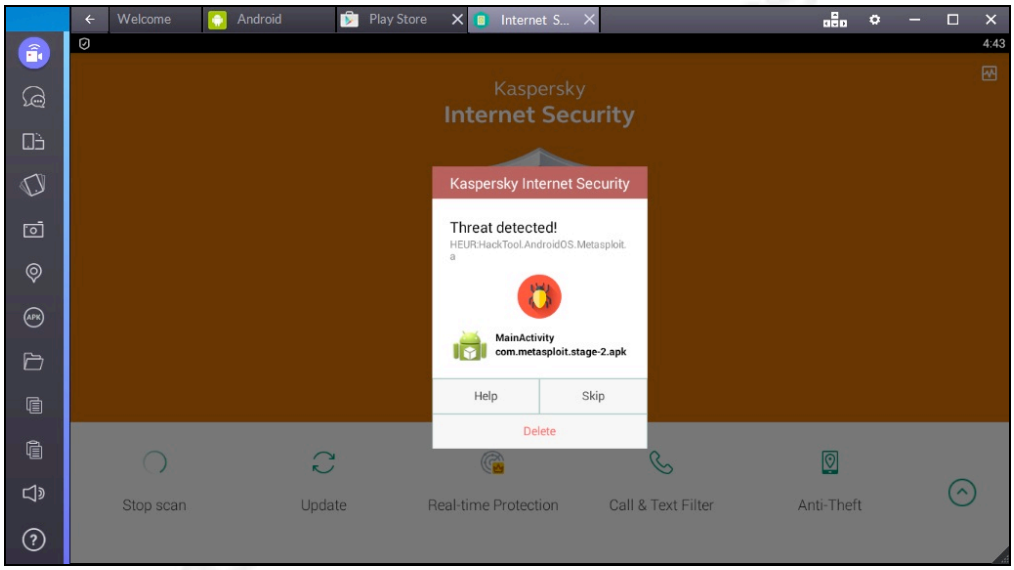

Ciphermail is an application available in the Google Play store that allows the user to send and decrypt email messages. It works in conjunction with an email client such as Gmail that supports S/MIME. During setup, the user can either create a certificate or utilize an existing one from a Certificate Authority (CA).

## 5. Device Security

Several companies have created anti-malware applications to provide protection for mobile devices. Kapersky Internet Security, Bitdefender Mobile Security, ESET Mobile Security & Antivirus, Sophos Free Antivirus and Security, Trend Micro Mobile Security & Antivirus, and Norton Security and Antivirus provide safe browsing features; however, the cost and coverage vary. Although available as a feature, none offer the web protection free to the user. All applications offer a free trial period for evaluation, but most only cover Chrome and the default web browser. While Norton Security and Antivirus also provides a safe web browsing features, the protection is limited. The standard free-of-charge offering notifies the user of unsafe sites during a search, and the

paid application only covers protecting the device from malware accessing personal information.

To test these anti-malware applications, Metasploit was used to create a file that, when installed, would create a backdoor and a connection back to the Metasploit console. After installing the software, Kapersky, Bitdefender, Sophos, and Trend Micro detected the presence of the Trojan using the default settings. Each provided a warning in various forms and offered removal. While not a default action, ESET can be enabled during setup to detect malware applications.




Anti-malware applications may help protect email as well. While those tested lack protection in direct relation to the email client, Kapersky does prevent access to malicious websites (if the user clicks a link in a phishing email), and several provide protection from the installation of a malicious application. ESET only offers the phishing protection in the premium edition.

Corporate solutions are also available. Sophos and Trend Micro both offer solutions and applications that cover a multitude of security features.

Sophos Mobile Security scans applications for malware during installation. It also checks URL's against a database they maintain for malicious websites and blocks access. Businesses can manage the devices centrally to provide equivalent configuration settings and detect threats.

Author Name, email@address

Trend Micro Mobile Security offers similar coverage for device protection. It provides protection from malware application installations and websites. It also provides central management of the devices.

Businesses with a vested interest in maintaining security across mobile devices may also purchase software services that provide additional protection. URL filtering and whitelisting may be available in this manner. For instance, AirWatch Mobile Browsing Management provides features such IP whitelisting and proxy services similar to a VPN ("Mobile Browsing Management | AirWatch," 2016). Some MDM software, such as AirWatch MDM or Symantec Mobility: Suite, may also provide solutions. These include the ability to block attachments or provide a proxy filter, which also serves to increase security for web browsing.

## 6. Conclusion

As mobile device use scales up, malware developers will continue to target these data-rich environments. Both personal and professional devices have much to offer malware developers with an agenda. It is important to heed the recommendations of the E-mail and Web Browser Protections critical control. Implementing available security features, anti-malware solutions, and properly managing software updates will help protect these devices.

The default web browser continues to be frequently used, especially among less skilled device owners. Also, users are less likely to look for alternatives to the default email application that comes natively installed on mobile devices. It is important for users to implement appropriate security features on both web browsers and email clients. Businesses should also consider other methods of policy enforcement to ensure the protection of the device and data.

In addition to the alternate web browsers and email clients, there are security solutions available for installation. These options range from personal to professional use and scale upwards from free to corporate solutions. Choices vary from specific protection, like phishing and anti-virus, to those that encompass the overall device, such as a more robust MDM option.

Author Name, email@address

While not an exhaustive list of either applications or security protections, this paper provides a guide to improve security for mobile devices. It is important to reference the critical control, identify the potential vulnerabilities, and mitigate the risks.



Author Name, email@address

# References

Amrutkar, C., Singh, K., Verma, A., & Traynor, P. (2012). VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. *Information Systems Security*, 16-34. doi:10.1007/978-3-642-35130-3_2

Be'er, H. (2016, March 24). GitHub - NorthBit/Metaphor: Metaphor - Stagefright with ASLR bypass. Retrieved August 23, 2016, from https://github.com/NorthBit/Metaphor

Brandt, A. (2016, April 25). Blue Coat | Android Towelroot Exploit Dogspectus Ransomware. Retrieved July 31, 2016, from https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware

Brinkmann, M. (2009, March 25). Configure Firefox To Only Open Whitelist Websites - gHacks Tech News. Retrieved July 31, 2016, from http://www.ghacks.net/2009/03/25/configure-firefox-to-only-open-whitelist-websites/

Center for Internet Security. (2016). Retrieved July 4, 2016, from https://www.cisecurity.org/critical-controls.cfm

Chaffey, D. (2016, April 27). Mobile marketing statistics 2016. Retrieved June 26, 2016, from http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Constantin, L. (2015, May 20). Android stock browser vulnerable to URL spoofing. *PCWorld*. Retrieved from http://www.pcworld.com/article/2924912/android-stock-browser-vulnerable-to-url-spoofing.html

Author Name, email@address

Email Client Market Share and Popularity - June 2016. (2016, June). Retrieved July 31, 2016, from https://emailclientmarketshare.com/

Heiderich, M., Horn, J., Aranguren, A., Magazinius, J., & Weißer, D. (2015). *Pentest-Report OpenKeychain*. Retrieved from Cure 53 website: https://cure53.de/pentest-report_openkeychain.pdfhttps://cure53.de/pentest-report_openkeychain.pdf

How does built-in Phishing and Malware Protection work? | Firefox Help. (2016). Retrieved August 26, 2016, from https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work

Kivva, A. (2016, June 6). Everyone sees not what they want to see - Securelist. Retrieved July 4, 2016, from https://securelist.com/blog/research/74997/everyone-sees-not-what-they-want-to-see/

Levy, S. (2008, September 2). Inside Chrome: The Secret Project to Crush IE and Remake the Web. *Wired*. Retrieved from http://archive.wired.com/techbiz/it/magazine/16-10/mf_chrome?currentPage=all

Market share for mobile, browsers, operating systems and search engines | NetMarketShare. (2016). Retrieved July 4, 2016, from http://www.netmarketshare.com/

Mobile Browsing Management | AirWatch. (2016). Retrieved July 31, 2016, from http://www.air-watch.com/solutions/mobile-browsing-management/

New access and security controls for Outlook for iOS and Android - Office Blogs. (2016). Retrieved August 26, 2016, from

Author Name, email@address

https://blogs.office.com/2015/06/10/new-access-and-security-controls-for-outlook-for-ios-and-android/

Ring, T. (2016, April 5). Android messaging apps leaking data through 'surreptitious sharing'. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/

Rotlogix. (2015, August 22). Remote Code Execution in Dolphin Browser for Android. Retrieved July 4, 2016, from http://rotlogix.com/2015/08/22/remote-code-execution-in-dolphin-browser-for-android/

Safe Browsing – Transparency Report – Google. (2016). Retrieved August 26, 2016, from https://www.google.com/transparencyreport/safebrowsing/

Scher, J. (2012, August 12). How can I disable JavaScript in Firefox Mobile for Android? | Firefox for Android Support Forum | Mozilla Support. Retrieved July 11, 2016, from https://support.mozilla.org/en-US/questions/934492

Schürmann, D. (2015, October 29). OpenKeychain 3.6: Security Audit and Tons of New Features · OpenKeychain. Retrieved July 31, 2016, from https://www.openkeychain.org/openkeychain-3-6

Security | K-9 Mail. (2016). Retrieved July 31, 2016, from https://k9mail.github.io/documentation/security.html

StatCounter Global Stats - Browser, OS, Search Engine including Mobile Usage Share. (2016). Retrieved July 4, 2016, from http://gs.statcounter.com/#mobile+tablet-browser-ww-monthly-201604-201606

Author Name, email@address

Test antivirus software for Android - May 2016 | AV-TEST. (2016, May). Retrieved July 31, 2016, from https://www.av-test.org/en/antivirus/mobile-devices/android/

What are Cookies & Trackers? | GHOSTERY. (2016). Retrieved August 6, 2016, from https://www.ghostery.com/intelligence/tracker-basics/



Author Name, email@address