Google Chrome OS and Chromebook Whitepaper

Version 0.2

July 2, 2013

Document History

DOCUMENT VERSION #	ISSUE DATE	BY	DESCRIPTION OF REVISION(S)
Version 0.1	June 4, 2013	Amélie Koran	Initial release
Version 0.2	July 2, 2013	Amélie Koran	Internal Review Draft

Table of Contents

1 Executive Summary

This whitepaper has been commissioned to explore the feasibility of the use of Chrome OS-based laptops, notably a Chromebook, for use by executive and upper-level management within the U.S. Department of the Interior as alternative for semi-disposable mobile computing devices while on travel. As with the advancement of the consumerization of information technology, prices have dropped significantly and many solutions are essentially commodity items that, while they may differ from their sourcing, will transparently run a common inexpensive platform to provide access to services and features of a provider. In recent cases, the mobility of executive staff to sensitive areas of the globe has required a rethinking of how services and data are access from their home agency, and in case of loss, theft or tampering (eavesdropping, malicious compromise, etc.), can we disposed of upon return without extensive cost of resources (both human and financial) if deemed non-reusable in day-to-day operations upon return home. With the advanced features, reduced cost, and computing model of a Google Chromebook, the investigation below will outline the benefits and issues with a possible use of such a device for these use cases.

2 Introduction

Mobile technology is tricky, so is sensitive travel, and combine the two it becomes a security nightmare. In days past, when an official returned from an area of sensitivity, whether or not the device (phone, laptop, tablet) was in use during the trip, it was often turned over to ***** or similar entity for forensics investigation for review of signs of tampering or compromise, and more often than not, was not returned to the owner, and a new replacement system was provided for future use. This is not only costly, but logistically it's difficult and time consuming to constantly be issuing, retrieving and examining devices at a volume at which executives and upper management perform travel.

As a number of critical services offered regularly to executives, most have moved completely to web-based, network accessible solutions, eschewing a specific host-based standalone application. To that end, the Chrome OS that power the Chromebooks are minimally outfitted with only a browser and internal media player to support applications designed in such a way, notably, most of Google's own offerings. This requires significant consideration of “always on” network connectivity for reasonable use, since the platform utilizes these services remotely, rather than providing local storage, execution and manipulation of data. The need for constant network transport, and the data either residing in a cloud-based solution or on a ***** controlled solution does also change the typical mode in how these solutions are secured, since before the advent of a more mobile workforce, it had been assumed most activity took place on tightly controlled commodity *****-furnished and on USG managed networks.

3 Use Cases

As noted earlier, the primary use case for consideration of Chromebooks is for executive and leadership travel. This will encompass both domestic and international travel. As more ***** computing services are enabled for web-based access and cloud-centric hosting, other employees, contractors and volunteers can take advantage of similar access to essential ***** systems. This initial use case also opens up potential for other users to consider the use of Chromebooks in light travel situations that may not involve sensitive travel areas, or even as replacements for standard issue *****-furnished laptops and desktops. Chromebooks can also be leveraged as technology enablers for job roles and positions traditionally not issued such technology in order to increase skills of workers and potentially enable

them to move up into positions they originally had no means to advance to. In other cases, where manual processes utilized, or access to computing systems by certain employees requires travel or location dependent access (such as time or data entry), these systems can be leveraged with appropriate communication capabilities to reduce those burdens.

3.1 Sensitive Executive Travel

This is the primary use case, and provided the Chromebook system can be adequately tested and provide access to crucial information systems and services that an executive may need while on travel, the use case is solid. Since forensics are often required for returning devices, as well as replacement, the costs on replacement of such devices will drive this use case scenario. However, since the information gathered from a forensics investigation from a possible breached device, even if the Chromebook should not store any information of note, locally, the costs involved with a cursory post-travel examination may still be attached.

3.2 Non-"Information Worker" Enablement

Much of the *****workforce is comprised of non-technical workers, this includes many hourly and wage-grade (WG) staff which typically are not presented with computing devices. In many cases, there's no workforce development placed in the hands of this staff, as much is unskilled and would not traditionally benefit from the use of computing. However, cases can be made, when looking at different ways to integrate their daily tasks with potential access to computing services, such as digital work orders, time tracking, education and training, data entry and gathering, GIS services, and entertainment. This does provide a great opportunity for ***** to train up much of its underserved staff to give them the tools to operate in the 21s century and potentially pass skills to family members and further their careers. The bonus for all workers is easier access to training provided by the ***** e-learning solution, often a yearly requirement for certification of staff training plans, and would be easily enabled by leveraging low-cost thin computing devices such as the Chromebook.

3.3 Lightweight Location Independent Service Access

***** is a dispersed organization, geographically challenging, since many locations are either staffed by a small number of people, or are in places where traditional network connectivity and system access is difficult. In a few cases, where an employee will be required to travel to a distant location to gain network access to complete required work or training, could possibly be eased by providing Chromebooks with cellular data connectivity. With the reduced functionality and low cost, providing this type of solution could be far lower than the cost of travel and lost time by the employee to complete the task in the previous arrangement, as well as opening up other functionality that wasn't available due to geographic location and service availability. Much like the use case for executive travel, if the device is lost, stolen or damaged, the replacement cost is far lower than providing the more traditional IT device of a laptop or desktop in a similar configuration. With a provisioning front-end and the use of authentication and access control services provided in "the cloud", getting a new or replacement device to a user is potentially streamlined as well.

4 Architecture

Essentially the Chromebook is a cloud-terminal, built around the assumption of nearly always-on access to the Internet for practical use of the device. The standard Chromebook configurations feature the following:

- 1.1-1.8GHz Intel-based CPU (Atom, Celeron or i5), optimized for mobile platforms
- 16GB SSD (on average)
- 2GB DDR3 RAM
- 11.6 - 12.1 inch screen
  802.11-based WiFi and optional 3G/4G Cellular Data connectivity

These specifications are far lighter than those in traditional laptops and near those generally found in tablet computers, tiered in such a way to accelerate communication and some client-side rendering and computing, but not for long-term local storage and manipulation. All data is stored in a cloud-based data repository depending on what application is used and who runs it, as while the initial suggestion would be to primarily utilize Google services, there are plenty of other similar application and solutions in the marketplace that work in a similar fashion. Both Microsoft and Apple offer compelling cloud office solutions that have desktop counterparts for off-line use, a possibility in architecture alternatives given the float between multiple devices and operation scenarios.

The system itself, is extremely basic, but has been designed for easy maintenance and configuration, but in turn, often lacks the "tuning" capabilities to modify policies or settings that would take this consumer oriented solution into an enterprise environment. There are some user-exposed settings, but this is strictly basic preferences to address the following:

- **System Settings**: locale, wifi network, owner, white-list, guest mode, proxies
- **User Preference**: bookmarks, new tab page, browser settings, apps, extensions, themes, pinned tabs, notifications, printer, thumbnails, auto-fill data

The system supports a secure mechanism that verifies the boot chain of various components as well as any system updates, including application, OS, and firmware modules. Part of this performance versus security battle has the Chromebooks doing all the cryptographic operations of verification on-the-fly at boot time, something, that even devices with a TPM (trusted platform module) enabled, still struggle at balancing. A lot of these checks are "bitwise" at the disk level, instead of evaluating the entire file system when the OS requests files, essentially taking a mathematical shortcut in order to increase operational speed. The "owner" being the first user to log on to the system will be what all the cryptographic keying material is based off of, so it may be important to think about a pre-deployment handling and provisioning of the device before it is shipped to the end user to ensure that the configuration operates as expected to protect the system.

As an aside to the security architecture, the development of backup locations for the system's kernel and other binaries used for updates keeps the OS and Chromebook from hard failures after possible corruption and crashes, as upon reboot or application restart, the binaries, kernel, modules and firmware are verified, and if corrupted or changed are checked and then restored from known good versions and run (but, only at boot). This has the offshoot capability of making the system virtually bulletproof for normal operations, a plus for a high-demand portable solution.

5 Risks

Upon initial release, the security of the platform was in dire question, with the lack of VPN support, robust 802.11 security modes, and other vendor supported connectivity (notably certified clients for Juniper). Added to the lack of direct support of these features, the lower level architecture of data encryption within the OS (at rest and in memory) and the use of SSL/TLS for communication over cloud services is not always directly available or disclosed to the device user.

While the Chromebook is designed for "always on" network connectivity to access cloud services and applications, the hardware does contain a small hard drive for OS use and minimal user file system for local storage. This local storage is at risk if a device is lost, stolen or by other means, compromised. It is vitally important to ensure that the OS configuration for the device has native disk encryption turned on for user accessible partitions, and that subsequent kernel protections for memory access and storage are similarly configured. The original model for Chrome OS, which the Chromebook runs on, does maintain a system and a user partition, with the latter encrypted.

Since most activity will take place in the cloud or on other hosted systems, it will be vitally important, per FISMA guidelines to have any service that stores PII or USG sensitive data that is being accessed or handled through these systems, be accredited and risk accepted before access and use by ***** staff. This may be possible for most services we are formally contracted with, but without an "always on" VPN, these systems sit outside the ***** internal network much like other mobile platforms do, and monitoring the use will prove to be slightly cumbersome at times, and possibly diminish the impact of any advantages the Chromebook may provide. The data protection and security policies for these services should garner the most scrutiny under potential contracting, and should take in account the differences in a fully mobile architecture versus those typically considered for ***** internal network access.

When evaluating the simple fact that Chrome OS, and it's browser, Chrome, inherits much from the open source community, with the former being Linux, and the latter being various components, including WebKit, a framework shared among a number of projects, that potential flaws and vulnerabilities, by nature will be exposed to a wide number of other platforms and also creating a large potential surface area to be attacked that risks must be carefully evaluated. WebKit, itself, is often exploited and is patched regularly by a number of vendors, including both Google and Apple, and offers one of the riskiest components to utilize on the device, but again being the main interface to the functionality of the entire system. A flaw within WebKit affects, globally, all applications built off of it, and since most content it rendered within HTML for UI and activity, it can also affect not only the Chrome browser, but the core OS, including the fire viewer and configuration/settings screens.

Chrome is seen as a "meta application", that of which is a single interface to all the services that can be offered over the World Wide Web and supported protocols and methods. Although Chrome does sandboxing and essentially isolates each tab that is open to prevent cross-sharing of data and even memory spaces, local user access still provides the greatest risk to the entire system, including data cached and in transit on the device. For Google provided services (via their API), the system is designed to cache the login keychain and sign it (via TPM in a component called "the übertoken"), allowing for off-line access and manipulation of data, still with a user authentication layer, however, other applications do not leverage that same luxury and can open the system up for compromise if the data is stored on the local system improperly, such as login cookies (replay attacks). As part of ongoing USG IT policy, the capabilities of cached credentials and stored logins (auto-login) should be revisited for such devices

(including other mobile platforms) as to viability in regards to increasing potential system and service compromise due to alternative security architecture choices from manufacturers and service providers.

In a paper from MIT, there are several scenarios discussed that potentially could compromise the Chromebook, even with a number of the built-in protections enabled, either through deliberate design, or the lack of mitigations that could prevent such vulnerabilities. As noted above, the system will check the validity of system components and applications against known good hashes and copies, but if the application or system is compromised while running, these checks are not done again until the system is rebooted, and therefore can suffer from an in-place attack. Another real and potential exploit of the trust system built into the architecture, is a "backup replay attack", which in essence is restoration of a known good kernel or binary to a previous version, but one that has a known vulnerability, and utilize that vulnerable module to gain access to the system, effectively gaming the verification process. Finally, an attack that seems to be prevalent on any mobile systems, and has been highlighted in risk assessments of multiple platforms for the ***** Office of the CIO, of which is the switch to "developer mode" which provides a low level access to the system and allows for the running of self-signed code on the device for a short period of time, creating yet another avenue for exploitation by a potential attacker.

Finally, as these devices are initially designed to not store large amounts of local data, the local stored data, whether purposely cached for faster access, local manipulation off-line, or manually stored, the consideration for strong encryption and protection of this information is vitally important. Under analysis, while Google claims "always on" encryption, it has been observed that not all user data may be effectively encrypted. However, the user directories are individually encrypted and separated, and in turn, would prevent multiple users from accessing individually stored data for other users of the system. The current, and preferred method of managing user-based keys is to leverage the system TPM for the key store, using it to create a system bound key that ties the data and sessions to the current Chromebook device, and only that device. so even if the data, as encrypted, is stolen, will most likely never be decrypted due to the initial keying procedure and uniqueness of the TPM configuration on that system. For session-based data access on the device, the keyset developed for that user activity is also stored in the TPM for both on-line and off-line access, but is cleared and reset upon reboots (which, as noted above, ensures the impermanence of certain data that could potentially harm the booted system).

6 Mitigations

In many cases, most of the risks on mobile platforms are solutions addressed by policy, proper management and configuration, monitoring, and user education. Some post acquisition policy development and configuration technical guidelines will need developed by the supporting organization for whom the maintenance and upkeep of Chromebooks falls under. Much can be pulled from existing technical and policy guidelines, as ones for mobile systems have been developed, as well as those for UNIX-based systems, more specifically, Linux, which serves as a core for Chrome OS, which runs on these devices.

The other possible threat and risk mitigations occur when using the models already developed for securely developing and accessing web-based applications. These include having a browser that strictly adheres to the document object model (DOM) and is developed to resist many web application attacks such as cross-site scripting (XSS), malicious JavaScript and injection attacks. In certain cases, where

required by law, regulation or policy, the system can be configured to utilize a "sanitizing" proxy before allowing access to external services, either advertised as an external service in ***** DMZ specifically for use by mobile users, but also through mandatory VPN access to adhere with possible TIC (Trusted Internet Connection) requirements.

The Chrome OS, and more specifically the firmware which runs on the hardware, has a secure boot model that ensures that patches and updates are not tampered with and, in sequence, are the ones executed and loaded in the right order for booting the system and running of the end user applications. Many of the potential risks identified in the MIT paper can be mitigated to a point by regular reboots and instantiation of the integrity checks on start up. For the developer mode situation, as switching to the configuration actually requires the flipping of a physical switch located behind the battery compartment, of which, to prevent that, can be disabled through potting or glue. If switched to the developer mode, the OS and device displays several screens and requires confirmation of the boot mode, as well as erasing user partitions, so the data that would be exposed, if compromised while in this setting, would be that which is generated during that developer session.

7 Summary

Chromebooks and their similar brethren, ultrabooks, fill and interesting and expanding niche within the computing ecosystem, namely those who are looking at an economical, lightweight and mobile, always connected computing device that you can realistically do a days worth of office work on. There are a number of assumptions a potential user/owner must make before acquiring and using the device, which is to ensure that it will effectively operate in the environment they plan to be in, that all of their duties can be performed satisfactorily with cloud-based services and systems, and that the device will still contain some limitations that will need to be adjusted for.

Some of the greatest concerns for system security revolve around configuration of the device, transport security for data, and the data storage and access policies and techniques on cloud-based services that the Chromebook is required to utilize. Further issues revolve around required management strategies for initial provisioning and ongoing maintenance of the systems, as they too, are based on a cloud service and OS maintained by an external vendor. These potential concerns could adjust the overall costs of ownership of these devices over a subjective period of time, and when evaluating the acquisition and placement of these technologies into the hands of user, should ultimately be factored in.

8 Conclusion

Currently there are plenty of applications within ***** that can be use cases for ultrabook-like devices such as the Chromebook. Ensuring that the use of them does not become the strict provenance of executives and senior management may offer a democratizing effect on the workforce and the ability for information to reach and be used by a larger portion of the *****workforce. The recommendation is for an investigative "use group" to be developed and consist of members of the suggested use case examples with a structured "goal orientated" test harness to be developed to ensure that the technology will adequately answer the proposed questions and suit the needs of each scenario. Open ended feedback should also be collected and reviewed, as well as an in-depth security risk analysis be completed in order to ensure that the operations model will adhere to FISMA requirements, NIST guidelines and best practices for information and physical security for these types of technologies.

9 Appendix

9.1 References

Wikipedia : Chromebook - http://en.wikipedia.org/wiki/Chromebook

Google : ChromeOS - http://www.chromium.org/chromium-os

Google : ChromiumOS Security - http://www.youtube.com/watch?v=A9WVmNfgjtQ

Google : Chromebook Security - Browsing More Securely - http://chrome.blogspot.com/2011/07/chromebook-security-browsing-more.html

Google : Chromebook Overview - http://www.google.com/intl/en/chrome/devices/chromebooks.html

Google : Browser Security Handbook - Part 2 - https://code.google.com/p/browsersec/wiki/Part2

OWASP Top Ten Project (Web Security Flaws) - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Massachusetts Institute of Technology : "Security of Google Chromebook" - http://dhanus.mit.edu/docs/ChromeOSSecurity.pdf

CVE Details : Google Chromebook (CR-48 reference model) - http://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-21137/Google-Cr-48-Chromebook.html

CVE Details : Google Chrome OS - http://www.cvedetails.com/product/20320/Google-Chrome-Os.html?vendor_id=1224

CVE Details : Google Chrome - http://www.cvedetails.com/product/15031/Google-Chrome.html?vendor_id=1224

SearchSecurty : "Assessing Google Chrome extension flaws and Chromebook security" - http://searchsecurity.techtarget.com/answer/AssessingGoogle-Chrome-extension-flaws-and-Chromebook-security

SearchSecurity : "Exploring Google Chromebook security for the enterprise" - http://searchsecurity.techtarget.com/tip/Exploring-Google-Chromebook-security-for-the-enterprise

9.2 Models

Samsung Chromebook - http://www.google.com/intl/en/chrome/devices/samsung-chromebook.html#ss-cb

- $249 (WiFi)
- $329 (3G)
- 11.6'' display
- 0.7 inches thin and 2.4 lbs
- Over 6.5 hours of battery
- Boots up in less than 10 seconds
- Samsung Exynos 5 Dual Processor
- 100 GB Google Drive Cloud Storage with 16GB Solid State Drive
- Built-in dual band Wi-Fi 802.11 a/b/g/n
- VGA Camera

- 1x USB 3.0, 1x USB 2.0
- HDMI Port
- Bluetooth 3.0™ Compatible

Acer C7 Chromebook - http://www.google.com/intl/en/chrome/devices/acer-c7-chromebook.html#ac-c7

- $199
- 11.6'' display
- 1 inch thin and 3 pounds
- 4 hours of battery
- Boots up in less than 20 seconds
- Dual-core Intel® Celeron® Processor
- 100 GB Google Drive Cloud Storage with 16GB SSD
- Dual band Wi-Fi 802.11 a/b/g/n and 10/100/Gigabit Ethernet
- HD Camera
- 3x USB 2.0
- 1x HDMI Port, 1x VGA port
- 2-in-1 memory card slot (SD, MMC)

HP Pavillion Chromebook - http://www.google.com/intl/en/chrome/devices/hp-pavilion-chromebook.html#hp-pav

- $329
- 14'' display
- 0.83 inch thin and 3.96 pounds
- 4.25 hours of battery
- Boots up in less than 10 seconds
- 100 GB Google Drive Cloud Storage with 16GB Solid State Drive
- Built-in dual band Wi-Fi 802.11 a/b/g/n and Ethernet
- HD Camera
- 3x USB 2.0
- HDMI Port
- 2-in-1 memory card slot (SD, MMC)
- Bluetooth 3.0™ Compatible
- Kensington™ key lock compatible

Chromebook Pixel - http://www.google.com/intl/en/chrome/devices/chromebook-pixel/

- $1299 (WiFi)
- $1449 (LTE)
- 12.85'' high res display (2560x1700)
- Multi-touch glass screen
- 0.64'' thin and 3.3 lbs
- Machined, full metal enclosure
- 1TB Google Drive, free for 3 years
- LTE built-in (optional)
- 12.85" display with a 3:2 aspect ratio
- Multi-touch screen

- Backlit Chrome keyboard
- Fully clickable, etched-glass trackpad
- HD Webcam
- 2 x USB 2.0
- mini display port
- 2-in-1 card reader supporting: SD, MMC
- Intel® Core™ i5 Processor (Dual Core 1.8GHz)
- Intel® HD Graphics 4000 (Integrated)
- 4 GB DDR3 RAM
- 32 GB Solid State Drive*
- Headphone/microphone jack
- Built-in microphone array
- Integrated DSP for noise cancellation
- Powerful speakers tuned for clarity
- Dual-band WiFi 802.11 a/b/g/n 2x2
- Bluetooth 3.0™

Samsung Chromebook 550 - http://www.google.com/intl/en/chrome/devices/chromebook-samsung-550.html#ss-550

- $449
- 12.1'' display
- Less than 1 inch thin and 3.3 pounds
- Over 6 hours of battery
- Boots up in less than 8 seconds
- Optional 3G
- Dual-core Intel® Celeron® processor
- 4 GB RAM
- 100 GB Google Drive Cloud Storage with 16GB Solid State Drive
- Built-in dual band Wi-Fi 802.11 a/b/g/n, Gigabit Ethernet, and 3G modem (optional)
- HD Camera
- 2 USB 2.0 ports
- 4-in-1 memory card slot
- DisplayPort++ Output (compatible with HDMI, DVI, VGA)
- Kensington™ key lock compatible