Evaluation of ChromeOS in Schools from an Information Security Management Perspective

Jonathan Fortune

ICTN 6823
Dr. Phil Lunsford
July 23, 2015

Abstract

In the last 25 years the K-12 public education system in the United States has seen a dramatic shift in its use of technology in the classroom. Both school districts and individual schools are increasingly faced with the decision about what kind of technology will be used inside, and in some cases, outside the classroom. Schools are increasingly seeking the goal of 1:1 technology, meaning that there is a device for each student in the school. This along with, in many cases, significant resources allocated for purchasing devices such as Title 1 funding for low-income schools, has resulted in an unprecedented increase in the amount of personal devices within public schools.

As such, schools are increasingly faced with the challenge of deciding which devices should be purchased, how to deploy these devices in the school environment, and how to effectively manage these devices. Unfortunately the speed at which this process has happened and continues to happen coupled with other limitations schools face such as a lack of technological knowledge with key decision makers, under-qualified and over-worked technology staff, lack of staff devoted to managing significant numbers of devices, etc. can result in information security being one of the last priorities of a school system.

In light of these significant challenges of the public school environment, this paper will evaluate the information security and management issues associated with Chromebooks using the ChromeOS. The paper will show the positives and negatives the Chromebook experience from an information security management perspective especially with reference to using Chromebooks in the school organization environment.

The Hardware and Software Security of the Chromebook/ChromeOS

Given that Google's Chromebook is not the same thing as traditional laptops, it is important to understand the unique security features built into the Chromebook. To begin with, according the Google (2011), there is two part hardware method of security consisting of "a custom firmware chip and a Trusted Platform Module" (Google, 2011). Chromebook firmware contains a custom chip which contains both a read-only and a read-write firmware. The read-write part of the firmware can be updated while the read-only part cannot. This allows a "verified boot" to occur where, upon pressing the power button, the Chromebook "uses an embedded 8192-bit RSA public key to verify the cryptographic signature on the read-write firmware" (Google 2011). After this happens, the read-write firmware verifies that the OS kernel is correct and will continue verifying that everything is correct as is loads the software. The purpose of this process is to ensure nothing has modified that system code (Google, 2011). To go along with this verification process, Chromebooks make sure that outdated signatures are not used by using non-volatile memory in the trusted platform module (Google, 2011).

In the event that the above protection is somehow not enough to prevent security breaches and malicious software is somehow put into a Chromebook, the Chromebook also implements another level of protection. As Kurt Marko notes, if this happens, Google has implemented a recovery mode that allows the user to plug in a recovery device into the USB port to recover the Chromebook back to its original, clean state (Marko, 2011).

This hardware security is of course coupled with what is standard for mobile browsers: app sandboxing, the standard Chrome browser app sandboxing and creating "barriers to cross-site scripting attacks" which are already a part of other mobile browsers as well (Marko 2011). By

running web apps in a sandbox within the Chrome browser, each app's memory and threads are kept separate which results in “preventing a malicious web app from accessing information or taking control of other apps” (Infante, 2014).

In light of these measures to keep the Chromebook secure, it is important to look at whether this technology really is a secure platform, especially as it relates to being used in the public school system environment. When all of these features have been evaluated, it has led many to laud the Chromebook as a near paragon of security. For example, Ifante writes that these features combined contribute ChromeOS being “one of the most secure operating systems in the word” (Infante, 2014). Indeed in making the comparison to the other major operating systems of Wndows, Linux, and OSX, he explains that the ChromeOS is significantly more secure than all of those (Infante, 2014).

When evaluating the ChromeOS for use in large educational settings, this information is surely a great benefit from an information security standpoint. It is of course imperative that a school organization seek to keep the hardware and software of student devices as secure as possible given their constraints. Also, given the low cost of Chromebooks compared to other alternatives such as Windows or OSX laptops and IOS Ipads, schools have a myriad of reasons to choose Chromebooks for their students.

With all of the seeming benefits of Chromebooks from a security standpoint, there might be an appearance that Chromebooks leave little security risks for the K-12 environment. However, as is often the case with security issues, this is not the complete story. Many have noted a number of less obvious security issues that nonetheless should be a part of the consideration from information security management standpoint.

The first potential network security issue relates to ChromeOS's reliance upon the sandbox.

While sandboxing application processes is certainly a positive measure, some have warned that this is not a fool-proof security measure. Infante notes that not only is this method of security largely unproven, there have also been a number of examples of sandboxing that have indeed been exploited for malicious purposes (Infante, 2014). Indeed he quotes security analyst Rik Ferguson who explains that there have already been exploits on other platforms that demonstrated that breaking out of sandboxing environments is indeed possible (Ferguson, 2011). This has been seen on Java, Google Android, Internet Explorer and the Chrome browser itself (Ferguson, 2011). While he admits that it is an effective method of protection, it is not perfect (Ferguson, 2011). Moreover, the WebGL 3D technology that is supported in the ChromeOS has been noted to allow for the possibility of serious risks to the security of the sandbox (Infante, 2014). This Is such a security concern that Microsoft itself is not implementing support for WebGL because they believe it may expose the user to malicious targeted attacks (Infante, 2014).

The potential for sandboxing to be vulnerable to attacks is not the only potential security issue with Chromebooks. Google also allows native apps to run on the Chromebook by way of browser extensions. Using this technology it would be potentially possible to install adware and software that might steal passwords (Infante, 2014). This is mitigated by the fact that all extensions must be approved by Google before they can get into the ChromeOS. However, this still leaves a potential vulnerability. To add to this, Google plans to allow native code to run on the Chromebook in the form of supporting apps that were originally designed to run on Google's Android OS which could potentially lead to more pernicious security issues with Chromebooks in the future (Infante, 2014).

The Cloud Environment and Security of the Chromebook/ChromeOS

These security issues with the Chromebook hardware and software are certainly worthy of consideration from the standpoint of managing security in a K-12 environment. But perhaps even more pernicious than the vulnerabilities in the hardware and software of the machine is the way in which Chromebooks encourage the use of using the cloud. In many ways what separates the Chromebook from other options such as Windows laptops, Mac laptops, Ipads, or Andoid tablets is its reliance on the cloud for storage and computing. By its very design of providing only the Chrome browser interface for the user, the Chromebook is set up so that both computing and information storage is all done in the cloud. For example, students writing a paper for class might open up the Google Chrome browser, navigate to Google Docs, begin writing, and save their document within Google Docs which saves it to their cloud Google Drive storage. So, no information is stored locally. Indeed, even a user's bookmarks and settings are stored in Google's cloud.

The result of the way the Chromebook is designed is that there is an almost full reliance upon the cloud for nearly each and everything that can be done on the Chromebook. This method of computing presents a number of security issues. Obviously issues with the cloud are not direct critiques against the direct security of Chromebooks themselves. However, because Chromebooks encourage a way of operating a computing device that puts computing almost exclusively in the cloud, from an information security management standpoint this is certainly an issue.

As the Chromebook ecosystem revolves around using Google products such as Google Drive, Google Docs, Gmail, Google Classroom, etc., the security of Googles cloud services must be examined. While it is in their best interest to keep their cloud storage secure, the leaked government documents released by Edward Snowden revealed, for example, that the NSA targeted and sought to exploit Google's infrastructure (Gallagher, 2013). Furthermore, the leaked documents showed that

one potential way to bypass Google's security and gain access to data, such as passwords, was to impersonate a secure SSL certificate in order to intercept SSL traffic (Gallagher, 2013). This could, in effect, allow the government to be able to read a user's emails, documents, etc. (Gallagher, 2013). Gallagher points out that this is a weakness of a platform that, by its very nature, has the user put his or her information in the cloud (Gallagher, 2013). While the possibility for the U.S. government to actually target the educational data of school children is extremely low, the fact that the U.S. government may have the ability to do so means that there are others who also might gain and use this ability for nefarious means.

Along with data stored on Google's servers being potentially vulnerable, the idea of promoting an almost exclusive use of cloud apps means that other sites that teachers might use for education, might be even more vulnerable to security risks. In the education sector, there are a number of examples of this. Upon examination, Software engineer Tony Porterfield found that the extremely popular educational cloud app Raz-Kids.com transmitted student's passwords over the internet with no encryption (Singer, 2015). In this particular instance, the site collects student's names, voice recordings, and skill levels (Singer, 2015). Another example is the classroom management software ClassDojo. About one-third of U.S. schools have teachers who use this software (Singer, 2015). This software includes names and behavioral issues for individual students. This site was also transmitting this private data about students insecurely over the internet until they were approached about the issue which they have since corrected (Singer, 2015). While these are just some of the examples, indeed the security risks within the industry of online educational software are indeed quite high as many educational software providers are failing to enact security which would keep student's sensitive data protected from potential threats (Singer, 2015). This

private information leaves students in a potentially dangerous situation as it could set them up for identity theft, cyberbullying, etc. While these security issues related to cloud-based educational apps cannot be said to be the fault of the Chromebook itself, they are certainly issues that anyone managing the information security in an educational environment should consider when deciding on devices for that environment. This is especially true given the Chromebook's reliance upon the cloud. If cloud data is not secure, then it is important to understand the potential risks of using a platform that is so heavily reliant upon the cloud.

The Benefits of using Chromebooks in an Educational Environment from an Information Security Management Perspective

Having evaluated the hardware and software security issues as well as the cloud computing issues involved with using the Chromebook in an educational environment, the benefits of using such a device need to be acknowledged. This paper has indeed argued that there are very real and serious issues related to such things as the Chromebook's sandboxing security being potentially vulnerable to attacks. Moreover, the ability to run native code on a Chromebook also introduces an area of vulnerability. Furthermore, the idea of pushing computing to the cloud for students also poses risks for keeping private student information secure. However, these potential risks must be kept in perspective.

Despite these potential security risks, the Chromebook platform is still a highly secure environment. Indeed, as mentioned above, from a hardware and software perspective, Infante explains that it is “leaps and bounds more secure” than basically every operating system (Infante, 2014). The issues that do present risks illustrate not that the Chromebook is insecure but rather that no platform is perfectly secure and those in information security management need to always be

vigilant in protecting their digital environment. The risks involved with using a Chromebook in an educational environment would also be the same risks involved with using other platforms but indeed the risk is less with the Chromebook. There is of course no way to eliminate all risks but the Chromebook provides one of the safest platforms for a K-12 educational setting.

To go along with the relative security of the Chrombook platform, from a management perspective, keeping the Chromebook secure is much easier than other alternatives. For example, as opposed to management of mass amounts of devices through physically connecting cats to a computer, Google's management solution can be done entirely through the cloud (Google, n.d.). Through the cloud over 200 security policies can be setup with the touch of a button and updated instantly across thousands of devices. As opposed to traditional laptop deployment which consists of imaging, often taking up valuable hours from an often overworked and underpaid IT department, Chromebooks need no imaging and update automatically. Furthermore, to ensure security, Google has added the ability to remotely disable a Chromebook directly from their web based management console (Moscaritolo, 2015). This is especially beneficial when managing hundreds or thousands of devices in a school environment as it eliminates the motivation for an unscrupulous student to steal one of the Chromebooks. If a student were to do this, the Chromebook administrator would then remotely disable the Chromebook rendering it useless.

These benefits of using Chromebooks in an educational environment have resulted in a significant increase in their adoption in this setting. As of 2014, Chromebooks were outselling Ipads in the education market and now make up nearly 50% of the educational computing market (Forrest, 2014). This is due to both price as well as the decreased amount of labor needed to manage the devices (Forrest, 2014).

In conclusion, this paper has evaluated the security of the Chromebook from a software and hardware perspective along with the potential issues involved with using a cloud-centered platform. From an information security management perspective, it has been shown that, while those in charge of information security management must remain vigilant when using any platform, including the Chromebook, in many ways the Chromebook has many security benefits that make the Chromebook a viable option for mass roll-outs in schools that are increasingly seeking to increase their use of technology.

References

Andre Infante. (2014, August 30). 3 Reasons Why Chromebook Does Not Solve Digital Security Issues. *Makeuseof*. Retrieved from http://www.makeuseof.com/tag/3-reasons-chromebook-solve-digital-security-issues/

Angela Moscaritolo. (2015, February 6). Google Adds Remote Chromebook Disabling for Admins. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,2817,2476409,00.asp

Google. (2011, July 29). Chromebook security: browsing more securely. *Google Chrome Blog*. Retrieved from http://chrome.blogspot.com/2011/07/chromebook-security-browsing-more.html

Conner Forrest. (2014, December 3). Chromebooks leapfrog iPads in US education market for first time, here's why. *Tech Republic*. Retrieved from http://www.techrepublic.com/article/chromebooks-leapfrog-ipads-in-us-education-market-for-first-time-heres-why/

Google. (2011, July 29). Chromebook security: browsing more securely. *Google Chrome Blog*. Retrieved from http://chrome.blogspot.com/2011/07/chromebook-security-browsing-more.html

Google. (n.d.). Googl for Education: Products. *Google*. Retrieved from https://www.google.com/edu/products/devices/

Kurt Marko. (2011, August 1). What Can Chromebook Teach Us About Mobile Security? *Information Week*. Retrieved from http://www.informationweek.com/mobile/what-can-chromebook-teach-us-about-mobile-security/d/d-id/1099293?

Natasha Singer. (2015, February 8). Uncovering Security Flaws in Digital Education Products for Schoolchildren. *New York Times*. Retrieved from http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html

Rik Ferguson. (2011, May 25). So secure we don't need security? *Trend Micro*. Retrieved from http://countermeasures.trendmicro.eu/so-secure-we-dont-need-security/

Ryan Gallagher. (2013, September 9). New Snowden Documents Show NSA Deemed Google Networks a "Target". *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html

Sean Gallagher. (2013, September 11). Why the NSA loves Google's Chromebook. *Ars Technica*. Retrieved from http://arstechnica.com/information-technology/2013/09/why-the-nsa-loves-googles-chromebook/