Chromium GSoC Contributor Proposal (Safety Erase project)

Summary
Self link:
Chromium GSoC Proposal - Sa...

This project proposal is aimed towards implementing safety erase of internal storage of Chromebooks in the powerwashing process in a way that is compliant to the NIST 800-88 guidelines.

Owner: ema@iaccarino.dev
Contributors:
Approver: gwendal, torsha
Status: Submitted
Created: 20/03/2024

Project Abstract

Currently Chromebooks encrypt all user data safely, and they get “erased” by simply erasing the vault containing the encryption key, making the data unreadable. While this is definitely a way to achieve the end goal of making user data unintelligible after the user decided to erase their device, it is not compliant with the current state of the art guidelines on media sanitization defined by NIST.

The goal of this project is extending the current method for device safety erase, proposing a way to safely erase data from a Chromebook’s internal storage based on sanitize commands and compliant with the NIST 800-88 Guidelines for media sanitization. This method will also be used during the ChromiumOS powerwashing process.

Background

The first necessary step is a deep dive in the ChromiumOS documentation for developers as a way to understand more about the power washing process and how data erasure currently works. The ChromiumOS Design Docs provide an in-depth explanation about the powerwashing process, available here. Furthermore, we can explore Chromium's bug reports to find more details about the task at hand, starting from the starter bug mentioned in the Project Ideas slide for the project, as the comments on that specific issue include some commits and pointers towards the interested parts of the codebase and description of how the system currently works and some implementation ideas, which show that the required background includes an understanding of ramdisks as well, so we can restore the data we want to preserve after the erasure is completed. Furthermore, it is necessary to read and understand the NIST 800-88 guidelines for media sanitization. These guidelines define three methods for media sanitization: Clear, Purge and Destroy and their specifications. The last one is

not interesting to us, as per those guidelines it involves physically destroying devices so the data is irreversibly erased.

Design Ideas

As mentioned by one of the mentors (Gwendal@) in one of the Chromium issues related to this project, there is already a starting solution for this problem in the form of multiple bash scripts that currently runs from an USB device through chroot from recovery mode, available at this commit: *https://chromium.googlesource.com/chromiumos/platform2/+/e3eb987d34149a73923f7a5b79c8e4a6e12f048d*

The technologies that are going to be used for the project are::

- C++ for the code that will land in the OS codebase and the related unit tests
- Bash for init scripts and for understanding the current state of the art

The solution currently proposed by the mentor is to initialize a ramdisk which is going to store the information we want to retain, proceed with the safety erase, in a similar methodology as the one currently applied in the scripts that are linked in the commit above, and then proceed to restore the device state with the data we deemed important by moving it back from the ramdisk to the internal storage.

The main information security concerns that arise with this project are mostly related to the safety of the erasing process (e.g. is the data correctly erased?) and the compliance to the NIST 800-88 guidelines.

As per the current state of the ChromiumOS codebase, all the code that will land in the OS will have unit and integration tests to ensure for a successful development.

Code Affected

From my understanding, the portions of code that would be affected are:

- Clobber: https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/init/clobber/
- Upstart/init scripts: https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/init/
- The state of the art solution that's currently available for safety erase: https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/secure-wipe
- Code that handles operations involving ramdisk devices can be found at: https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/libstorage

/storage_container/ramdisk_device.cc

Pre proposal Work

I have successfully cloned the ChromiumOS repository on my computer and followed the instructions for a build. My understanding of the things to do during the project is:

- The scripts that are currently available scripts for safe device wipe need to be turned into something that can be launched straight from device rather than from an external drive.
- A ramdisk will be created before the wiping process to save data that we are going to persist after the wipe, including a script that will be responsible for restoring the preserved data before destroying the ramdisk.
- Once the powerwashing process is completed, we expect the user to have a completely wiped system except for the data we preserved in the ramdisk.

The process for wiping a disk varies depending on the storage media used, so we have to accurately detect what type of storage the user is utilizing (SATA/NVMe/eMMC), as we can see from https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/secure-wipe/secure-wipe.sh
It might also be important to consider which specific version of a device specification we are using. As mentioned in the comment available here https://chromium.googlesource.com/chromiumos/platform2/+/refs/heads/main/secure_erase_file/secure_erase_file.cc#167, the method for Secure Erase that was supported up to eMMC 4.51 is now deprecated in favor of TRIM+SANITIZE.

Schedule of Deliverables (timeline)

May 1 - May 26 (Community Bonding Period)

- Weeks 1-2: Getting confident navigating around the source tree, the documentation and the parts of the codebase that will be impacted by the project.
- Weeks 3-4: Interact with mentors and discuss expectations, requirements (e.g. is our focus the “Clear” method or the “Purge” method? They have different specifications to meet for the method to be deemed compliant), pointers, goals and an initial architecture idea for a solution and its implementation.

May 27 - July 12 (Phase I)

- This primary phase will be mostly focused on understanding how to include in the codebase the creation of a ramdisk and copy of the data we need to preserve.. The solution proposed by Gwendal in comment #30 of a starter bug gives some insight on the process, along with some resources to look up. A first proof-of-concept would be working on this solution and adding up on it, working out any quirks that might arise.

- Weekly sync ups with mentors will be held to ensure the project is heading in the right direction and is being implemented on track.

July 12 - August 12 (Phase II)

- The secondary phase will be focused on integrating the scripts into the powerwashing process when it is initiated from the device itself.
- During this phase, testing of the proposed solution will be performed on a physical Chromebook.
- Furthermore, the documentation for the code that is going to get shipped will be written and reviewed in collaboration with the mentors.
- Weekly sync ups with mentors will be held to ensure the project is heading in the right direction and is being implemented on track.

A one-week buffer period (from **August 12th** to **August 19th**) has been allocated for any inconveniences that might arise during the project development.

Communications

- Timezone/ Working hours: UTC+1, can allocate from 9:00 AM to 5:00 PM with some small regular breaks to the project during Mon-Fri. This schedule is only set to show a commitment of around 8 hrs a day, and is completely flexible should there be a need to cooperate/have meetings with people based in other timezones.
- Email: ema@iaccarino.dev
- Phone: Ideally I would love to communicate with the mentors hosting a weekly catch up on Google Meet, since the platform allows for screen sharing which would help a lot when discussing programming or doubts about the project.
- Slack, IRC ids: I am flexible on the platform used for communication with mentors, I can use Discord, Teams, IRC or Slack.

About Me

My name is Emanuele Iaccarino and I am currently a M.Sc. in Computer Science student at University of Salerno. I have successfully completed a Bachelor's Degree in Computer Science in October 2023 defending a thesis on using machine learning techniques for the prediction of the exploitability of software vulnerabilities. During this time, I have also managed to get some work experience through an internship as a backend developer at an Italian startup which then turned into a full time employment; in these roles I was responsible for the backend development of a subscription-based platform related to education around cryptocurrency topics. After that, for Summer 2022 I did an internship in Quality Engineering at Apple where I got to learn Swift and End-to-End testing. My interests mostly span through everything concerning information security, as that has been one of my interests since childhood and one of the things that never failed at sparking my curiosity, and I love experimenting with new technologies I have never tried before. Another field that I am interested in is

Operating Systems development, which is why this project has caught my attention. During my education and work experiences, I have gained some experience with Swift, JavaScript/TypeScript, C++, C, Java and Python and Solidity, with a focus towards backend engineering. I have also worked with both SQL (MySQL) and NoSQL (MongoDB) databases, Kafka and Redis. I believe that this very diverse background that I have developed during these years, together with my curiosity towards technologies I do not know in depth, has given me the ability to quickly adapt to new technologies and get up to speed on the stack and technologies used on a specific project . My resume is available at https://iaccarino.dev/public_cv.pdf.

Prior Experience with open source

I am fairly new to the world of open source, although I strongly believe in the impact writing open source software has on the world. This strong belief of mine has lead me to share all of the source code of the projects I am working on for recreational purposes, especially as I believe it might help out people who are trying to learn the same technologies as I am, or trying to solve similar problems as the ones I was tackling at that specific time.
My GitHub is reachable at https://github.com/meelunae.
As a way to get in touch with the process of landing a CL in a Google project, I have filed a PR on the wpt.fyi project, which can be found here and was successfully merged. I have also started working on some small PRs aimed at solving open issues on projects from organizations spotlighted in the Google Summer of Code program that caught my attention (like Fixed Docker container permission denied issue and FEATURE: Defining multiple flags in challenge for CTFd, both merged in the OWASP Juice Shop CTF CLI project), which are available on my GitHub as well.

Why Chromium?

I have chosen Chromium as an org for my Google Summer of Code because I appreciate the contribution Chromium brings to the web ecosystem, but furthermore I am very enthusiastic about the impact Chromebooks and ChromeOS (as a derived product from ChromiumOS) are currently having in making schools and academic institutions less "passive" by enabling a lot of institutions to access devices which allow for collaborative and interactive learning methods. This specific project would help me learn more about low-level development in an Operating System environment, and about Open Source best practices. It would also help me broaden my understanding on safety and data erasure by working on a critical project which requires a very detail oriented approach which I believe I can offer. There are a lot of talented people working on Chromium and its related projects on a daily basis, and this would be a great opportunity to get in touch with them and learn as much as I can from great engineers who work on such a big and impactful project. This is particularly interesting to me because even though I believe that my university course taught me a lot of useful skills, we lack experience when it comes to understanding and confidently navigating big codebases.

Feedback from Chromium

If you read this document please provide your short general feedback in the section below. Please also feel free to make comments above.

Username	Date	Comment