Richtlinie zum „Software-Sprint“

LiViR - Linux-Festplattenverschlüsselung im Ruhezustand

Schlussbericht

Zuwendungsempfänger:

Dittler Meurer GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS19S05 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Notebookfestplatten werden häufig verschlüsselt, um ihre Daten gegen physischen Diebstahl zu schützen. Im Gegensatz zu proprietären Lösungen, funktioniert dies unter Linux bisher nur während das Gerät vollständig heruntergefahren ist. Tatsächlich ist dies bei Notebooks heute selten der Fall. Im Rahmen des Projekts sollte die größte unkommerzielle Linux-Distribution Debian derart erweitert werden, dass auch das einfache Schließen des Notebookdisplays zum Schutz vor physischem Zugriff führt. Nutzer*innen werden dann beim Öffnen des Gerätes erneut nach ihrem Festplattenpasswort gefragt. Dazu waren folgende Meilensteine vorgesehen:

1. Vergleichen der bisherigen (unvollständigen) Lösungen und Kommunikation mit deren Entwickler*innen.
2. Notwendigen Kernel Patch mit den Linux Kernel Entwickler*innen diskutieren und zur Aufnahme in den Debian Linux Kernel vorschlagen.
3. Proof of Concept weiter verfeinern.
4. Ausführliches Testing Dokumentation des Verfahrens und damit einhergehender Risiken
5. Integration der Suspend-Funktion und zugehöriger Konfiguration in Betriebssystem
6. Entwicklung von Plugins, um weitere sensible Daten aus RAM zu löschen (z.B. private SSH/GnuPG Schlüssel)
7. Integration der Konfiguration des suspend-Featuress in Gnome Power Management
8. Vorstellung der Lösung bei Betreuern anderer Linux-Distributionen

Beitrag des Projektes zu den Zielen der Förderinitiative „Software-Sprint“

Mit dem Projekt werden verschieden Ziele des „Software-Sprint“ verbesser. Grundsätzlich wird vor allem die IT-Sicherheit der Nutzer*innen von Debian-basierten Linuxdistributionen verbessert. Ganz konkret, wird die Sicherheit von Nutzer*innen von Linux-Festplattenverschlüsselung verbessert, indem ihre Laptops auch im Ruhezustand geschützt sind. Freie Software wird aus guten Gründen, viel im Bereich der Zivilgesellschaft und des Journalismus eingesetzt. Die Sicherheit dieser Menschen zu erhöhen, halten wir für einen wichtigen Beitrag zu Civic Tech. Des weiteren wurde auch die Softwareinfrastruktur von Debian und Cryptsetup durch unser Projekt verbessert. Projekte, auf die zehntausende von Menschen täglich vertrauen.

Ausführliche Darstellung der Ergebnisse

Wir haben erfolgreich einen funktionierenden Prototypen entwickelt, der auf vielen Systemen zuverlässig funktioniert. Auch haben wir eine Verbesserung im Linux Kernel entwickelt, die nun offiziell aufgenommen und mit dem Release 5.6 des Linux Kernel veröffentlicht wurde. Unser Code läuft somit auf allen aktuellen Linuxcomputern. Die entwickelte Software ist in das offizielle Debian-Pakete für Linux Festplattenverschlüsselung aufgenommen worden, was eines unserer Hauptziele war. Es kann über die offiziellen Debian-Repositories heruntergeladen werden. Aufgrund von Problemen auf mancher Hardware ist das Paket derzeitig noch als „experimentell“ bezeichnet. Wir führen unsere Bemühung Hardwareinkompatibilitäten zu beheben seit dem Ende des Förderzeitraums fort.

Die Projektbegleitung durch die Open Knowledge Foundation hat uns insbesondere bei der organisatorischen und administrativen Arbeit deutlich unterstützt. Auch die zwei in der Projektförderung enthaltenen Coachings (in unserem Fall UI/UX Coachings durch Simply Secure) haben uns stark weiter geholfen. Wichtig war hier vor allem die Planung, welche Funktionalität eine Nutzer*in erwartet, wenn sie unser Paket installiert. Sinnvolle Standardwerte und eine verständliche Anzahl an Einstellungen zu geben war der Schwerpunkt in dieser Beratung. Weiterhin gaben sie uns gute Tipps zur Kommunikation mit der Linux Kernel Community.

Einer breiten Öffentlichkeit wurde unser Projekt am 02.02.2020 durch einen Vortrag auf der FOSDEM 20 vorgestellt. FOSDEM ist die größte Open Source-Messe Europas mit mehr als 8000 Teilnehmer*innen. Es ergaben sich spannende Diskussion über die Integration mit anderen Projekten, welche die physische Sicherheit von Linux-Computern erhöhen.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Zielgruppe waren insbesondere Menschen, die Ihre Daten vor gezielten physikalischen Angriffen schützen müssen - also Journalist*innen, Aktivist*innen, oppositionelle Politiker*innen in aller Welt. Des weiteren profitieren Nutzer*innen von Festplattenverschlüsselung auf Linux-Laptops allgemein, da ihre Daten im Ruhezustand besser geschützt sind. Auch größte Konzerne vertrauen auf die Verschlüsselung mittels Cryptsetup und profitieren letztlich von unserer Entwicklung

Da die Lösung in Debian implementiert wurde, wird sie mittelfristig alle Nutzer*innen von Debian-Derivaten (etwa Ubuntu, Tails, Linux Mint) erreichen, sobald diese auf eine aktuelle Version ihres Betriebssystems aktualisieren. Unsere Software wird bereits zuverlässig auf Ubuntu-Systeme

eingesetzt. Eine Adaption für Qubes OS ist in Diskussion. Dies ist eine völlig neuartige Linuxdistribution mit dem Schwerpunkt auf Sicherheit durch Isolation. Unsere Erwartungen wurden übertroffen, da unsere Arbeit bereits für Fedora adaptiert wurde. Fedora ist die zweite große Linux-Distribution neben Debian, von der sich weitere Distribution ableiten.

Da das Projekt noch nicht ganz abgeschlossen ist, arbeiten wir weiter um den experimentellen Status der Pakete zu entfernen und es in einen breit getesteten, zuverlässigen Zustand zu bekommen. Wie oben geschrieben, handelt es sicher hier um Probleme der Hardwareinkompatibilität, welche immer recht komplex sind.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Im kleinen gab es immer mal wieder Ansätze, die sich später als nicht zielführend raus gestellt haben. Im Großen aber hatten wir von Beginn an eine gute Vorstellung von den nötigen Teilschritten. Während der Entwicklung hatten wir kurzzeitig versucht, nicht nur Debian, sondern alle Systemd-basierten Linuxdistributionen anzuvisieren. Da die Entwickler von Systemd unserer Idee allerdings nicht besonders offen gegenüber waren, mussten wir diesen Plan wieder aufgeben. Systemd hat einen anderen Ansatz gewählt, welcher nur die Home-Laufwerke der Nutzer*innen verschlüsselt, da sie perspektivisch den Rest des Systems unveränderbar machen wollen. Diese Lösung liegt allerdings für Desktopsystem noch in weiter Ferne, während unsere Lösung heute funktioniert.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Unser Projekt inklusive Sourcecode, Problemtracking und Anleitungen findet sich unter https://salsa.debian.org/mejo/cryptsetup-suspend. Anleitungen zur Installation finden sich unter https://salsa.debian.org/mejo/cryptsetup-suspend/-/wikis/home. Weitere Dokumentation wird mit dem Paket „cryptsetup-suspend“ installiert und ist über das Werkzug „man“ abrufbar. Die Folien und das Video der Präsentation des Projekts auf FOSDEM 20 ist unter https://fosdem.org/2020/schedule/event/dip_close_lid_encrypt/ abrufbar.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Wir waren wesentlich länger mit der Kommunikation mit der Linux Kernel Community beschäftigt, als wir eingeplant hatten. Daher war auch unsere Beratung mit Simply Secure stark auf diesen Bereich fokussiert. Dies ist hauptsächlich darauf zurück zu führen, dass wir als Einzelpersonen an diese Community heran getreten sind und nicht durch eine große Firma unterstützt worden, welche die Kernel-Entwicklung mitfinanziert. Letztlich waren wir aber in unserem Projektzeitraum erfolgreich und konnten die zusätzlich notwendig Zeit durch gradlinige Entwicklung wieder gut machen. Hier erwies sich unsere Vertrautheit mit der Codebasis, sowie das gute Durchdenken des prinzipiellen Problem als besonders hilfreich. Die von uns geplanten Arbeitsziele konnten größtenteils erfüllt werden. Nur „7. Integration der Konfiguration des suspend-Features in Gnome Power Management“ musste aus Zeitgründen entfallen. Wir haben uns hier für einen generischen Weg der Konfiguration über eine Konfigurationsdatei entschieden. Die grafische Integration mit Gnome hätte letztlich zu wenig Nutzen für sehr großen Aufwand gebracht. Probleme mit spezieller Hardware waren in unserem Projektplan nicht vorgesehen und müssen daher auch im Nachhinein gelöst werden.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Es gab keine nennenswerten Einflüsse durch andere Institutionen, die den Verlauf des Projekts maßgeblich beeinflusst haben.