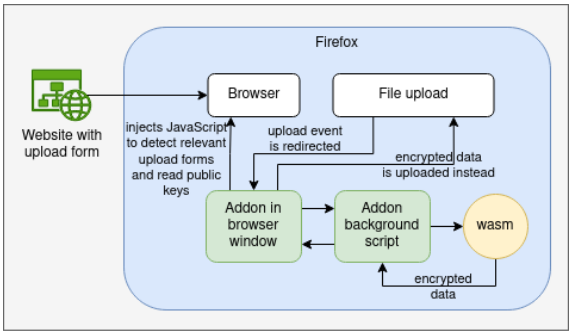
Moderne Verschlüsselung in Web und Mail mit WebAssembly

Vortrag zu den Chemnitzer Linux-Tagen 2022
Dominik Pataky, https://dpataky.eu/acus

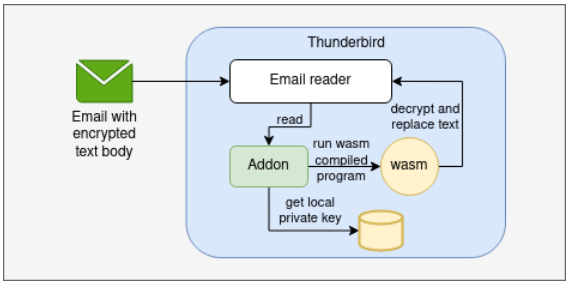
Zusammenfassung
Die Verschlüsselung von Nachrichten und Dateien ist weiterhin ein wichtiges Ziel für mehr vertrauliche Kommunikation im Internet. Jedoch ist der Zugang zu den benötigten Tools nicht immer so einfach. In diesem Projekt untersuchen wir deshalb die Verwendung von modernen Verschlüsselungstools in Browsern und E-Mail-Programmen. Mit Hilfe der neuen WebAssembly-Technologie lassen sich solche Tools, die bisher z. B. nur für das Terminal gedacht waren, in die UI alltäglicher Programme einbinden. Der Vortrag stellt die Idee kurz vor, zeigt, wie dieses Vorhaben in Firefox und Thunderbird aussieht und welche Möglichkeiten sich eröffnen.

Firefox
Für Firefox ist das Addon so gebaut, dass es einerseits ein Script auf Websiten ausführt, welches automatisiert Verschlüsselung von Dateien vornehmen kann. Sobald eine Datei über den Submit-Button hochgeladen werden soll, fängt das Addon diese Aktion ab. Die Datei wird dann durch das wasm-Programm geroutet und erst der verschlüsselte Datensatz wird hochgeladen. Weitere Ideen:



- Ent-/Verschlüsselung von Text in Textfeldern im Browser (Webmail, Kontaktformulare) oder von Chatnachrichten, z. B. innerhalb eines Matrix- oder XMPP-Chatclients in JavaScript
- Automatische Verschlüsselung von Dateien, die über ein Formular hochgeladen werden (in Demo gezeigt)

Thunderbird
In Thunderbird wurde eine automatisierte Entschlüsselung von verschlüsselten E-Mails implementiert. Beim Öffnen einer solchen E-Mail wird der Ciphertext mit dem Cleartext ersetzt. Anwendungsbeispiel: Verschlüsselung von E-Mails an andere sowie Entschlüsselung bei Empfang.



Infos zum Vortrag
Vorkenntnisse in der WebExtension-Entwicklung sind hilfreich für das Verständnis, aber keine Voraussetzung. Das Tool wird anhand einer Demo vorgestellt, der Quelltext wird auf der oben verlinkten Projektseite hinterlegt. Hilfreiche Quellen:

- https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions
- https://developer.thunderbird.net/add-ons/mailextensions
- https://golangbot.com/webassembly-using-go/