Moderne Verschlüsselung in Web und Mail mit WebAssembly

Dominik Pataky

Chemnitzer Linux-Tage 2022

Was auf den folgenden Folien zu finden ist..

1. Ziel des Ganzen

2. Theorie
   - WebAssembly? WASM? WAT? WASI?
   - Aus Go & Rust mach' wasm
   - Verschlüsselung mit age
   - WebExtensions.. MailExtensions..

3. acus
   - Dreimal umrühren, kneten und kleben
   - Der Rest der Eule (Demo)
   - Ausblick

Warum das Ganze?

WebAssembly ermöglicht uns, in C/Go/Rust geschriebene Programme in Addons zu integrieren.

Eine **Re-Implementierung** der Programme in JavaScript ist **nicht notwendig**.

Dies betrifft ganz besonders **Kryptographie** und Hardware-nahe Programme.

WebAssembly? WASM? WAT? WASI?

- WebAssembly: eine portierbare Binärsprache/-schnittstelle für Webbrowser, quasi parallel zu JavaScript (vgl. `asm.js`)
- `.wasm`: kompilierte WebAssembly-Programme
- `.wat`: menschenlesbares Textformat von WebAssembly
- WASI: das "WebAssembly System Interface", quasi ein POSIX für WebAssembly, von Mozilla

Aus Go & Rust mach' wasm

- Ausgangslage ist erstmal ein Go- oder Rust-Programm (oder andere, via LLVM)
- Diese werden **nach WebAssembly kompiliert**
- Über JavaScript-**Gluecode** wird das Binary im Browser geladen und ausgeführt

Binaries im Browser

Im Browser werden somit kompilierte Dateien ausgeführt, deren Code man nicht direkt einsehen kann. Reproduzierbare Builds und offener Quellcode sind daher wichtig

Verschlüsselung mit age

- age ist ein modernes Verschlüsselungsprogramm von Filippo Valsorda (@FiloSottile) und Ben Cartwright-Cox (@Benjojo12) mit ausgereiftem CLI
- „*It's meant to replace the use of gpg for encrypting files, backups, streams, etc.*“
- Super einfach zu bedienen, nutzt ECC mit Curve25519. Beispiel-Keypair:
  `age1fgm483g3att6fg4j0vvye2rcwex9fhftwfxaz02z8ard0zxnypdqnap658` /
  `AGE-SECRET-KEY-1NUZUKCZL87FXD26J0DH72HHHNDM83GM2AQKT6AXFSS4V8L7RJYKQD9ULXH`
- Design ist unter age-encryption.org/v1 als Dokument lesbar
- Code für Go auf github.com/FiloSottile/age und Rust github.com/str4d/rage

WebExtensions.. MailExtensions..

- WebExtension API von Mozilla ist angelehnt an die Chrome API, Kompatiblitität
- Mit Firefox 57 ("Quantum", 2017) Abschaltung von alten XUL Addons
- Gleiches mit Thunderbird 78 (2021)
- → Beide nutzen die gleiche unterliegende Browser-Engine inkl. WebAssembly-API
- Referenz: developer.thunderbird.net

Web- oder MailExtensions?

MailExtensions sind das Pendant zu WebExtensions, jedoch spezifisch für E-Mail-Kontext (zusätzliche APIs, nicht alle Firefox-APIs nutzbar)

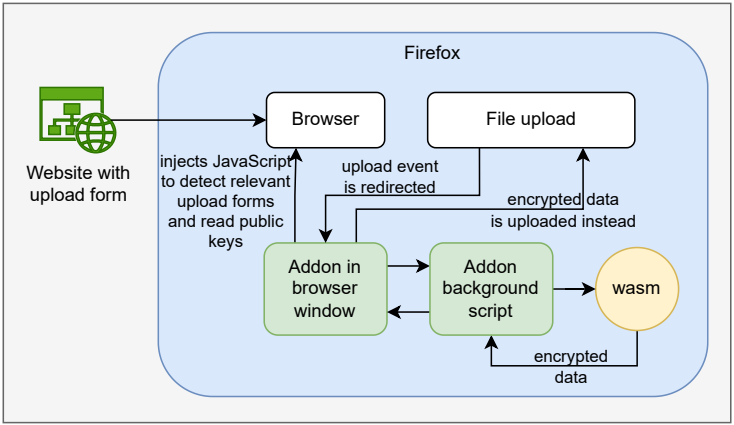
acus Projektidee

- WebAssembly ermöglicht, so wie JavaScript, eine plattformübergreifende Ausführungsumgebung. Definierte Schnittstellen, Sandbox, nativer Code für Performance
- Portabilität von nützlichen Programmen in Web- und Mail-Umgebungen
  → acus: Portierung eines Verschlüsselungsprogramms mit Base64-Output
  → Proof of Concept anhand zweier Szenarien
- Übertragbar auf jede andere Applikation (Beispiel LibreOffice WebAssembly)

POC Workflow in Firefox

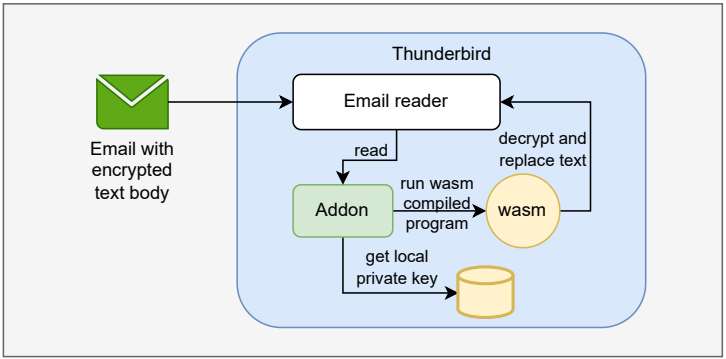
Szenario: nach Installation des Addons werden Uploads vor Übertragung verschlüsselt.

Public-Key ist als `<form>`-Attribut hinterlegt



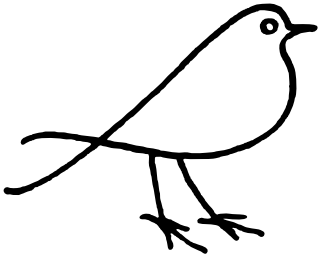
POC Workflow in Thunderbird

Szenario: Es wird eine verschlüsselte E-Mail empfangen. Das Addon erkennt den Base64-Ciphertext, entschlüsselt diesen und ersetzt den Textblock mit Klartext



Der Rest der Eule (Demo)

Code-Repository von acus: codeberg.org/bitkeks/acus



Ausblick

- Weitere Möglichkeiten für **acus im Browser**: Textverschlüsselung vor Absenden, Integration in E-Mail-Webinterface
  → großartige Alternative zu PGP in Browsern und Webmailclients

- **acus in Thunderbird**: Key-Generator, Pubkey im Kontakt speichern, Anhänge verschlüsseln, `.well-known` oder DNS TXT für automatische Schlüsselabfrage

Danke für's Interesse

Projekt-Website auf dpataky.eu/acus

Kontakt mail@dpataky.eu

Code unter freier Software-Lizenz GPLv3, gerne nehmen und weiterentwickeln

Credit for Logo: freesvg.org/line-art-drawing-of-a-bird (Public Domain)

Siehe auch: „Neues Werkzeug für moderne Netzwerksicherheit“ bei den Datenspuren 2019, Vortrag zum Thema nftables und WireGuard