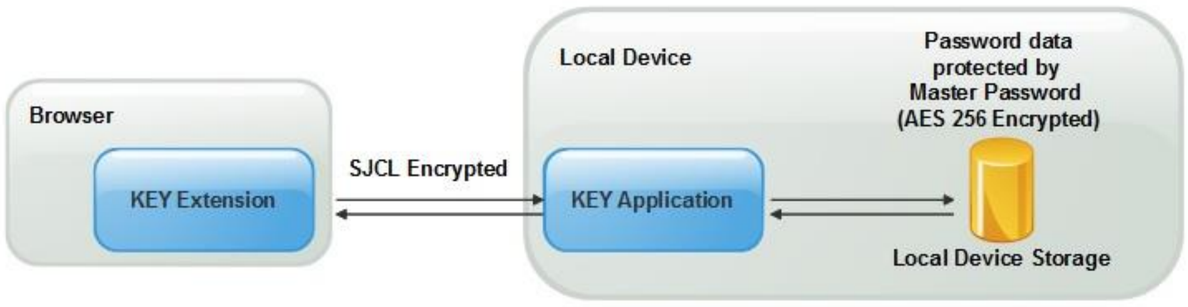
Secure Systems Group, Aalto University

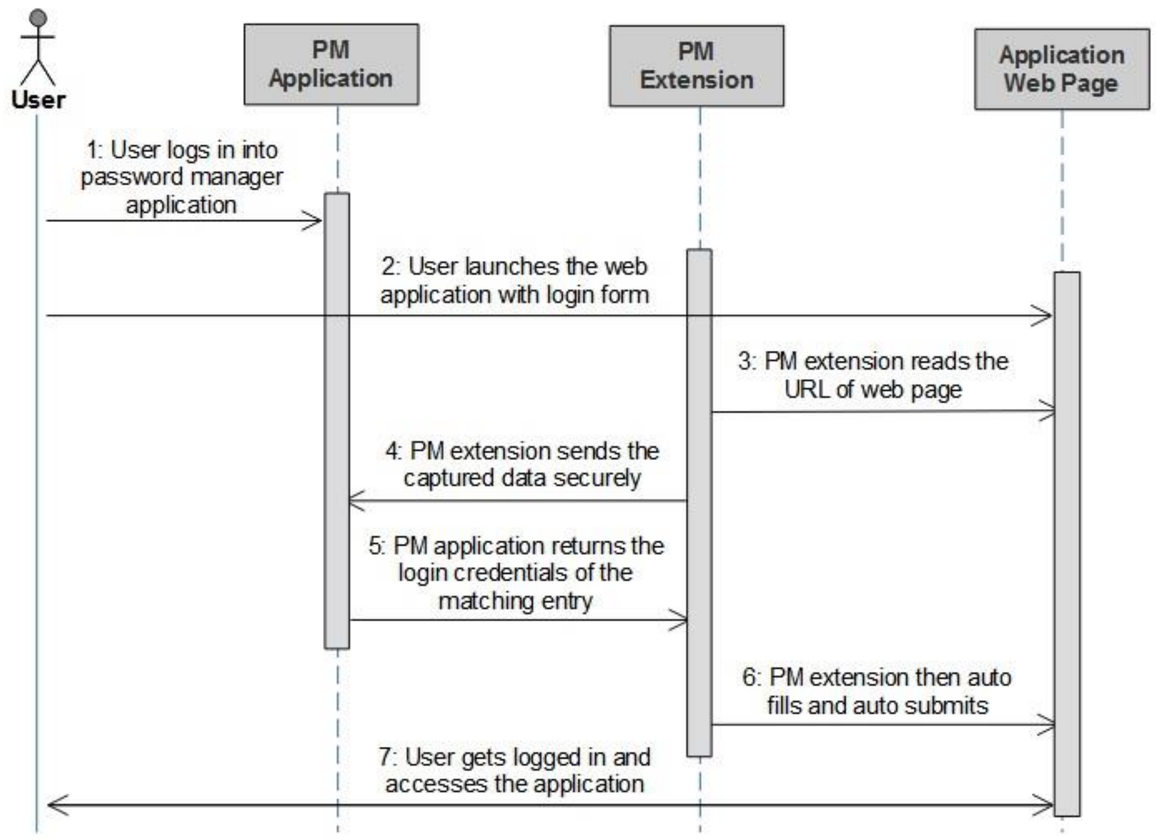
Viswanathan Manihatty Bojan, Thanh Bui, Tuomas Aura

Security Evaluation of Password Manager Browser Extensions

Example: F-Secure KEY

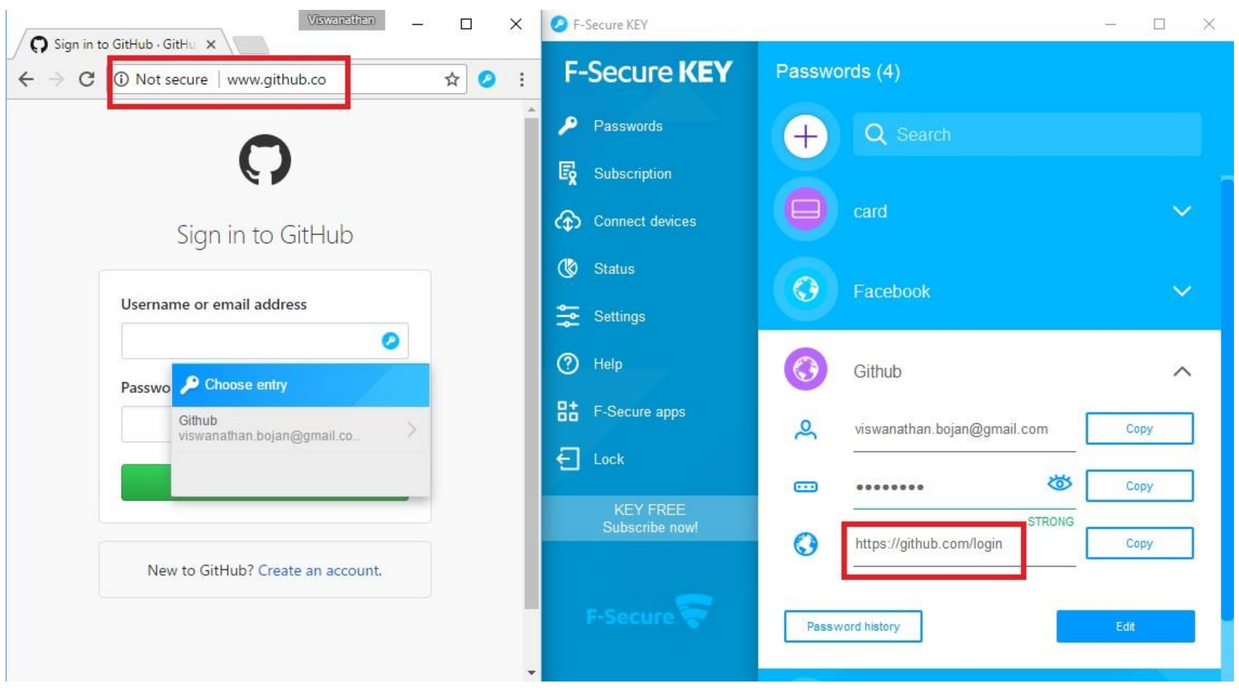


- Secure vault protected by the Master password
- Master Password + PBKDF2 using 20000 iterations → Master Encryption key
- Master Encryption Key + AES-256 + password data in Vault → Secure Storage
- Encrypted password data stored in local device
- Data in transit between the extension and the application is encrypted using SJCL.js



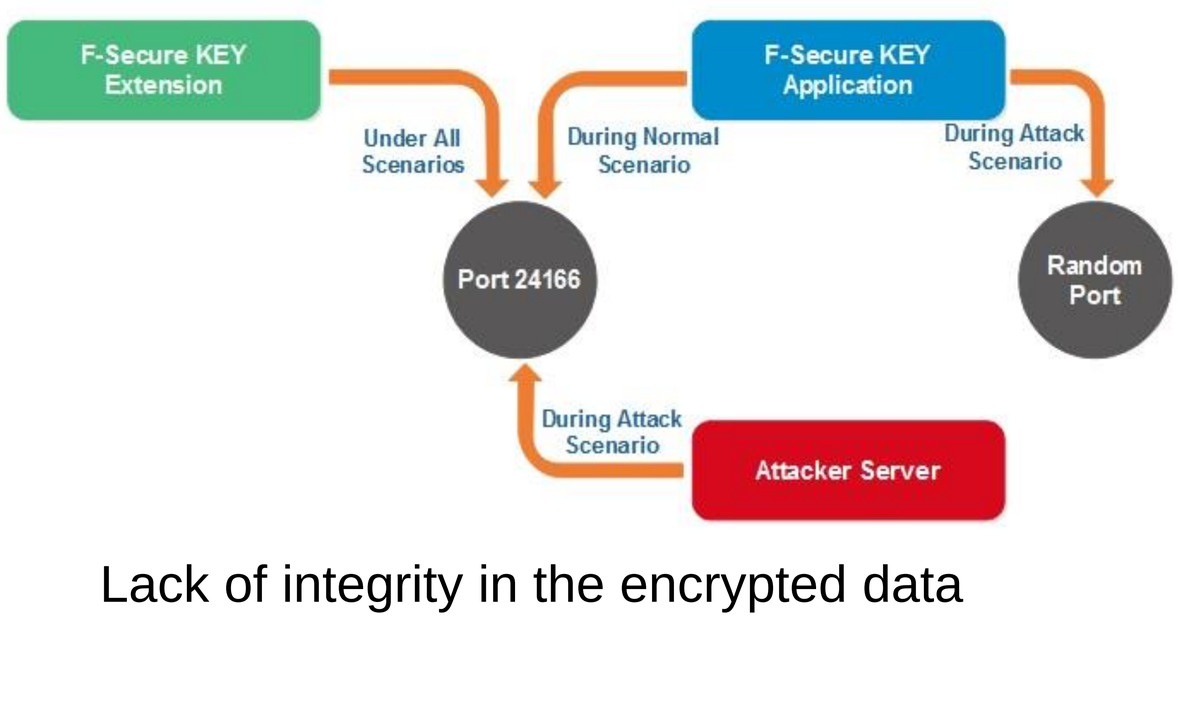
Potential Vulnerabilities

1. Improper Domain Matching



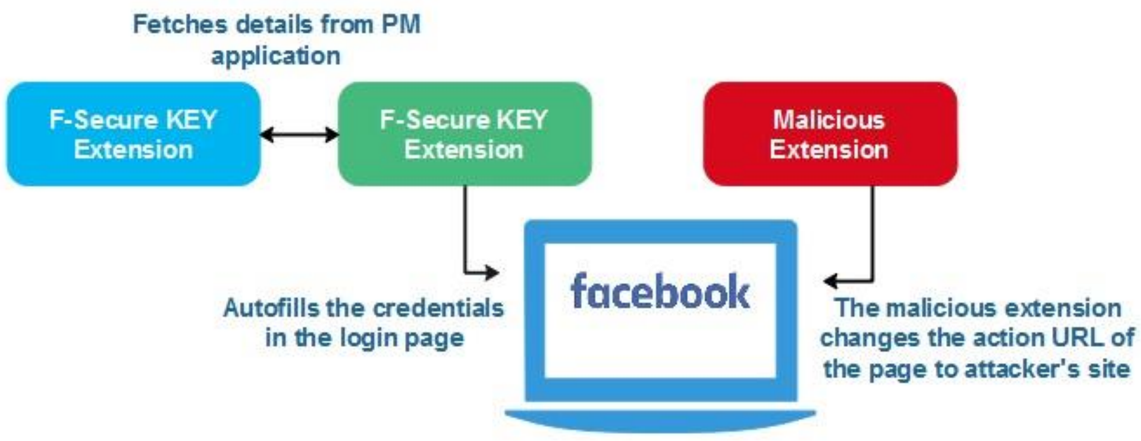
2. Capturing the secret authorization code via clipboard by a malicious application

3. Man-in-the-Middle by a malicious application



Lack of integrity in the encrypted data

4. Unvalidated Redirects by a malicious browser extension



5. Stealing the credentials during form submission by a malicious browser extension

Best Practices for Password Manager applications

- Strict domain matching
- No secret data should be copied to clipboard. Instead use secure pairing for authorization.
- Better validation of the password manager application by the browser extension
- Check the integrity of the encrypted data
- Warn user when there is a change of domain, port or the protocol of the URL at the time of redirection
- Better security model for browser extensions?

Aalto University

Contact: manihav1@aalto.fi, Thanh.bui@aalto.fi, tuomas.aura@aalto.fi

In cooperation with F-Secure, https://www.f-secure.com/en/web/home_global/key