

Review of Master's Thesis

Student: Matějka Jiří, Bc.
Title: GPG Encrypted Web Pages (id 22307)
Reviewer: Pluskal Jan, Ing., DIFS FIT BUT

1. **Assignment complexity** **simple assignment**
Cílem práce je implementovat klientský middleware, který umožní dešifrovat statický i dynamický obsah z DOM webu. Práce nedostatečně osvětluje motivaci a účel použití. Vzhledem k tomu, že zadání je možné splnit s využitím již existujících frameworků/aplikací a jejich propojením, považuji zadání za jednoduché.
2. **Completeness of assignment requirements** **assignment fulfilled**
3. **Length of technical report** **in usual extent**
4. **Presentation level of technical report** **70 p. (C)**
Práce je psaná netradiční formou popisující agilní přístup k vývoji. Tento přístup jasně komunikuje čtenáři jednotlivé funkční požadavky vedoucího a architektonická rozhodnutí autora.

Jednotlivé úvody kapitol neobsahují stručný popis obsahu, což znesnadňuje čitelnost a zavádí moment překvapení pro čtenáře, který neví, co ho v kapitole čeká.
5. **Formal aspects of technical report** **75 p. (C)**
Práce je psaná v anglickém jazyce. Místy jsou patrné stylistické, gramatické prohřešky:
 - překlepy, chybějící mezery, atd.,
 - použití neobvyklých synonym, viz. wealth (sekce 2.1), basic knowledge (kapitola 3),
 - špatné použití osob, viz its (sekce 2.3.1),
 - chybné použití n/m dash,
 - nekonzistentní styl enumerací v úvodech kapitol, viz kapitola 2 a 3,Faktické chyby:
 - tvrzení o použití privátního klíče odesílatele pro ověření podpisu zprávy příjemcem - bod 6, druhé enumerace v sekci 2.2.
 - sekce 2.3.2 - Signing Data, listing - použití parametru --encrypt místo --sign
6. **Literature usage** **60 p. (D)**
Práce obsahuje poměrně malý počet literárních zdrojů (13), z kterých 7 směřuje na online zdroj vývojářské dokumentace Mozilla. Použití hromadné reference v úvodu kapitoly 3 a dále nepodložené jednotlivé tvrzení konkrétními zdroji považuji za nepřehledné. Citace číslo 3 má nekonzistentní jméno autora vzhledem k ostatním citacím.

Práce neobsahuje průzkum alternativních, již existujících řešení.
7. **Implementation results** **75 p. (C)**
Realizovaný výstup je funkční a plní požadavky zadání. Praktickou použitelnost znesnadňuje pomalé dešifrování obsahu stránky. Z pohledu bezpečnosti bych se velmi obával jako uživatel využívat nativní aplikaci, a rozšíření prohlížeče, které po mne požaduje heslo k použití sudo.
8. **Utilizability of results**
Zdrojové kódy jsou dostupné na GitHub bez uvedení licence. Rozšíření prohlížeče Firefox je publikováno dle požadavku zadání v repozitáři addons.mozilla.org.
9. **Questions for defence**
 1. V testech ukazujete, že výkon nejvíce ovlivňuje komunikace s nativní aplikací sloužící pro dešifrování obsahu. Nebylo by možné využít nativní aplikaci k získání přístupu k privátnímu klíči a dešifrování řešit v OpenPGP.js?
 2. Vysvětlíte princip elektronického podpisu a ověření zejména bod 6, druhé enumerace v sekci 2.2.
10. **Total assessment** **70 p. good (C)**
Práce je vypracována netradičním způsobem popisující agilní přístup při vývoji aplikace schopné dešifrovat

obsah webové stránky šifrovaný pomocí GnuPG. Práce obsahuje slabou motivaci a přestože téma má velký potenciál, autor jej nedokázal dostatečně využít, ani neprojevil snahu práci zasadit do kontextu průzkumem existujících řešení. V práci se objevují místy překlipy, nekonzistentní typografie a faktické chyby.

Navrhuji hodnotit práci stupněm C.

In Brno 15 August 2020

Pluskal Jan, Ing.
reviewer