Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Peter Bátora** **Oponent:** **Ing. Michal Šmiraus, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2019/2020**

Téma diplomové práce: **Návrh autentizačního protokolu za využití bezpečnostních tokenů**

Hodnocení práce:

Předkládaná diplomová práce ve své teoretické části obsahuje přehledně zpracované penzum znalostí a principů, nutných pro základní pochopení dané problematiky kryptografie a šifrování v oblasti webových aplikací.

Ve své praktické části je již blíže specifickým způsobem osvětlena konkrétní problematika využití stávajících standardů autentizačních tokenů a následně je autorem představeno na příkladu vlastní webové aplikace funkcionálně ztvárněné řešení návrhu autentizačního protokolu.

Návod na zprovoznění prostředí i samotné aplikace je psán jasnou a srozumitelnou formou, oceňuji pro daný účel vhodně zvolený framework FLASK. V práci naopak postrádám nedostatečný počet monografických zdrojů, což je však do jisté míry vyváženo zpracováním a vytěžením veskrze hodnověrných zahraničních zdrojů elektronických a závěrečná část by mohla blíže specifikovat zamýšlené možnosti omezení přenositelnosti s vazbou na geolokaci a HW/SW fingerprinting.

Konstatuji, že předem dané cíle práce byly bez výhrad splněny. Ať už se týká zpracování teoretické rešerše k dané problematice autentizace za využití tokenů, tak i následná praktická interpretace výsledků procesu tvorby a použití vlastního řešení bezpečnostního tokenu s využitím moderního hashovacího algoritmu. Za hlavní přínos závěrečných výstupů celé práce pak lze označit zejména inovativní přístup při tvorbě vlastního tokenu s následným doplňkovým šifrováním a nastíněnými potenciálními možnostmi dalšího vývoje či vylepšení v budoucnu.
V práci jako celku se až na výjimky drobných překlepů (str. 8,18,35,52,55) nevyskytují žádné zásadní stylistické chyby a použité zdroje jsou řádně citovány.

Otázky k obhajobě:

1. Zdůvodněte své tvrzení v teoretické části u Opaque tokenu (3.2.3.2). Z jakého důvodu je výhodou uváděné neprůhlednosti fakt, že takto generované tokeny se nemusejí podepisovat?

2. V kapitole Porovnání tokenů (6.1) praktické části práce není blíže rozváděno, nicméně dovedl byste ze své zkušenosti při vývoji a testování svého vlastního autentizačního protokolu uvést a doplnit také možná výkonnostní porovnání s již zavedenými SAML 2 a OAuth 2 z hlediska času nutného pro zpracování požadavků v závislosti na délce použitého klíče - stačí jednoduché statistické srovnání, popř. jaký vhodný nástroj by se pro účely takového performance testingu dal použít?

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 26. 8. 2020 Podpis oponenta diplomové práce