FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Kritéria pro hodnocení bezpečnosti kryptografických knihoven
Student:	Milan Špinka
Vedoucí:	Ing. Josef Kokeš, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Informační bezpečnost 2021
Katedra:	Katedra informační bezpečnosti
Platnost zadání:	do konce letního semestru 2024/2025

Pokyny pro vypracování

Práce bude sloužit jako východisko pro řešení projektu Bezpečné použití kryptografických knihoven. Cílem tedy je vypracovat metodiku, která umožní porovnat různé kryptografické knihovny mezi sebou a doporučit pro dané použití tu nejvhodnější.

1) Seznamte se s problematikou bezpečnosti softwaru - bezpečný návrh, implementace i použití.
2) Po dohodě s vedoucím vyberte 3-4 open-source knihovny realizující kryptografické protokoly. Nastudujte hlavní vlastnosti těchto knihoven.
3) Zaměřte se na technicko-organizační opatření zajišťující bezpečnost zkoumaných knihoven, například pravidla pro přispívání do projektu. Porovnejte zkoumané knihovny mezi sebou a také s OpenSSL.
4) Navrhněte metodiku, jak pro obecnou knihovnu nalézt a vyhodnotit typické chyby, ke kterým při jejím použití dochází. Takovým zdrojem může být např. seznam publikovaných zranitelností (CVE) aplikací, které knihovnu používají. Použijte tuto metodiku na knihovny z předchozích bodů.
5) Na základě předchozích zjištění určete hlavní kritéria, která ovlivňují bezpečnost jak knihovny, tak jejího použití aplikačním vývojářem. Formulujte doporučení pro vývojáře, jak zvolit a použít knihovnu tak, aby výsledná aplikace byla co nejbezpečnější.

Elektronicky schválil/a prof. Ing. Róbert Lórencz, CSc. dne 26. ledna 2024 v Praze.