MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

21. června 2021

Posudek vedoucího bakalářské práce Martina Pastyříka

Práce kolegy Pastyříka se zabývá formálním popisem a studiem vlastností schématu pro distribuované trasování kontaktů ze článku K. Pietrzaka (INDOCRYPT 2020). Hlavní motivací Pietrzakovi byla nedostatečná odolnost prvních takovýchto schémat vůči replay a relay útokům, které mají devastující následky pro distribuované trasování kontaktů s minimem úsilí a prostředků na straně útočníka. Pietrzakova alternativní konstrukce je založena na novém kryptografickém primitivu nazvaném Delay-MAC, jež je rozšířením standardního MAC pro integritu dat.

Prvním přínosem bakalářské práce kolegy Pastyříka je modulární popis Pietrzakova schématu, který odděluje důkaz bezpečnosti konstrukce Delay-MAC od vlastností samostatného schématu, které je pomocí Delay-MAC Pietrzakem konstruováno. Ve druhé kapitole autor nejprve předkládá formální definici pro Delay-MAC a poté dokazuje, že:

1. Pietrzakova konstrukce Delay-MAC ze standardního MAC a výpočetně zavazujícího commitment schématu dosahuje požadovanou úroveň integrity.
2. Pietrzakova konstrukce Delay-MAC ze standardního MAC a statisticky důvěrného commitment schématu dosahuje statistickou záruku důvěrnosti.

Tato část práce pokrývá výsledky, které jsou obsaženy v Pietrzakově článku. Zásadním rozdílem je však úroveň formality a dosažená modularita popisu. Pietrzakova definice a konstrukce Delay-MAC nejsou jasně odděleny. Tím, že kolega Pastyřík představuje samostatnou definici pro Delay-MAC, mohl se v následující kapitole oprostit od zbytečných detailů implementace Delay-MAC, které by komplikovaly již tak rozsáhlý popis samostatného schématu.

Druhým přínosem práce je popis a analýza vlastností navrženého schématu v modelu ze článku Danz et al. (IACR Cryptol. ePrint Arch., 2020). Ve třetí kapitole autor v krátkosti představuje model distribuovaných schémat pro trasování kontaktů od Danz et al., předkládá formální popis Pietrzakova schématu v tomto modelu a poté dokazuje, že:

1. Pietrzakovo schéma je rezistentní proti replay útokům a diskutuje také variantu schématu z Pietrzakova článku, která zajišťuje odolnost také vůči relay útokům.
2. Pietrzakovo schéma dosahuje vyšší úroveň důvěrnosti pro data uživatelů než aktuálně používaná schémata.

Tato část práce představuje nové výsledky o vlastnostech Pietrzakova schématu, kterým se Pietrzakův článek formálně nevěnoval. Kolega Pastyřík musel také rozšířit model od Danz et al., aby mohl zachytit dosaženou úroveň důvěrnosti dat uživatelů v Pietrzakově schématu a porovnat ji se stávajícími schématy. Specificky, definice vlastností *identity-leak resistence* a *time-reveal resistence* jsou samostatným příspěvkem autora.

Formální stránka práce je velmi dobrá, matematická úroveň práce je adekvátní a práce se zdroji důsledně rozlišuje nové a známé výsledky. Popis modelu od Danz et al. je stručnější, což možná částečně ubírá na srozumitelnosti. Vidím to však jako akceptovatelné vzhledem k doporučovanému rozsahu bakalářské práce, protože je model využit k důkazu nových tvrzení a cílem práce není pouhá rešerše článku od Danz et al. a jejich modelu.

Výsledky své práce bude kolega Pastyřík prezentovat na workshopu Mikulášská kryptobesídka 2021, kde získal druhé místo v rámci soutěže studentských prací KEYMAKER. Práci kolegy Pastyříka považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Mgr. Pavel Hubáček, Ph.D.

Informatický ústav Univerzity Karlovy
Malostranské nám. 2/25, 118 00 Praha 1
telefon: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz