Posudek vedoucího diplomové práce:

„Konkrétní bezpečnost protokolu IPSec“

Stanovisko vedoucího práce k volbě a náročnosti tématu:

Protokol IPSec má dvě hlavní části a to protokol pro ustanovení klíče (tím je některá z verzí protokolu IKE) a schémata využívající ustanovený klíč k ochraně datové komunikace mezi účastníky protokolu. Úkolem diplomantky bylo zabývat se konkrétní bezpečností některé z verzí protokolu IKE pro ustanovení klíče.

V odborné literatuře jsou publikovány důkazy formální nebo asymptotické bezpečnosti protokolu IKE, ale nikoliv důkaz jeho tzv. konkrétní bezpečnosti. To souvisí se skutečností, že důkazy výpočetní bezpečnosti v praxi používaných schémat a protokolů bývají často těžkopádné a obtížně kontrolovatelné a jejich formulace v rámci konkrétní bezpečnosti tuto těžkopádnost a obtížnost kontroly ještě zvyšuje.

Problematika bezpečnosti kryptografických protokolů navíc bývá kontra-intuitivní, což je i případ bezpečnosti protokolu IKE s využitím digitálního podpisu, který je předmětem posuzované diplomové práce.

Přechod od důkazu asymptotické bezpečnosti k důkazu konkrétní bezpečnosti může mít značný praktický význam. To je zřejmé například z důkazu bezpečnosti RSA-OAEP, jehož výpovědní hodnota je pro běžně používané délky RSA klíčů 1024 a 2048 bitů podstatně degradována nepřiléhavostí příslušné redukce.

Diplomantka využila již existující důkaz tvrzení o asymptotické bezpečnosti tzv. SIGMA protokolu, který je podstatou verze protokolu IKE využívající digitální podpis, a transformovala toto tvrzení a jeho důkaz na případ konkrétní bezpečnosti.

Uvažované tvrzení dokazuje dvě bezpečnostní vlastnosti protokolu SIGMA, přičemž první z nich zaručuje to, že, pokud oba účastníci odvodí v rámci testovacího sezení svoji hodnotu klíče, pak jsou tyto hodnoty shodné.

Druhá bezpečnostní vlastnost především zaručuje to, že útočník, který na konci běhu protokolu zvolí některé z dokončených sezení jako testovací, a poté obdrží bitový řetězec, o kterém neví, zda je náhodný nebo, zda je identický s klíčem ustanoveným v testovacím sezení, není schopen efektivně zjistit, která z obou možností nastala.

Dále však tato druhá vlastnost zaručuje i to, že, pokud některé sezení používá stejný identifikátor sezení jako sezení testovací, pak je toto sezení s testovacím sezením shodné v tom smyslu, že kromě stejného identifikátoru má i stejné účastníky (nebo není dokončené).

Potřebnost důkazu zmíněné druhé části druhé bezpečnostní vlastnosti (k důkazu její hlavní části) není na první pohled zřejmá. Plyne z možnosti „útoku s podvržením identity účastníka“ (*Misbinding Attack*) na příbuzné varianty protokolu. Po úspěchu v tomto útoku sice útočník nezná klíč, který byl v rámci testovacího sezení ustanoven, ale zato jednomu z účastníků testovacího sezení úspěšně předstírá, že druhým účastníkem tohoto sezení je právě on.

Model útočníka předpokládá, že může zkorumpovat v podstatě kterékoliv sezení, kromě testovacího sezení a sezení s ním shodného. Proto je důkaz shodnosti sezení se stejným identifikátorem nutný k vyloučení „útoku s podvržením identity účastníka“ a tím i vyloučení možnosti zkorumpování druhého majitele klíče odvozeného v testovacím sezení.

Nicméně vyloučení útoků s podvržením identity je samo o sobě důležitou bezpečnostní vlastností, jejímuž vysvětlení mohla být v diplomové práci věnována větší pozornost.

Důkaz druhé bezpečnostní vlastnosti je technicky poměrně náročný. Využívá techniku „střídání her“ (*game hopping*) tak, že definuje uspořádanou pětici simulátorů, z nichž dva krajní definují úspěšnost řešitele rozhodovacího Diffieova-Hellmannova problému a trojice zbylých umožňuje postupný kontrolovaný přechod mezi nimi.

Tento postup je výrazně zkomplikovaný nutností odhadnout pravděpodobnosti, s nimiž se jednotlivým simulátorům podaří uhodnout, které sezení vybere útočník jako testovací. Jde o to, že v případě tří „prostředních simulátorů“ dochází k modifikaci průběhu sezení odhadnutého příslušným simulátorem jako testovací, což může ovlivnit pravděpodobnost toho, že útočník po ukončení běhu protokolu toto sezení skutečně jako testovací vybere.

Dalším citelným ztížením důkazu bylo prokázání toho, že každé sezení, které má stejný identifikátor jako sezení testovací, je s ním shodné. Ukázalo se, že výpočet odhadu pravděpodobnosti úspěchu útočníka při snaze o narušení této vlastnosti byl v rámci konkrétní bezpečnosti pro některé simulátory překvapivě značně komplikovaný.

Shrnutí

- Vedoucí práce považuje její téma za důležité zejména z hlediska jeho praktické potřebnosti.
- Samotný obsah práce považuje za náročný zejména z důvodů řady (výše vysvětlených) komplikací vlastní realizace hlavní myšlenky důkazu.
- Převážnou část těžkopádnosti a obtížné kontrolovatelnosti některých partií vlastního důkazu je podle jeho názoru nutno připsat na vrub samotnému tématu práce.

Stanovisko vedoucího práce k jejímu provedení:

Diplomová práce je rozdělena do sedmi kapitol, z nichž prvních pět lze chápat jako přípravné a šestou kapitolu jako vlastní důkaz konkrétní bezpečnosti SIGMA protokolu. V závěrečné sedmé kapitole je diskutován praktický význam výsledků a jejich aplikovatelnost na protokol IKE v IPSec.

Prvních pět kapitol je napsáno srozumitelně a čtivě. Rovněž jejich členění považuji za dobře zvolené.

- V první kapitole je načrtnuta struktura diplomové práce a vysvětlen obsah a význam pojmů „asymptotická bezpečnost“ a „konkrétní bezpečnost“.
- Ve druhé kapitole je popsán protokol IPSec včetně základních pojmů potřebných pro pochopení jeho praktického používání a schémat pro kryptografickou ochranu

uživatelských dat. Největší pozornost je pochopitelně věnována různým variantám protokolu IKE pro ustanovení klíčů.

- Ve třetí kapitole jsou vysvětleny základní pojmy bezpečnosti protokolů pro ustanovení klíčů sezení. Značná pozornost je zde (správně) věnována vysvětlení pojmů: „sezení“ a „shodné sezení“. S těmito pojmy úzce souvisí model útočníka, zejména formulace jeho možností v rámci uvažovaného bezpečnostního modelu. V závěru kapitoly je definována tzv. „SK-bezpečnost“ protokolů pro ustanovení klíčů, jejíž podstatou je neschopnost útočníka odlišit klíč testovacího sezení od náhodného řetězce .

- V rámci použitých definic shodného sezení a povolených akcí útočníka zahrnuje definice SK-bezpečnosti v tomto kontextu rovněž i požadavek vyloučení již zmíněných útoků s podvržením identity (*Misbinding Attacks*). To ovšem není na první pohled zřejmé, a proto by bylo vhodnější tuto skutečnost na tomto místě zmínit, případně i stručně vysvětlit.

- Čtvrtá kapitola nazvaná „Protokol Σ_0“ obsahuje kromě popisu protokolu i vysvětlení výchozích myšlenek důkazu jeho bezpečnosti včetně definice a popisu jednotlivých simulátorů. Tyto části jsou sice uvedeny v samostatných podkapitolách, takže nepůsobí rušivě, ale možná by bylo vhodnější je vyčlenit do samostatné kapitoly.

- Pátá kapitola je věnována definicím pojmů konkrétní bezpečnosti použitých ve formulaci a důkazu tvrzení o bezpečnosti protokolu SIGMA. Rovněž je věnována podrobnějšímu popisu komunikace útočníka s jednotlivými orákuly.

Hlavní náplní diplomové práce je ovšem šestá kapitola „Důkaz bezpečnosti Σ_0 v kontextu konkrétní bezpečnosti“ zabírající téměř třetinu jejího rozsahu. Je v ní realizován důkaz konkrétní bezpečnosti protokolu SIGMA a to obou bezpečnostních vlastností zmíněných v první části posudku.

Hlavní myšlenky a schéma postupu přitom vycházejí z práce: R. Cannetti, H. Krawczyk: *Security analysis of IKE's Signature-based Key-Exchange Protocol*. Přechod ke konkrétní bezpečnosti si ale vyžádal podstatně podrobnější úvahy než byly v citovaném článku, což se projevilo zejména v důkazech lemmat 5 a 6.

Důkaz druhé bezpečnostní vlastnosti je značně rozsáhlý a některé jeho části (zejména důkaz lemmatu 6) jsou obtížně kontrolovatelné. Ty mohly být podrobněji komentované. Pro lepší přehlednost důkazu by bylo užitečné, kdyby na jeho začátku byla popsána a vysvětlena jeho struktura.

Pro čtenáře důkazu může být trochu matoucí, že hodnota bitu b určujícího, zda útočník na konci experimentu obdržel reálný session klíč nebo jeho náhodnou imitaci, je v práci zavedena opačně (b = 1 pro náhodnou hodnotu), než bývá obvyklé (b = 1 pro reálnou hodnotu). Ale, vzhledem k tomu, že tato konvence je v práci důsledně dodržena, nejde o věcnou chybu.

Transformace důkazu z rámce asymptotické bezpečnosti na případ konkrétní bezpečnosti zahrnuje úvahy související jak s omezením úspěšnosti - „výhody“ (*advantage*) útočníka, tak i s omezením jeho výpočetního času a jeho přístupových možností – omezení typů a počtů dotazů na různá orákula. Totéž se týká uvažovaných simulátorů.

Je přirozené, že největší pozornost je v práci věnována vztahům mezi konkrétními omezeními úspěšnosti - „výhody“ (*advantage*) simulátorů a útočníka. Souvisí to s tím, že účelem většiny kroků důkazu je zdůvodnění omezení útočníkovy úspěšnosti.

Vztahům mezi omezeními výpočetních časů (ale i počtů dotazů na různá orákula) různých verzí simulátoru a útočníka při důkazu druhé vlastnosti již taková pozornost věnována není. Což je škoda, protože tyto vztahy by si zasloužily alespoň krátké, stručné vysvětlení.

Kromě výpočetního času, který útočník potřebuje k útoku, musí simulátor rovněž simulovat útočníkovi téměř celou síť (běh většiny sezení protokolu). Výpočetní náročnost této simulace sice můžeme pokládat za zanedbatelnou ve srovnání s výpočetním časem efektivního útočníka, ale mohlo to být alespoň stručně vysvětleno.

S tím souvisí drobné, ale nepříjemné, nedopatření. Předpokládané omezení výpočetního času útočníka by mělo být minimem z hodnot t_{SIG}, t_{DDH} a t_{PRF}. V práci je omylem uvedeno maximum z nich.

U lemmat 9 až 13 nejsou uvedeny jejich důkazy, což samo o sobě příliš nevadí, protože jsou analogiemi předchozích, již dokázaných, lemmat, ale krátké komentáře u jednotlivých lemmat by pravděpodobně byly na místě.

Shrnutí

- Zadání diplomové práce bylo splněno.
- Diplomová práce obsahuje nové - z praktického hlediska důležité - výsledky, které by si zasloužily nějakou formu publikace.
- Jejich získání spočívalo v transformaci již známého důkazu asymptotické bezpečnosti protokolu SIGMA na důkaz jeho konkrétní bezpečnosti. Již původní verze důkazu byla technicky značně náročná a kontra-intuitivní. Přechod ke konkrétní bezpečnosti vnesl do provedení důkazu další citelné komplikace.
- Předložený důkaz obsahuje některé obtížně kontrolovatelné části, které by si zasloužily podrobnější vysvětlení. Zasloužilo by si ho i stanovení omezení útočníkových možností (zejména výpočetní kapacity a dotazů na orákula). Před publikací výsledků doporučuji zmíněná vysvětlení doplnit, aby se předešlo zbytečným nejasnostem.
- Většina diplomové práce (s výjimkou některých partií důkazu) je napsána srozumitelně a čtivě.

Diplomovou práci doporučuji hodnotit známkou …

V Praze 2. 9. 2015

RNDr. Bohuslav RUDOLF