Fiks 2021/2022 úloha č. 10 „Tučňáci z Madagaskaru“

Kryštof Olík

Tučňáci, značení jako A, se vydávají z naší základny, značenou jako B, na tajnou misi a potřebují se základnou komunikovat. Je tu však jeden háček, mezi našimi zprávy je tak zvaný Man in the middle, značený jako M, který dokáže naše zprávy číst, a dokonce zprávy mířené z A do B dokáže pozměnit. Naším cílem je vymyslet bezpečný protokol komunikace, tak, aby M nedokázal pochopit o co ve zprávě jde, abychom poznali, zda útočník zprávu nějakým způsobem pozměnil a abychom dokázali přečíst zprávy i po změně pořadí a přerušení.

Návrh protokolu a odůvodnění

Ještě před tím, než se tučňáci vydají na cestu, tak si se základnou domluví nějaký společný náhodný seed, který budeme používat na pseudo-náhodnou generaci klíčů. Tímto zajistíme, že obě strany pokaždé vygenerují nové a stejné klíče. Poté co se vydá A na cestu, tak můžeme začít bezpečně komunikovat. Řekněme, že první potřebujeme poslat zprávu z B do A.

Nejprve si náhodně vygenerujeme klíč s použitím společného seedu. Pokaždé používáme jiný náhodný klíč na šifrování, aby M neměl možnost rozpoznávat stejné zprávy a zároveň k tomu, aby nemohl náhodou naše zprávy znovu použít a poslat. Jelikož bývají naše zprávy krátké, tak k ním přidáme trochu výplně (náhodná výplň, která nemá s naší zprávou nic společného). To děláme pro to, abychom ještě více znemožnili možnost zprávu dešifrovat metodou bruteforce a zároveň, aby M nemohl poznat o jakou zprávu se jedná podle její délky. Zprávu poté zašifrujeme naším klíčem a pošleme jí A.

Když zpráva dorazí do A, tak vygenerujeme stejný klíč (opět, protože máme stejný začáteční seed), zprávu dešifrujeme, výplň odstraníme a nakonec si zprávu můžeme přečíst. Avšak teďka, když chceme poslat zprávu z A do B, musíme zprávu před odesláním více ošetřit, jelikož je M schopný zprávu pozměnit. Aby B poznalo, zda bylo se zprávou od A manipulováno, tak musíme zprávu tzv. podepsat.

Vygenerujeme nový klíč a dáme se do procesu podepisování. Nejprve přidáme k naší zprávě výplň a poté z ní vytvoříme otisk. Tedy, vytvoříme tzv. hash této zprávy s výplní. Tento otisk zprávy bude fungovat jako náš podpis. Poté otisk a naši zprávu s výplní zašifrujeme stejným klíčem.

Abychom poznali, zda M zprávu poupravoval, tak musíme udělat na straně B následující kroky. Nejprve znovu vygenerujeme nový klíč pomocí seedu a následně zprávu i otisk dešifrujeme. Poté si z obdržené zprávy vytvoří další otisk, který poté porovná s otiskem obdrženým od A. Pokud se otisk od A shoduje s vygenerovaným otiskem od B, tak je zpráva ověřena a znamená to, že s ji M nijak nepoupravil.

Už se bráníme proti dvou nejdůležitějším útokům, ale je tu však ještě jeden otravný útok, proti kterému se musíme bránit, a to je změna pořadí obdržených zpráv a jejich rušení. Ke každé zprávě přidáme ID, které se po každé zprávě zvětšuje o jedna. Díky těmto ID, můžeme poznat správné pořadí zpráv, a dokonce i pokud nějaká zpráva mezi byla zrušena.

Má to však jeden háček, a ten se týká naší generace klíčů. Momentálně náš algoritmus vyžaduje generovat klíče ve stejném pořadí jako poslané zprávy, avšak jak už víme, nemusí tomu tak být. Vyřešíme to tak, že si vygenerované klíče budeme ve správném pořadí ukládat. Pokud B přijde zpráva, která nejde dešifrovat, tak vygenerujeme nové klíče, které si budeme popořadě ukládat a zkoušet je na

dešifraci. Jakmile přijde další zpráva, tak stačí vyzkoušet dešifrovat s našimi uloženými klíči nebo vygenerujeme nové. Toto nám zajistí, že budeme schopni dešifrovat zprávy i se změněným pořadím.

Dále můžeme ke zprávě přidat čas odeslání, díky kterému můžeme analyzovat, že byla zpráva nějaký čas držena.

A to je vše, teď už můžou tučňáci bezpečně posílat základně zprávy a nebát se útočníka.

Útok na ukázkový protokol

Ukázkový protokol úlohy šifruje zprávy pokaždé stejným klíčem a nestará se o nic jiného. My jako útočníci se můžeme takovéto komunikaci jenom zasmát a udělal neplechu už jenom z principu.

Naschvál bychom mohli měnit pořadí zpráv v síti a tím základnu zmást a sabotovat. Posílala by tučňákům odpovědi, které by nedávali jim nedávali smysl nebo by jim dokonce špatně radili. Tímto by mise určitě padla.

Také bychom mohli zprávy mazat, buď celé, nebo třeba jenom z půlky. Základna by byla určitě zmatená a myslela by si, že má s tučňáky špatné spojení. Možná by i strávili zbytečný čas debugováním, který by vedl k ničemu.

Dále tu máme jeden zdrcující útok. Jelikož jsou zprávy vždycky v následujících formátech: „VYCKEJTE, POKRACUJEM, OPAKUJ atd…“, a všimneme si, že každá z těchto zpráv má jinou délku, tak můžeme pokaždé nehledě na šifrování zjistit co daná zpráva znamená (kromě zprávy POSLETE MI n). Tímto se v podstatě stává toto šifrování klíčem úplně k ničemu.

Na toto navazuje můj osobně oblíbený útok, který ovšem funguje pouze tehdy, jestli klíč šifruje pokaždé stejné písmenko stejně. Když víme, co jsou zašifrovaná písmenka zač, tak si můžeme vytvořit vlastní zprávy! A to nejenom takové na pokažení mise, ale také můžeme základně docela dost vynadat. Ze zprávy „OPAKUJ“ si vypůjčíme písmena P, A, K a ze zprávy „STAHUJEME SE, NEMA TO CENU“ si můžeme vypůjčit frázi za čárkou. Opakovaně budeme posílat základně „PAKA, NEMA TO CENU“ společně s jinými nadávky do té doby, dokud se posádka základny neurazí a nevzdá.