Řešení 3. úlohy 4. kola - Tučňáci z Madagaskaru

Problémy ukázkového protokolu

Kromě zmíněné replay attack má ukázkový protokol i jiné problémy.

- Odeslaná zpráva je stejně dlouhá jako zdrojová zpráva, a protože má každá možná zpráva jinou délku, tak se dá jedoduše určit, podle počtu znaků, o jakou zprávu se jedná.
- Stejným způsobem můžeme odhadnou argument zprávy `POSLETE MI`, podle délky můžeme odhadnou řádovou velikost.
- Pokud bude nějaká zpráva zadržena, tak se ani jedna strana nedozví o tom, že se zpráva někam ztratila, nebo s ní bylo manipulováno. A pokud dorazí v jiném pořadí, tak se o tom také nedozví.

Návrh protokolu

Struktura zprávy

Zpráva se skládá z několika částí $Z_1.Z_2."||".Z_3.Z_4.Z_5$

- Z_1 je aktuální čas v mikrosekundách
- Z_2 je vlastní obsah zprávy
- Z_3 je náhodný string
- Z_4 je číslo zprávy
- Z_5 je hash $Z_1.Z_2.Z_3.Z_4$

Každá z těcho částí má nějakou vyhrazenou délku.

$$
\begin{gathered}
len(Z_1) = 16 \\
len(Z_2) + len(Z_3) = 32 \\
len(Z_4) = 4 \\
len(Z_5) = 64
\end{gathered}
$$

Délka Z_2 a Z_3 je určena společně, protože pokud bude Z_2 kratší než 32 znaků, tak se doplní náhodnou zprávou délky tak, aby byla celková délka Z_2 a Z_3 32 znaků. Z_2 a Z_3 jsou odděleny `||` aby měli tučňáci jasné, kde končí zpráva a také, aby bylo jednodušší zprávu strojově spracovat.

Celá odeslaná zpráva tak bude vždy mít délku 118, tím je odstraněna možnost zjištění obsahu zprávy na základě délky. Dále čas, číslo zprávy a náhodný string zajistí, že po zašifrování bude vždy zpráva uplně jiná, takže na základě toho také nepujde zprávě rozumět.

Číslo zprávy je zfilled na délku 4 cifer (tudíž je menší než 10 000) a $\in \mathbb{N}$. A každá strana má dvě počítadla. Číslo odeslané zprávy a číslo přijaté zprávy. Číslo odeslané zprávy se inkrementuje po odeslání zprávy a číslo přijaté zprávy se nastavuje na číslo příhozí zprávy. To pomáhá zjisti, jestli se nějaká zpráva stratila. Také společně s časem pomáhá v určení pořadí zpráv.

Čas umožňuje zjitit, jestli se jedná o novou zprávu, nebo o replay attack v případě přetečení čísla zprávy. A také může pomoct upozornit na nějaké nekalé věci, pokud se bude čas vytvoření a čas přijetí zprávy o hodně lišit. Zároveň se hodí vědět jak moc je informace obsažena ve zprávě aktuální.

Hash je určen pro ověření zprávy, pokud se hash přijaté zprávy bude lišit s poslaným hashem, tak bylo se zprávou manipulováno.

Zpráva je odesílana zašifrovaná klíčem, který si tučňáci dohodli před misí.

Strategie

Před misí si tučňáci dohodnou klíč, kterým budou šifrovat zprávy, a timeout pro přijetí zprávy.

Dále funguje komunikace následovně: Stanoviště A odešle zprávu s číslem C a po přijetí stanovištěm B odešle stanoviště B zprávu s obsahem Z

$$Z = \begin{cases} C \text{ - OK} & \text{pokud je přijatá zpráva v pořádku} \\ C \text{ - POZMENENA} & \text{pokud zpráva v pořádku nedorazila} \end{cases}$$

Pokud bude C o více než jedna větší než počítadlo přijatých zpráv (některé zprávy ještě nedorazily), tak tučňáci vyčkají dohodnutý timeout a pokud během něj zpráva nedorazí, tak odešlou zprávu s obsahem $Z = C$ - NEDORAZILA

Na tyto stavové zprávy se neodpovídá, jinak by se z toho stal nekonečný kruh.

Samozřejmě tu narážíme na problém dvou generálů. Ten je ale za nás vyřešen. Vzhledem k tomu, že $A \to B$ projde vždy a bez změny, pouze $B \to A$ se může ztratit, tak A si je jisté, že B dostalo všechny zprávy a B zároveň ví o statusu všech zpráv. Proto by B ani nemuselo odesílat status zprávy, ale protokol je pak přehlednější, protože obě strany dělají to samé.