Řešení úlohy č. 1
Tučňáci z Madagaskaru

Úkolem je navrhnout protokol, který bude bezpečný. Máme body A a B a mezi nimi komunikační kanál, který je bezpečný (ale jde odposlechnout) z jedné strany. Z druhé strany je kompletně nezabezpečený, a úkolem je to spravit. Máme několik předem definovaných zpráv, které budeme posílat a nepřítel má perfektní znalost protokolu.

Poznámka: úkolem bylo vytvořit protokol, který nebude zranitelný v alespoň těch hlavních a poměrně přímočarých oblastech. Některým účastníkům se podařilo najít i nějaké další potenciální zranitelnosti a opravit je. Tyto zranitelnosti překračují požadavky této úlohy, a všem, kterým se to povedlo, moc gratulujeme. Účastníci za tyto nadstandardní výkony byli odměněni extra body.

5 bodů

Za návrh potokolu bylo možné získat až pět bodů. Bylo potřeba zprávu zašifrovat, ale předtím ji ještě nějak upravit.

První zranitelnost byla kvůli replay útoku. Kdybychom poslali zašifrovanou zprávu, nepřítel by si ji prostě mohl poznamenat a někdy později odeslat znovu (nebo třeba nějakou zprávu během posílání přerušit). Základna by se nedozvěděla, že nějaká zpráva chybí, nebo by nějakou mohla dostat dvakrát a nemůže poznat, jestli to je správně. Řešení bylo číslovat zprávy, které se odesílají (ještě před zašifrováním). Poté základna pozná, kdyby některou zprávu dostala dvakrát, nebo kdyby nějakou nedostala vůbec.

Druhá zranitelnost byla kvůli zprávám. Je pět druhů zpráv, každá s odlišnou délkou. Operace *šifruj* ale zachovává délku zprávy. Každý kdo poslouchá a zná typy zpráv by tedy mohl velmi jednoduše zjistit typ zprávy. (A u zprávy typu *POSLETE MI n* i řád čísla, které se posílá.) Bylo tedy nutné přidat *padding* a každou zprávu nafouknout na jednotnou délku před samotným zašifrováním.

Třetí zranitelnost byla kvůli poznámce, že když změním znak na konci zprávy (která je zašifrovaná), pravděpodobně to změní znak na konci zprávy i po dešifrování a zbytek bude v pořádku. Nepřítel by tedy mohl například změnit číslo ve zprávě typu *POSLETE MI n* a příjemce by to občas nemusel poznat. Řešením bylo připojit ke zprávě před zašifrováním i její *hash* (otisk zprávy). Ve chvíli, kdyby po dešifrování otisk neodpovídal zprávě by bylo jasné, že se zprávou bylo manipulováno. Nepřítel nemá žádný spolehlivý způsob jak hash upravit tak, aby odpovídal.

Čtvrtá zranitelnost byla drobná a za zlomek bodů. Jednalo se o to, že nepřítel může zprávy pozastavit a později odeslat znova. Pokud byla ošetřena první zranitelnost, tak sice dorazily zprávy ve správném pořadí, ale základna mohla dostat zprávy ve chvíli, kdy už nejsou relevantní a kvůli tomu udělat akci, která tučňákům uškodí. Řešením bylo ke zprávám přidat timestamp ohledně toho, kdy se zpráva odeslala.

2 body

Další dva body bylo možné získat, pokud byly předchozí útoky (a obrana před nimi) dobře a srozumitelně popsané.

3 body

Úkolem bylo navrhnout útok na protokol popsaný v zadání. V podstatě se jedná o totožné zranitelnosti, kterým bylo potřeba se bránit. Jednalo se tedy o replay attack, odhadnutí

konkrétní zprávy podle délky, upravování zprávy a konečně i změna času/pořadí doručení. Všechny jsou popsané výše v sekci návrhu vlastního protokolu, jednalo se o totožné útoky.