StaySecure

8

2019

Vaše měsíční dávka kybernetické bezpečnosti

Téma: Symetrické šifrování

Co je to symetrická kryptografie?

Symetrická kryptografie je šifrování, ve kterém je pro zašifrování zprávy požívaný ten samý klíč jako k jejímu dešifrování. Je zásadní, aby bez tohoto klíče nebylo možné zprávu rozšifrovat a zároveň, aby byl algoritmus (většinou veřejný) spolehlivý, tzn. po použití klíče získáme odpovídající původní text.

Výhody?

- ✓ Snadná implementace a rychlé šifrování dat pomocí krátkých klíčů
- ✓ Základ pro vytváření různých kryptografických mechanismů, s možností vytváření silných šifer kombinací jednoduchých šifer

Nevýhody?

- ✓ Strany si mezi sebou musí vyměnit šifrovací klíč, což může vést k snadnému vyzrazení klíče a prolomení algoritmu útočníkem
- ✓ Nutnost udržovat velké množství klíčů a dostatečně často je obměňovat pro zajištění bezpečné komunikace

Jde to hacknout? Jde.

K prolomení tohoto systému potřebuje útočník odhalit šifrovací klíč a algoritmus. Tyto dva prvky brání dešifrování textu v komunikaci. Přenos klíčů přes nezabezpečenou síť (březnové číslo Stay Secure) vytváří příležitost pro útočníka k neautorizovanému přístupu k symetrickému klíči a následnému zneužití odposlechnutých informací. K tomu útočník využívá obor kryptoanalýzy, což je proces hledání zranitelností v algoritmech a následné využití nalezených slabostí k dešifrování šifry i bez znalosti tajného klíče.

Jak Vám můžeme pomoci?

Pokud Vás šifrování zaujalo a máte další otázky, neváhejte se na mě obrátit. Rád Vám poradím i v dalších oblastech kybernetické obrany a jsem připraven poskytnout okamžitou pomoc.

Oddělení IT Security