УДК 003.26:004.056.55

ОЦІНКА СТІЙКОСТІ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Малішевська М.І., Добош М.П.
Тернопільський національний економічний університет, магістранти

I. Вступ

Проблема захисту комп'ютерних мереж від несанкціонованого доступу на сьогоднішній день є дуже актуальною та особливо гостро постає при передачі конфіденційної інформації комерційних та урядових організацій. Одним із методів ефективного захисту інформації від несанкціоного доступу є використання криптографічних протоколів в основі яких лежить набір правил, що регламентують використання криптографічних перетворень та алгоритмів. При виборі криптографічного протоколу доцільно оцінювати його стійкість, яка впливає на ефективність системи захисту інформації та є індикатором загального рівня її конфіденційності.

II. Мета роботи

Метою роботи є аналіз критеріїв оцінки стійкості криптографічних протоколів.

III. Критерії стійкості криптографічних протоколів

Принцип Керкхоффа, який має бути покладений в основу будь–якої криптосистеми, полягає в тому, що стійкість системи має визначатися лише стійкістю криптографічного ключа.

Питання про теоретичну стійкість криптографічних алгоритмів було сформульоване Шенноном та опубліковане у праці [1]. У цій же праці визначено вимоги до ідеального криптографічного шифру – це шифр, в якому кожен біт шифротексту залежить від кожного біта відкритого тексту і від кожного біта ключа.

Крім теоретичної стійкості відомі практично стійкі або обчислювально стійкі системи захисту інформації. Стійкість таких систем напряму залежить від обчислювальних можливостей криптоаналітика. Практична стійкість таких систем базується на теорії складності і оцінюється виключно на якийсь певний момент часу і послідовно з двох позицій:

1) експертна оцінка стійкості криптографічного алгоритму до зламу (колективна оцінка, що базується на тривалому криптоаналізі алгоритму різними групами фахівців);

2) оцінка обчислювальної неможливості перебору всіх комбінацій символів у ключах криптосистеми на підставі прогнозів зростання продуктивності обчислювальної техніки (на практиці така оцінка криптостійкості виявляється надмірно оптимістичною, оскільки зростання обчислювальних потужностей комп'ютерів випереджає прогнози).

У кожному конкретному випадку можуть також існувати додаткові критерії оцінки стійкості. Практичне застосування теоретично стійких криптографічних протоколів обмежено міркуваннями вартості і зручності користування.

Висновок

У роботі наведено критерії стійкості криптографічних протоколів. Аналізуючи дані критерії можна зробити висновок, що криптографічний протокол вважається стійким, якщо для його зламу супротивник повинен затратити недосяжні обчислювальні ресурси. В свою чергу, оскільки в основі багатьох криптопротоколів лежать криптографічні алгоритми, то зрозуміло, що остаточна стійкість протоколів буде не більшою за стійкості використовуваних криптографічних алгоритмів.

Список використаних джерел

1. Shannon C. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, 1949. — Vol. 28. — P. 656–715.
2. Мао В. Современная криптография : Теория и практика / Венбо Мао. — М. : Издательский дом «Вильямс», 2005. — 768 с.
3. Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.
4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е издание.: Пер. С англ. – М.: Издательский дом «Вильямс», 2001 – 672 с.