МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет
імені Тараса Шевченка

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

“ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ” (PCSITS)

05-06 квітня 2018 року

Київ – 2018

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповодідей та тез; м. Київ, 05-06 квітня 2018 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2018. – 510с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, російською, англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

Київський національний університет імені Тараса Шевченка, 2018

ВСТУП

Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. **Одн**ак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері. У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах. Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

У збірнику матеріалів науково-практичної конференції опубліковано тези доповідей вчених, науково-педагогічних працівників, аспірантів, студентів Київського національного університету імені Тараса Шевченка та інших вищих навчальних закладів та організацій України, в яких розглядаються науково-технічні та практичні аспекти створення та використання засобів безпеки інформаційно-телекомунікаційних систем та методи управління інформаційною безпекою таких систем.

В роботі конференції взяли участь представники: Київського національного університету імені Тараса Шевченка, Харківського національного університету радіоелектроніки, Одеського національного політехнічного університету, Харківського університету Повітряних Сил імені І. Кожедуба,

Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Державного університету телекомунікацій, Національного авіаційного університету, Державний науково-дослідний інститут спеціального зв'язку та захисту інформації України, Харківського Національного Університету ім.В.Н.Каразіна, ООО «ІТЦ «Хай-Тек Бюро»,Військовий інститут телекомунікацій та інформатизації, АТ «Інститут інформаційних технологій», Військової частини А0515, Національного університету біоресурсів і природокористування України, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Державної наукової установи Інститут модернізації змісту освіти, Державного університету інфраструктури та технологій, Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна, Інституту проблем математичних машин і систем НАН України, Київського університету імені Бориса Грінченко, Одеської національної академії харчових технологій, Чернівецького національного університету ім.Ю.Федьковича, Кавказського університету, Міжнародного чорноморського університету, Національного університету «Львівська політехніка», Національної академії Служби безпеки України, Національної академії внутрішніх справ, Східноукраїнського національного університету імені В. Даля, та інші

СЕКЦІЯ 1.
«НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ»

УДК 004.056

Г.М. Гулак[1], П.М. Складанний[2]
[1]Інститут проблем математичних машин і систем
Національної академії наук України
[2]Київський університет імені Бориса Грінченко
gena.gulak@gmail.com
p.skladannyi@kubg.edu.ua

РАЦІОНАЛЬНИЙ ВИБІР СТЕПЕНІ ПІДСТАНОВОК ШИФРУ БАГАТОАЛФАВІТНОЇ ЗАМІНИ ТА ДЖЕРЕЛА РІВНОМІРНО РОЗПОДІЛЕНОЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ

У сучасному світі спостерігається постійне зростання сфер застосування системах управління технологічними процесами (СУТП), починаючи з енергетики, зв'язку, повітряного та залізничного транспорту й завершуючи високотехнологічними галузями економіки країн світу, як металургійні та хімічні виробництва тощо. Використання у якості транспортної мережі в СУТП глобальної мережі Інтернет підвищує ризики порушення їх гарантоздатності, що включає, зокрема, потенціал виконання визначених завдань, уникаючи можливості непередбачуваних змін системи та послуг, що надаються (властивість цілісності, інакше - імітостійкості), а також неавторизованого доступу до інформації про послуги (властивість конфіденційності) [1].

В роботі [2] запропоновано швидкий алгоритм реалізації шифру багатоалфавітної заміни з використанням шифрувальної послідовності від блокового шифру в режимі OFB, доведено коректність відповідної процедури та можливість формування будь-якої підстановки з симетричної групи підстановок S_n. Проведено імітаційне моделювання алгоритму, що дозволило підтвердити необхідні статистичні якості матриці перехідних ймовірностей шифру. який забезпечить високий рівень стійкості шифрування та імітостійкість команд і службової інформації, що циркулює в СУТП. В роботі Зубова А.Ю. [3] отримані фундаментальні результати в плані оцінки імітостійкості,

зокрема, доведено, що для будь-якого шифру для ймовірності $p_п$ підміни повідомлення в каналі зв'язку справедлива нерівність:

$$p_п \geq \frac{|\mathcal{M}|-1}{|\mathcal{C}|-1}, \quad (1)$$

де $|\mathcal{M}|$ - потужність множини припустимих відкритих повідомлень, $|\mathcal{C}|$ - потужність множини шифрованих повідомлень.

Посилив вимогу щодо криптографічної стійкості шифру, оцінку (1) можливо посилити, для цього доведемо наступну лему.

Лема. В випадку практичної криптографічної стійкості шифру та джерела повідомлень без пам'яті для ймовірності $p_п$ підміни шифрованого повідомлення в каналі зв'язку справедлива нерівність:

$$p_п \geq 2^{-(1-H_0)L}, \quad (2)$$

де $H_0 = -p_0 \log_2 p_0 - p_1 \log_2 p_1$ – бітова ентропія відкритого повідомлення, величина L є довжиною відкритих та шифрованих повідомлень.

Слід зазначити, що для інформаційного обміну в рамках СУТП, за звичай, характерний високий ступінь формалізації повідомлень, які переважно мають деяку фіксовану довжину, тому обмеження щодо довжини можна вважати припустимим.

По-перше, звернемо увагу, що і теоретично, і практично стійкі шифри забезпечують розподіл ймовірностей знаків шифрованого тексту, який не відрізняється від случайного та рівномірно. Тому потужність шифрованих текстів $|\mathcal{C}|$ дорівнює величині 2^L.

Оскільки, виконані умови другої теореми Шеннона [18], то для $|\mathcal{M}|$ потужності множини припустимих відкритих повідомлень справедлива оцінка:

$$|\mathcal{M}| = 2^{H_0 L}.$$

Далі скористаємось нерівністю (1) і отримаємо:

$p_п \geq \frac{|\mathcal{M}|-1}{|\mathcal{C}|\text{-}-1} = \frac{2^{H_0 L}-1}{2^L-1} \approx 2^{-(1-H_0)L}$, для достатньо великих L, що і було потрібно довести.

Слід відмітити, що імітостійкість шифру можливо характеризувати за допомогою складності $C_{\text{п}}$ підробки зловмисником повідомлення, яку можна оцінити наступним чином. Нехай, за допомогою шифру багатоалфавітної заміни с ключем K легальним користувачем системи було зашифроване та передане в канал зв'язку деяке істинне повідомлення $M = (m_1, m_2, \dots, m_l)$ із множини припустимих відкритих повідомлень: $M \in \mathcal{M}$:

$$C = E_K(M).$$

Зловмисник, який перехопив шифротекст $C = (c_1, c_2, \dots, c_l)$, намагається провести атаку з відомим відкритим повідомленням для нав'язування фіктивного повідомлення $\tilde{M} = (\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_l)$. Вважаємо, що дані M та $\tilde{M}$ відрізняються лише на r місцях, тобто маємо:

$$|\{i: m_i \neq \tilde{m}_i\}| = r$$

Тоді зловмисник на $(l - r)$ місцях співпадаючих знаків $m_i = \tilde{m}_i$ використовує відомі йому символи шифротексту, оскільки:

$$E_K(m_i) = E_K(\tilde{m}_i) = \begin{pmatrix} \dots & m_i & \dots \\ & c_i & \end{pmatrix}.$$

На інших місцях він буде вимушений обирати один з невідомих $(n - 1)$ варіантів переходів навмання, а загальна кількість варіантів підбору шифротексту $\tilde{C}$, який після розшифрування буде сприйнятий як $\tilde{M} = E_K^{-1}(\tilde{C})$, становить величину:

$$C_{\text{п}} = (n - 1)^r.$$

Звідси отримуємо ймовірність вгадування зловмисником r символів з першого разу, яка може слугувати оцінкою для рівня імітостійкості шифру багатоалфавітної заміни:

$$q_r = (n - 1)^{-r}. \qquad (3)$$

Тобто, складність задачі підробки повідомлень, які зашифровані за допомогою багатоалфавітної заміни зростає залежно від кількості символів, що підробляються, за експоненціальним законом (відповідно, зменшується ймовірність правильного угадування).

Загалом оцінка, нерівність, а також рівняння (2-3) дозволяють раціонально обрати величину степені підстановок. Зважаючи необхідність врахування вимоги що зручності

застосування запропонованої методики у вигляді програмних реалізацій доцільно обирати значення степені підстановки такі, що узгоджуються з форматами даних у мікропроцесорах, а саме: $n = 2^m$, де $m = 2,4,8$ (зауважимо, що для $m = 1$ шифр багатоалфавітної заміни перетворюється у звичайний шифр гамування по mod 2).

В таблиці 1 наведені характеристики методики генерації послідовності підстановок для випадків $n = 4,16,256$.

№ №	Характеристики методики		Степінь підстановки		
			4	16	256
1.	q_1	Імовірність вгадування 1 символу	0.333	0.067	0.008
2.	N	Стійкість при повторі ключа	2	8	128
3.	S	Швидкодія порівняно з МБН (%)	138.6	277.2	554.5
4.	V	Обсяг двійкової РРВП для генерації однієї підстановки (біт)	8	64	4096

Табл. 1. Розрахункові характеристики розробленої методики генерації підстановок

На підставі аналізу таблиці можливо відмітити, що характеристики імітостійкості та криптографічної стійкості при повторі ключа для $n = 2^2$ є найгіршими, а у випадку $n = 2^8 = 256$ найкращими. Але останній варіант внаслідок занадто великого обсягу вихідної РРВП призведе до суттєвого уповільнення процесу шифрування порівняно з іншими варіантами. Тому для практичного застосування пропонується обирати степінь підстановок $n = 2^4 = 16$.

Література:

1. Гулак Г.М. Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури. / Гулак Г.М., Складанний П.М. // II Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одесса, 17 листопада 2017р.). – Одесса: ОДУВС, 2017 – С.12-14.

2. Гулак Г. М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г. М. Гулак, В. Л. Бурячок, П. М. Складанний // Захист інформації. – 2017. – №2. – С. 173–177.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. – М.: Гелиос АРВ, 2005, - 160 с.

4. Духин А.А. Теория информации: Учебное пособие. – М.; Гелиос АРВ, 2007. -248с., ил. ISBN 978-5-85438-168-0

УДК 004.056.5:004.75

Т.А.Радівілова[1], М.Х. Тавалбех[1]
[1]Харківський національний університет радіоелектроніки
tamara.radivilova@gmail.com
tavalbeh@icloud.com

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ПРИ НАЯВНОСТІ САМОПОДІБНИХ ВЛАСТИВОСТЕЙ ВХІДНОГО ТРАФІКУ

Виявлення вторгнень (атак) - це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку ознак можливих інцидентів. Мережеві системи виявлення та запобігання вторгнень (NIDS/NIPS, Network Intrusion detection system/Network Intrusion prevention system) це необхідний елемент захисту від мережевих атак. Найбільш часто використовується розподілена архітектура, в якій кожен датчик NIDS аналізує отриманий трафік на наявність незаконних мережевих дій і, при необхідності, генерує попередження. Вузьким місцем, що впливає на продуктивність мережі, є швидкість обробки вхідних даних мережевим пристроєм безпеки.

ЗМІСТ