УДК 003.26.09 : 004.056.55

Д. М. Самойленко[1]

[1]канд. фіз.-мат. наук., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНОГО РЕСУРСУ

Запропоновано ряд заходів з покращення комплексної системи захисту інформаційного ресурсу з використанням криптографічних та стеганографічних принципів.
Ключові слова: захист інформаційних ресурсів, інформаційна безпека.

Постановка проблеми

Класично, існує два найбільш поширені методи захисту інформації, яка передається відкритим каналом: криптографічний та стеганографічний. Незважаючи на наявність криптографічно надійних рішень для реалізації конфіденційності при роботі з відкритими каналами, найбільш поширені протоколи обміну гіпертекстовими документами не передбачають жодних захисних рішень щодо передавання даних.

Сервери установ, для яких необхідне збереження конфіденційності зберігають у базах даних хеш-образи даних, проте, при самій авторизації дані передаються через незахищені канали у неперетвореному вигляді. Частково безпека покращена у протоколі HTTPS (HTTP Secure), проте, для його реалізації необхідна реєстрація у центрах сертифікації, що, неодмінно, супроводжується фінансовими витратами та рівнем довіри до відповідних центів сертифікації, що спряжене, зокрема, з проблемами міждержавного визнання сертифікатів.

При меншій популярності, стеганографічні методи дістають ґрунтовну математичну основу, яка наближає ці методи за надійністю до криптографічних, а ряд інших переваг, на зразок прихованості та швидкодії, значно підвищує актуальність їх дослідження.

Поєднання засобів захисту утворює комплексну систему захисту інформаційного ресурсу (КСЗІР).

Аналіз публікацій

Більшість комунікацій у Інтернеті здійснюється через транспортні протоколи: гіпертекстовий (HTTP) та файловий (FTP), які за своєю структурою є відкритими і не передбачають обмін конфіденційною інформацією. У той же час існує ряд можливостей забезпечення захисту інформації у відкритому каналі.

У роботі [1] наведено порівняльний аналіз методів комп'ютерної стеганографії у застосуванні для задач захисту інформаційних ресурсів. Проведений аналіз особливостей використання стеганографічних методів у модулях перевірки автентичності інформаційних ресурсів дозволив висловити пропозиції щодо впровадження у такі модулі методів динамічної стеганографії з вибором текстових стегоконтейнерів за принципом цифрових «водяних» знаків.

У роботах [2-4], зокрема, наводяться алгоритми обміну ключами, відомі як алгоритми Діффі-Хеллмана. Зазначені алгоритми призначені для роботи у відкритих каналах

і, при адаптуванні їх для обмінних протоколів, можуть покращити функціонування КСЗІР.

Математичні основи функціонування сучасної стеганографії, розроблені у роботі [5]. У роботах [6-7] розглянуто обмеження, які накладає на стегометоди теорія інформації. У [6] розглянуто один вид атак, у [5, 7] атаки розділені на вторгнення (impersonate) та підміну (substitution [5], spoofing attack [7]).

Метою роботи є розширення можливостей використання криптографічного та стеганографічного підходів до покращення КСЗІР.

Основна частина

Доведена (напр. [2]) можливість обміну даними у відкритих мережах за допомогою протоколів Діффі-Хеллмана дозволяє реалізувати модуль обміну конфіденційною інформацією у відкритих мережах без необхідності звернень до центів сертифікації.

У принципі функціонування протоколу Діффі-Хеллмана покладено можливість генерування випадкових чисел збоку сервера та клієнта незалежно. Слід наголосити саме на незалежності генераторів випадкових чисел з двох боків. Наприклад, посилання сервером випадкового числа клієнту не покращить захищеність інформаційного ресурсу, оскільки перехоплення передачі буде супроводжена перехопленням сеансового ключа протоколу.

Головна особливість ненав'язливої (прихованої) роботи реалізованого алгоритму полягає у тому, що гіпертекст, переданий сервером, має містити активні частини, які виконаються на клієнтському апаратному забезпеченні і у результаті згенерують випадкове число, величина якого буде по-перше, унікальна для кожного клієнта (при одному сервері) та, по-друге, недоступна для перехоплення у каналі комунікацій клієнт-сервер.

Головну проблему становить відсутність узгодженості між кодуваннями символів, доступних у серверній та клієнтській частинах. Засобами серверної мови PHP доступне перетворення символів у 1-байтній системі ASCII, у той же час клієнтська мова JavaScript (JS) дозволяє лише Unicode трансформацію. Для символів російської і, особливо, української абетки відсутнє аналітичне узгодження кодів символів.

У якості розв'язку проблеми узгодження кодів пропонується використання кросмасиву, побудованому з порядкових кодів ASCII символів у таблиці Unicode. Мовою JS функція визначення ASCII коду матиме вигляд:

```
function ASCII(n){
        var
codes=[1026,1027,8218,1107,8222,8230,8224,8225,8364,8240,1033,8
249,1034,1036,1035,1039,1106,8216,8217,8220,8221,8226,8211,8212
,152,8482,1113,8250,1114,1116,1115,1119,160,1038,1118,1032,164,
1168,166,167,1025,169,1028,171,172,173,174,1031,176,177,1030,11
10,1169,181,182,183,1105,8470,1108,187,1112,1029,1109,1111,1040
,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051,1052,10
53,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064,1065,
1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,107
8,1079,1080,1081,1082,1083,1084,1085,1086,1087,1088,1089,1090,1
091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1101,1102,1103
];
        if(n<128) return n;
         else return 128+codes.indexOf(n);}
```

Для забезпечення принципової випадковості даних клієнта ураховується динаміка руху маніпулятора «миша» на відповідному комп'ютері клієнта. Для збільшення ентропії випадкового числа дві координати вказівника, доступні для оброблення, додаються.

Додаткова зовнішня ентропія у формуванні випадкового числа може походити від

показів дати та часу користувача. У цьому аспекті можна вважати, що дані про час на клієнтському боці є унікальними, оскільки більшість персональних комп'ютерів досить рідко синхронізовані з службами точного часу. У такій ситуації навіть повністю одночасні звернення серверу до різних клієнтів призведе до формування різних часових міток збоку клієнта. Додаткове джерело ентропії випадкових чисел може бути використано від функції Math.random().

При відправленні даних від клієнта до сервера згенероване випадкове число використовується у стандартній реалізації протоколу Діффі-Хеллмана, а введені дані кодуються по одному байту з використанням відповідного узгодження кодів до 1-байтового розміру.

В основу динамічного методу текстової стеганографії покладено метод знаків однакової форми. Відповідно до зазначеного методу, передбачається заміна літер української (або російської) абетки на символи латинської абетки, що мають однаковий нарис, проте різні коди символів. Аналіз природної статистики літер засвідчує достатність тексту зі 113 літер задля успішного використання запропонованого стегометоду.

Динамічність методу полягає у періодичному оновленні змісту стеганографічного повідомлення – використовувати у якості стегоінформації дати і часу.

Ентропійні обмеження щодо атаки вторгнення, відомі також як межа Сіммонса, задаються наступним виразом [6]:

$$\log_2 P_d \geq H(\mathrm{MES}) - H(\mathrm{E}) - H(\mathrm{M}) \qquad (1)$$

де P_d – імовірність успішної атаки, H – функція інформаційної ентропії: H(M) – ентропія каналу (множини повідомлень), H(E) – множина правил перетворень, H(MES) – сумісна ентропія множин повідомлень (M), правил перетворень (E) та джерела (S).

Для довільного способу подання часу сумісна ентропія дорівнюватиме нулю, оскільки для заданого стану джерела S (часу) та вибору способу перетворення (E) зміст стеганографічного повідомлення (M) обраховується єдиним чином.

Ентропія множини повідомлень відповідає кількості біт, які виділяються для збереження стегоінформації, ентропія способів перетворень відповідає кількості обраних способів представлення дати і часу. У разі використання лише одного способу H(E)=0. Для кількох рівноімовірних способів $H(\mathrm{E})=\log_2 N$, де N – кількість способів. Якщо способи обираються з різною імовірністю необхідно використати формулу Шеннона для інформаційної ентропії. Проте, останнє не вбачається за доцільне, оскільки за аксіомами Хінчіна ентропія максимальна саме для рівноімовірних подій.

Окремо слід розглянути атаки підміни. Подібні атаки полягають у спробі підміни стегоінформації за результатами аналізу декількох перехоплених повідомлень. При цьому атаку вторгнення можна розглядати як атаку підміни при нульовій кількості перехоплень [7].

Імовірність атаки підміни може бути обчислена за формулою (1), але вирази для ентропій мають бути замінені на умовні H(M) -> $H(\mathrm{M}|m_1 m_2\ldots)$, де m_1, m_2 – перехоплені повідомлення [7].

Для обчислення відповідних умовних ентропій слід визначити кількість біт у представленні стегоінформації, які зазнають змін у кожному наступному повідомленні. Незмінні біти зловмисник використає «як є» і лише змінні біти визначатимуть ентропію множини повідомлень.

Практична реалізація полягає у створенні масивів літер однакового нарису (один масив містить українські літери, інших – латинські):

```
  $cont_symbols=array("a","c","e","i","o","p","x","A","C","
E","I","O","P","X","M","H","K","T");
```

```
$steg_symbols=array("a","c","e","i","o","p","x","A","C","E","I","O","P","X","M","H","K","T");
```

Введення стегоінформації реалізується побітно для кожної літери (у циклі) командою

```
if($sym&$bit_mask[$data_bit])$res[$cont_pos]=$steg_symbols[$num];
```

з використанням масиву бітових масок

```
bit_mask=array(1,2,4,8,16,32,64,128);.
```

Відновлення стегоінформації відбувається шляхом бітового синтезу кодових байтів збоку клієнта: `bait |= bit_mask[bit_pos];`

Одночасне поєднання засобів криптографічного та стеганографічного захисту інформаційного ресурсу суттєво покращує КСЗІР. У найгіршому випадку використання однобайтного ключа (8 біт) та двобайтного подання дати-часу від стандартної функції (16 біт) імовірність атак вторгнення та підміни зменшиться у $2^{(8+16)} \approx 16$ млн. разів. Використання більшої бітової розмірності ключа та стегоповідомлення може суттєво покращити наведене значення.

Висновки

Наведено пропозиції використання засобів криптографічного та стеганографічного перетворень для покращення комплексної системи захисту інформаційного ресурсу.

Запропоновано модифікації криптографічного протоколу Діффі-Хеллмана та стеганографічного принципу цифрових водяних знаків для покращення надійності захисних рішень.

Проведено оцінку надійності систем автентифікації, заснованих на динамічній текстовій стеганографії.

Перспективи подальших розвідок вбачаються у дослідженні більш широкого спектру криптографічних перетворень та стеганографічних інтервенцій у комплексну систему захисту інформаційного ресурсу.

Література

1. К. М. Новосьолова Порівняльний аналіз методів комп'ютерної стеганографії. – Матеріали всеукраїнської НТК з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК. – 2012. – с.188-193
2. Шнайер Б. Прикладная криптография.– М.: Триумф, 2002. – 816 с.
3. А. В. Аграновский, Р. А. Хадим Практическая криптография: алгоритмы и их программирование. – М.: Соломон-пресс. – 2009. – 256 с.
4. Захарченко М. В., Йона Л. Г., Щербина Ю. В., Онацький О. В. Розвинення криптології та її місце в сучасному суспільстві. – Одеса: ОНАЗ ім. О. С. Попова. – 2003. – 80 с.
5. G. J. Simmons. The Prisoners' Problem and the Subliminal Channel. – Advances in Cryptology Lecture Notes in Computer Science. – 1985. – Vol. 209. – pp. 364-378.
6. G. J. Simmons. Authentication Theory / Coding Theory. – Advances in Cryptology Lecture Notes in Computer Science. – 1985. – Vol. 196. – pp. 411-431.
7. D. Y. Pei. Authentication Schemes. – Singapore: Institute for Mathematical Sciences. – 2001. – 36 p. [WWW document] URL: www2.ims.nus.edu.sg/Programs/coding/files/dypei.ps

Надійшла до редколегії 28.05.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

Д.М. Самойленко

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО РЕСУРСА

Предложено ряд мер по улучшению комплексной системы защиты информационного ресурса с применением криптографических и стеганографических принципов.

Ключевые слова: защита информационного ресурса, информационная безопасность.

D.M. Samoylenko

COMPLEX PROTECTION SYSTEM IS INFORMATION RESOURCES

Several improvements were proposed for increasing the reliability of complex security system for information resource with use of crypto- and stego-principles.

Keywords: information resource security, information security.