УДК 004.056.53

О.В. Нарожний,
к.т.н.,
Одеський національний політехнічний університет
e-mail: spawns7650@ukr.net

В.В. Коленко,
аспірант,
Одеський національний політехнічний університет
e-mail: violka86@mail.ru

ПРАКТИЧНІ ОЦІНКИ СТІЙКОСТІ СИСТЕМ

В.В. Коленко, О.В. Нарожний. **Практичні оцінки стійкості систем.** Розглянуто існуючі види атак на стегосистеми з цифровим водяним знаком. Запропоновано використання мультиагентних технологій для вирішення проблеми захисту даних стегосистем.

V.V. Kolenko, A.V. Narozhnij. **Analysis of attacks and defence methods of steganosystems.** The existent types of attacks are considered on steganosystems with a digital threadmark. The use of multi-agent technologies is offered for the decision of problem of data protection for steganosystems.

Вступ. У порівнянні з досить добре дослідженими криптографічними системами поняття й оцінки безпеки стеганографічних систем більш складні й допускають більшу кількість їх тлумачень. Зокрема, недостатнє теоретичне і практичне обробка питань безпеки стегосистем, так і більшою розмаїтістю завдань стеганографічного захисту інформації.

Матеріал і результати дослідження. Стегосистеми водяних знаків, зокрема, повинні виконувати завдання захисту авторських прав на електронні повідомлення при різних спробах активного порушника перекручування або стирання вбудованої в них аутентифікуючої інформації. Отже, системи цифрових водяних знаків (ЦВЗ) повинні забезпечити аутентифікацію відправників електронних повідомлень. Подібне завдання може бути покладена на криптографічні системи електронного цифрового підпису (ЕЦП) даних, але на відміну від стегосистем водяних знаків, відомі системи ЕЦП не забезпечують захист авторства не тільки цифрових, але й аналогових повідомлень. Інші вимоги по безпеці пред'являються до стегосистем, призначеним для приховання факту передачі конфіденційних повідомлень від пасивного порушника. Також має свої особливості забезпечення імітостійкості стегосистем до введення в схований канал передачі помилкової інформації.

Як і для криптографічних систем захисту інформації безпека стегосистем описується й оцінюється їхньою стійкістю. Під стійкістю різних стегосистем розуміється їхня здатність приховувати від порушника факт схованої передачі повідомлень, здатність протистояти спробам порушника зруйнувати,

спотворити, видалити передані повідомлення, а також здатність підтвердити або спростувати дійсність переданої інформації.

Досліджуємо стегосистеми, завданням яких є схована передача інформації. У криптографічних системах ховається зміст конфіденційного повідомлення від порушника, у той час як у стеганографії додатково ховається факт існування такого повідомлення. Тому визначення стійкості й злому цих систем різні. У криптографії система захисту інформації є стійкою, якщо маючи у своєму розпорядженні перехоплену криптограму, порушник не здатний читати повідомлення, що втримується в ній. Неформально визначимо, що стегосистема є стійкою, якщо порушник спостерігаючи інформаційний обмін між відправником й одержувачем, не здатний виявити, що під прикриттям контейнерів передаються приховувані повідомлення, і тим більше читати ці повідомлення.

У ряді стегосистем необхідно відновлювати контейнер, тому що він фізично являє собою звичайні повідомлення (зображення, мовні сигнали й т.п.) кореспондентів відкритого зв'язку, під прикриттям яких здійснюється схований зв'язок. Ці повідомлення відкритого зв'язку повинні доставлятися їхнім одержувачам з якістю, обумовленою встановленими вимогами до вірогідності відкритого зв'язку. Однак навіть якщо використовуваний контейнер є тільки переносником приховуваного повідомлення, ступінь припустимої погрішності контейнера також повинна бути обмеженої, тому що інакше порушник легко виявить факт використання стегосистеми.

Стійкість стегосистеми повинна забезпечуватися при використанні несекретних (загальновідомих) функцій вбудовування. Безпека стегосистем повинна опиратися на такі принципи їхньої побудови, при яких якщо порушник не знає секретної ключової інформації, то навіть при повнім знанні функцій вбудовування приховуваної інформації, законів розподілу приховуваних повідомлень, контейнерів і стего він не здатний установити факт схованої передачі інформації.

Уведемо моделі порушника, що намагається протидіяти прихованню інформації. Випливаючи К. Шеннону, назвемо першу із цих моделей теоретико-інформаційною. Нехай, як це прийнято для систем захисту інформації, для стегосистем виконується принцип Кергоффа: порушник знає повний опис стегосистеми, йому відомі імовірнісні характеристики приховуваних повідомлень, контейнерів, ключів, формованих стегограм. Порушник має необмежені обчислювальні ресурси, запам'ятовувальними пристроями довільно великої ємності, має у своєму розпорядженні нескінченно більший час для стегоаналізу і йому відомо довільно велика безліч перехоплених стегограм. Єдине, що невідомо порушникові це використовуваний ключ стегосистеми. Якщо в даній моделі порушник не в змозі встановити, утримується чи ні приховуване повідомлення в спостережуваному стего, то назвемо таку стегосистему

теоретико-інформаційною стійкою до атак пасивного порушника.

Стійкість різних стегосистем може бути розділена на стійкість до виявлення факту передачі (існування) приховуваної інформації, стійкість до добування приховуваної інформації, стійкість до нав'язування помилкових повідомлень по каналу схованого зв'язку (імітостійкість), стійкість до відновлення секретного ключа стегосистеми.

Якщо стегосистема є стійкою до виявлення факту передачі (існування) приховуваної інформації, то логічно припустити, що вона при цьому є стійкою й до читання приховуваної інформації. Зворотне в загальному випадку невірно. Стегосистема може бути стійкою до читання приховуваної інформації, але факт передачі якоїсь інформації під прикриттям контейнера може виявлятися порушником.

Стійкість стегосистеми до нав'язування помилкових повідомлень по каналу схованого зв'язку характеризує її здатність виявляти й відкидати сформовані порушником повідомлення, що вводять їм у канал передачі приховуваних повідомлень із метою видачі їх за дійсні, вихідні від законного відправника. Якщо в системі ЦВЗ зловмисник здатний ввести в контейнер, завірений законним відправником, свій водяний знак і детектор буде виявляти водяний знак зловмисника й не виявляти ЦВЗ дійсного відправника, то це означає дискредитацію (злом) системи ЦВЗ.

Стійкість до відновлення секретного ключа стегосистеми характеризує її здатність протистояти спробам порушників обчислити секретну ключову інформацію даної стегосистеми. Якщо порушник здатний визначити ключ симетричної стегосистеми, то він може однозначно виявляти факти передачі приховуваних повідомлень і читати їх або нав'язувати помилкові повідомлення без усяких обмежень. Така подія можна назвати повною компрометацією стегосистеми. Атаки порушника на ключ стегосистеми можуть бути побудовані аналогічно атакам на ключ систем шифрування інформації й систем аутентифікації повідомлень.

Якщо порушник здатний обчислити ключ вбудовування водяного знака якого-небудь автора (власника) інформаційних ресурсів, то він може поставити цей водяний знак на будь-який контейнер. Тим самим порушник дискредитує або водяний знак даного автора (власника), або цілком всю систему ЦВЗ. В обох випадках ставиться під сумнів законність прав одного або всіх власників інформаційних ресурсів.

Дана проблема має велике практичне значення для захисту авторських прав виробників різного роду інформаційних продуктів, таких як ліцензійне програмне забезпечення, CD й DVD дисків, відео й аудіо і т.п.

Якщо система ЦВЗ побудована як симетрична, то декодер повинен використати конфіденційний ключ виявлення водяного знака. Отже, такий детектор проблематично вбудовувати масово, що експлуатуються пристрої,

до яких доступ порушника технічно складно обмежити, наприклад, у персональні програвачі DVD дисків.

Несиметрична система ЦВЗ використає секретний ключ вбудовування водяного знака в контейнери й відкритий ключ перевірки ЦВЗ. З відкритого ключа перевірки повинне бути неможливо обчислення секретного ключа вбудовування водяного знака. Порушник не повинен бути здатний у контейнер вмонтовувати водяний знак довільного автора (виробника), а сам водяний знак повинен однозначно ідентифікувати цього автора. Вимоги до ключової інформації несиметричних систем ЦВЗ дуже нагадують вимоги до ключів відомих із криптографії систем цифрового підпису даних. При використанні несиметричних систем ЦВЗ можна вбудовувати декодери в будь-яке устаткування, не побоюючись компрометації ключа вбудовування водяного знака. Зрозуміло, при цьому треба виключити можливість обходу порушником системи захисту. Якщо зловмисник здатний відключити детектор ЦВЗ, то він зможе несанкціоновано скористатися платними інформаційними ресурсами. Наприклад, у сучасні DVD пристрою записується інформація про географічний регіон їхнього виробництва й продажу, у межах якого дозволяється або обмежується програвання DVD дисків з відповідними мітками доступу. Росія відповідно до цього розмежування доступу ставиться до регіону, у якому ймовірність електронного злодійства значно вище, ніж, наприклад, у Західній Європі.

Висновки.

Отже, побудова несиметричних систем ЦВЗ й інших стегосистем викликає істотні практичні проблеми.

По-перше, несиметричні системи, як відомо із криптографії, у реалізації виявляються обчислювально складніше симетричних систем.

По-друге, крім вимог до стійкості ключа стегосистеми, пред'являються тверді вимоги до стійкості системи ЦВЗ до різноманітних спроб порушника перекручування водяного знака. Несиметричні системи побудовані на основі односпрямованої функції з потаємним ходом, ідея яких запропонована У.Діффі й М.Хелманом . Принципи побудови переважної більшості відомих односпрямованих функцій з потаємним ходом такі, що будь-яке як завгодно мале перекручування вихідного значення цієї функції при використанні законним одержувачем потаємного ходу приводить до істотного розмноження помилок у прийнятому повідомленні. Цей недолік односпрямованих функцій характерний і для нині використовуваних несиметричних криптографічних систем. Однак його можна компенсувати використанням додаткових заходів підвищення вірогідності переданих криптограм або цифрових підписів повідомлень. Але в стегосистемах використання цих же способів підвищення вірогідності складніше:

- їх застосування демаскує схований канал;

- активний порушник в атаках на стегосистему ЦВЗ має більші можливості підібрати такий руйнуючий вплив, при якому доступні скриваючому інформацію способи підвищення вірогідності можуть виявитися неефективними.

Література

1.Понятие стеганографической стойкости [Електронний ресурс] // URL: http://crypts.ru/ponyatie-steganograficheskoj-stojkosti.html (дата: 10.04.2010)

2.Брюс Шнайдер. Прикладная криптография. 2-е изд. [Текст] – Москва: «Диа Софт», 2000. – 368 с.

3.Грибунин, В.Г., Оков, И.Н., Туринцев, И.В. «Цифровая стеганография» [Текст] – Москва: «СОЛОН-Пресс», 2002. – 272 с.

4.Классификация атак на стегосистемы ЦВЗ [Електронний ресурс] // URL: http://crypts.ru/klassifikaciya-atak-na-stegosistemy-cvz.html (дата: 13.04.2010)

5.Поспелов, Д.А. Искусственный интеллект. Кн. 2. Модели и методы: Справочник [Текст] – Москва: «Радио и связь», 1990. – 304 с.