МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»
ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

РАДА МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

VIII ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

Частина І

24 листопада 2016 р.

м. Дніпро

УДК [004+621.39](06)
І 74
ББК 32.973

Оргкомітет конференції:

Голова:	Декан факультету інформаційних технологій, д.т.н., професор Алексєєв М.О.
Заступник голови:	Голова ради молодих вчених факультету інформаційних технологій Мєшков В.І.
Члени оргкомітету:	д.т.н., професор Корнієнко В.І. к.ф.-м.н., доцент Гусєв О.Ю. к.т.н., доцент Флоров С.В. ст. викл. Кручинін О.В. ст. викл. Мартиненко А.А. ст. викл. Войцех С.І. ас. Масальська О.О.

І 74

Інформаційні технології. Безпека та зв’язок: Матеріали всеукр. наук.-практ. конф. – Дніпро: Державний ВНЗ «Національний гірничий університет», 2016. – 29 с. – Частина І (укр. м., рос. м.).

Викладено тези доповідей учасників VIII Всеукраїнської науково-практичної конференції «Інформаційні технології. Безпека та зв’язок», яка відбулася у Державному ВНЗ «Національний гірничий університет» 24 листопада 2016 року. На конференції було розглянуті найбільш актуальні проблеми розвитку інформаційних технологій, безпеки та зв’язку в Україні та шляхи їх вирішення.

УДК [004+621.39](06)
ББК 32.973

ЗМІСТ

Секція «Кібербезпека»

Секція «Телекомунікації та радіотехніка»

Секція «Кібербезпека»

Голова секції: д.т.н., професор кафедри безпеки інформації та телекомунікацій Корнієнко В.І.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Мєшков В.І.

УДК 004.03142:004.056.5

ВРАЗЛИВОСТІ ПЛАТІЖНИХ ТА ІНФОРМАЦІЙНИХ ТЕРМІНАЛІВ

Автор: Колісніченко Дмитро Вадимович
Керівник – співавтор: Масальська Олена Олександрівна
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, SDKolisnichenko@gmail.com

На сьогоднішній час в більшості сфер IT-діяльності присутні платіжні термінали. Існують вразливості, до яких схильна велика кількість терміналів, такі як: виклик контекстного меню (Tap fuzzing); ведення некоректних даних, що призводить до появи на екрані стандартних елементів операційної системи (Data fuzzing); зовнішні посилання, стандартні елементи інтерфейсу.

Платіжні термінали – це інформаційні системи, що вимагають ретельного дослідження і сучасного захисту.

Ключові слова – термінальне обладнання, зовнішні посилання, інтерактивна графічна оболонка, вразливість, шкідливі додатки.

ВСТУП

У 21 столітті в більшості культурних, освітніх, розважальних місць присутні платіжні та інформаційні термінали. В цій доповіді, розглянемо термінальне обладнання, яке присутнє в більшості сфер діяльності:

1. Touch – термінали з оплатою різних послуг (квитки, мобільний рахунок, парковки, комунальні послуги, поповнення банківських карт);
2. Інформаційні термінали для пасажирів;
3. Термінальне обладнання в якому присутні «карти», побудова маршрутів.

Чим функціональніший пристрій, тим більше шанс наявності вразливостей в конфігураційній системі. Використання злочинцем термінального обладнанням в своїх цілях, безпосередньо витікають з особливостей.

- доступність;
- велика кількість термінального обладнання, що розташована в публічних місцях;
- обробка особистих даних користувачів;
- однакова структура, в рамках одного типу пристроїв.

У цій доповіді розглянемо деякі елементи, вразливості, недоліки платіжних та інформаційних терміналів [3].

ТЕХНОЛОГІЇ ВИХОДУ З ІНТЕРАКТИВНОЇ ГРАФІЧНОЇ ОБОЛОНКИ

Існує кілька типів вразливостей, до яких схильні дуже багато терміналів. Послідовність дій для виходу з графічної оболонки проілюстрована на рисунку 1.

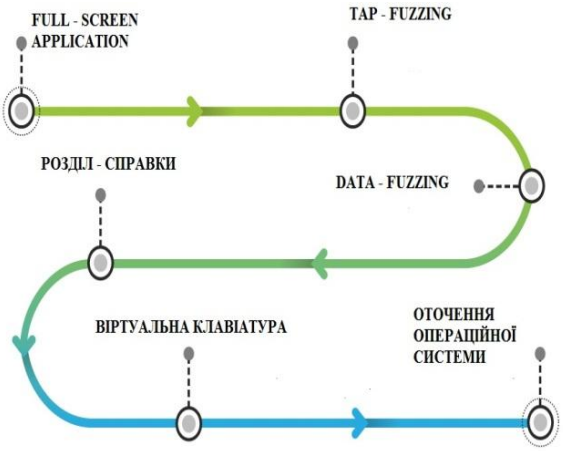


Рисунок 1. Основні дії для виходу з графічної оболонки

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ

В технічному сенсі все термінальне обладнання – це звичайні персональні комп'ютери з сенсорним екраном. Одна з основних відмінностей в них, це інтерактивна графічна оболонка, в якій присутня оплата послуг. Графічна оболонка перекриває первинні функції операційної системи. У деяких терміналів відсутній надійний захист від виходу з даного режиму, що тягне за собою повне отримання доступу і функціоналу операційної системи [2].

Розглянемо технологію «Tap fuzzing», що являє собою вихід з повноекранного додатка за рахунок некоректної обробки. Зловмисник намагається знайти в інтерактивній графічній оболонці вразливі місця, за допомогою тривалого натискання на них, за рахунок чого викликається контекстне меню операційної системи. При знаходженні даної уразливості зловмисник намагається відкрити командний рядок, за допомогою якого може заходити на жорсткий диск,

встановлювати шкідливі програми, виходити в мережу [2].

Технологія «Data fuzzing» при вдалому використанні також призводить до появи на екрані елементів операційної системи. Зловмисник намагається спровокувати некоректну роботу термінального обладнання. Даний метод може спрацювати, якщо розробник не зміг налаштувати коректно фільтр на обмеження вводимих даних (наявність спеціальних символів, довжини рядка, розмір символу). Наприклад, зловмисник вніс некоректні дані в додаток, і ця помилка розробки призведе до відкриття вікна операційної системи [2].

Присутні інші способи виходу з інтерактивної графічної оболонки, на деяких терміналах фігурують зовнішні посилання (Facebook, Google +, Вконтакте).

Ще одним способом виходу за межі інтерактивної графічної оболонки можуть стати стандартні елементи інтерфейсу операційної системи. Якщо в даному терміналі встановлена операційна система сімейства Windows, є можливість, що зловмисник зможе викликати елементи управління діалоговим вікном, це дозволить залишити середу графічної оболонки [2].

Не можна забувати і про термінал в якому присутні карти. Деякі розробники в термінальне обладнання встановлюють карти від компанії «Google», при цьому «Google» має «віджет», у якому містяться такі елементи: «Повідомлення про помилку», «Конфіденційність», «Умови використання». Перехід по кожній з цих посилань гарантує попадання в браузер [1].

Розглянемо термінали, які обслуговують пасажирів. Важлива відмінність даного термінального обладнання в тому, що вони працюють з особистою інформацією клієнтів. В даних терміналах також присутня деяка подоба інтерактивної графічної оболонки. В більшості таких пристроїв використовується політика фільтрації веб-сайтів. Проте доступ і керування даною політикою відкритий, при бажанні зловмисник може видалити або додати будь-який сайт.

Наприклад, вільний доступ до фішингових сайтів, шкідливих сайтів.

Так само присутні вразливості перегляду бази даних. Якщо є можливість виходу з інтерактивної графічної оболонки, будь-який зловмисник може переглянути всю інформацію про клієнтів з їх логінами та паролями [3].

Вразливості термінального обладнання в параметрах друку також присутні. Після того, як користувач заповнив всі поля, він вводить реквізити і натискає кнопку "створити", термінал на обмежений час відкриває вікно друку, в якому присутні всі можливі параметри друку.

В такому випадку у зловмисника є обмежений час натиснути клавішу для зміни параметрів друку, після чого він зможе потрапити в довідковий розділ операційної системи. З даного розділу зловмисник може потрапити на панель керування або викликати віртуальну клавіатуру. За допомогою даної вразливості зловмисник зможе переглядати інформацію про вже роздрукованих раніше квитанції, запускати шкідливий код та інше [2].

ВИСНОВОК

Успішно проведена атака на термінальне обладнання може заподіяти прямі фінансові витрати його власнику. Зловмисник може використовувати "підлеглий" термінал для злому інших, адже вони часто об’єднані в мережу.

Для того що б мінімізувати шкідливу активність на публічних пристроях, потрібно використовувати такі методи:

- в інтерактивної графічній оболонці не повинно знаходитись зайвих функцій, які дозволять вийти за межі даної оболонки;
- додаток необхідно запускати за допомогою технології «пісочниця»;
- дані зберігати на сервері, якщо зловмисник видалив додаток з термінального обладнання, основна інформація про користування цим додатком залишиться на сервері;
- обмежити привілеї звичайного користувача – це утруднить встановлення нових додатків на сервері;
- для кожного пристрою повинен бути окремий логін і пароль, щоб не дозволити зловмиснику скомпрометувати один термінал, а потім використовувати отриманий пароль для всіх інших.

З кожним роком термінальна інфраструктура поступово поповнюється все новими пристроями, які пов’язані з іншими пристроями і системами. Термінальне обладнання – це окрема система, яка вимагає спеціального підходу та розробки ефективної системи захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Денис Макрушин, Владимир Дащенко вразливості в платіжних та інформаційних терміналах [Електронний ресурс]. – Режим доступу: http://www.kaspe rsky.ru/about/news/virus/2016/fooling- the-smart-city, вільний;

2. Денис Макрушин, Владимир Дащенко розумне але не безпечне місто [Електронний ресурс]. Режим доступу: https://securelist.ru/analysis/obzor/29286/fooling-the-smart-city/, вільний;

3. Кенін А.М. Практичне керівництво системного адміністратора. – СПБХ. БХВ – Петербург, 2010. – 464 с.: ил. – (Системний адміністратор);

УДК 044.056

АНАЛІЗ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Савич Ю.О., к.т.н., доцент Вовк Р.Б., к.т.н., доцент Пасєка М.С.
Івано-Франківський національний технічний університет нафти і газу, http://nung.edu.ua/,
E-mail: julliasavych@gmail.com

В даному дослідженні виконано аналітичний огляд методів застосування криптографічного та стеганографічного захисту інформації в програмних додатках та комп'ютерних системах. Проведено групування алгоритмів шифрування даних на дві групи з подальшим їх аналізом та описом перспектив використання.

Ключові слова – криптографія, стеганографія, алгоритм, програма, алгоритм шифрування, стійкість.

ВСТУП

Проблема захисту інформаційних ресурсів набуває все більш важливого значення, хоча вона є однією із найскладніших задач. В першу чергу, це пояснюється прискореними темпами науково-технічного прогресу, результатом якого є нові технічні та електронні засоби, які становлять небезпеку виникнення каналів витоку інформації. Також одним із факторів, які визначають трудомісткість вирішення завдань захисту інформації, є розширення кола користувачів, що мають доступ до ресурсів комп'ютерної системи і масивів даних, які знаходяться в ній.

Для вирішення цієї проблеми потрібна система заходів, головною ціллю якої є попередження від несанкціонованого доступу, наслідком якого може бути втрата, модифікація і витік інформації. Проведений аналіз літератури [1-3] показав, що серед багатьох організаційних, програмних і системних мір криптографія є одним з основних інструментів, що забезпечують секретність і цілісність інформації, авторизацію, електронні платежі, оперативний контроль за процесами управління й обробки даних.

Швидкий розвиток інформаційних технологій привів до нових досягнень в сфері безпеки інформації, яка є дуже важливою для сучасного суспільства. Питання розроблення та впровадження методів захисту інформації є актуальними не лише для криптографії та стеганографії, а й для майже всіх галузей науки, враховуючи високу автоматизацію різних сфер людської діяльності. До початку XX століття криптографія була пов'язана з лінгвістичними схемами. Довгий час криптографія залишалася секретною діяльністю спецслужб і державних структур. Вона також сприяла розвитку електронно-обчислювальної техніки – перші такі машини були створені для злому шифрів військових [1]. Перетворившись на загальнопоширений інструмент передачі та захисту даних, сучасна криптографія базується на математичному апараті, що включає теорію ймовірності та абстрактну алгебру. Основним завданням математики в криптографії є забезпечення криптографічної стійкості, тобто здатності протистояти практичному злому. Криптографічна стійкість визначається кількістю затраченого часу і ресурсів, щоб із шифр тексту відновити вихідний відкритий текст. Результатом стійкої криптографії є шифртекст, що винятково складно зламати без володіння визначеними інструментами по дешифруванню.

ОСНОВНА ЧАСТИНА

Криптографія – наука про способи перетворення інформації з метою її захисту від несанкціонованого доступу. Одним із видів такого перетворення є шифрування, яке забезпечує практичну неможливість читання або модифікації інформації зловмисниками. Існує цілий ряд алгоритмів шифрування даних, які можна розбити на дві великі групи, що показано на рис. 1.

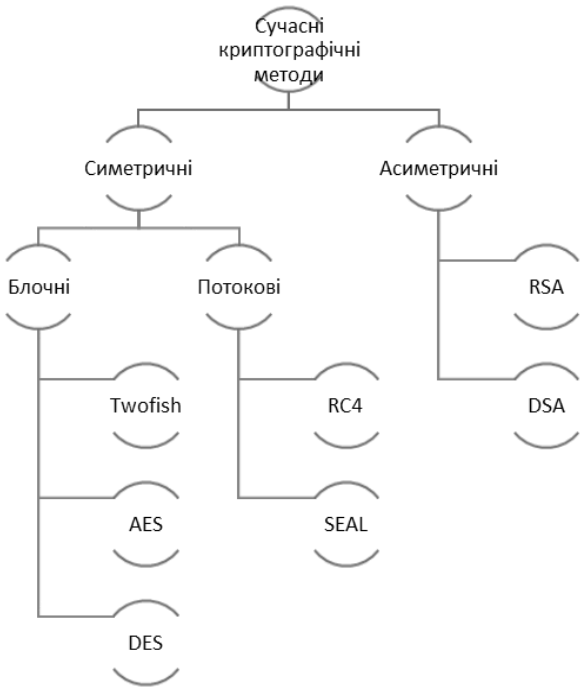


Рисунок 1. Алгоритми криптографії

Проведемо порівняльний аналіз симетричної та асиметричної криптографії. Характерною рисою симетричної системи є використання одного і того ж ключа для виконання операції шифрування і розшифрування, яке можливе лише тоді, якщо існує безпечний канал передачі інформації. Це не стосується військової справи, розвідки, фінансово-кредитних операції тощо. У таких ситуаціях використовують асиметричні алгоритми шифрування. Дані системи криптографічних перетворень характеризуються тим, що для шифрування даних

використовується один ключ (відкритий, тобто доступний користувачам), а для розшифрування – інший (секретний) ключ. Ця властивість дозволяє в певній мірі вирішити проблему розподілу ключів між користувачами, яка є основним недоліком симетричних систем. Для гарантії захисту даних, до асиметричних систем шифрування ставляться дві найважливіші умови [2]:

- перетворення відкритого тексту повинно бути незворотнім і виключати його відновлення на основі відкритого ключа;
- визначення секретного ключа на основі відкритого має бути неможливим для сучасного рівня розвитку обчислювальних засобів.

Вирішення задач автентифікації, розповсюдження ключів відкритими каналами зв'язку, застосування електронного підпису реалізується лише засобами асиметричної криптографії. Однак слід зазначити, що алгоритми асиметричних криптосистем настільки трудомісткі в порівнянні зі звичайними симетричними алгоритмами, що на практиці раціонально їх використовувати там, де обсяг шифрованого інформації незначний, але дуже важливий. Практичний досвід показує, що застосування асиметричних алгоритмів шифрування не дозволяє забезпечити інтерактивний режим роботи сучасних інформаційно-телекомунікаційних систем. Таким чином, очевидна необхідність використання в таких системах пристроїв шифрування, які побудовані на симетричних криптографічних алгоритмах.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення, блочні алгоритми, в свою чергу, працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам, але, в алгоритмі AES використовуються блоки довжиною 128 біт. Симетричні алгоритми шифрування не завжди використовуються самостійно. В сучасних криптоситемах, використовуються комбінації симетричних та асиметричних алгоритмів, для того, аби отримати переваги обох схем. До таких систем належить SSL, PGP та GPG. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів. До деяких відомих, поширених алгоритмів з гарною репутацією належать: Twofish, Serpent, AES, Blowfish, CAST5, RC4 та IDEA [3].

В цілому ряді задач для повноцінного забезпечення інформаційної безпеки використання лише криптографічних методів є недостатнім, оскільки вони не дозволяють приховати власне факт передачі й зберігання конфіденційної інформації. Подібні задачі можливо вирішувати з застосуванням методів крипто-стеганографічних алгоритмів. Крипто-стеганографічна система захисту інформації – це складний інформаційний комплекс методів та засобів, загальна стійкість якого залежить від правильного узгодження криптографічної і стеганографічної складових системи. Ключову роль при цьому відіграють алгоритми узгодження, які дають змогу перетворити рівномірно розподілені бітові послідовності, отримані на виході криптографічних алгоритмів, на бітові послідовності, аналогічні тим, що використовуються для вкраплення стеганографічними алгоритмами у пусті контейнери. Вимогою коректного використання цих алгоритмів є точна статистична відповідність вхідних і вихідних даних. Інтеграція крипто-стеганографічних алгоритмів дає можливість позбутися вразливих сторін відомих методів захисту інформації та розробити ефективніші з позицій обчислювальної складності і стійкості до зламу нові методи розв'язання задач інформаційної безпеки як програмного додатку так і інформаційних потоків даних.

ВИСНОВОК

Автоматизація призводить до зростання загроз несанкціонованого доступу до інформації, як наслідок, до необхідності постійної підтримки і розвитку системи захисту. Захист інформації є не разовим заходом і навіть не сукупністю заходів, а безперервним процесом, який повинен реалізовуватися на всіх етапах життєвого циклу автоматизованої системи обробки інформації. Підвищення продуктивності обчислювальної техніки і поява нових видів атак на шифри веде до зниження стійкості відомих криптографічних алгоритмів. Таким чином, використовувані криптографічні засоби повинні постійно оновлюватися. Підтримка і забезпечення надійного функціонування механізмів системи захисту інформації може здійснюватися лише висококваліфікованими фахівцями, які можуть гарантувати надійність використовуваних алгоритмів і програмних засобів, що реалізують функції захисту інформації.

Отже, в пропонованому дослідженні виконано порівняльний аналіз методів криптографічного захисту інформації, наведена їх класифікація, визначено переваги та недоліки і здійснено опис практичного використання описаних методів у різних системах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с. Дошина А. Д., Михайлова А. Е., Карлова В. В.

2. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] // Современные тенденции технических наук: материалы IV междунар. науч. конф. (г. Казань, октябрь 2015 г.). – Казань: Бук, 2015.

3. Венбо Мао Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. – М.: Вильямс, 2005. – 768 с. – 2 000 экз. – ISBN 5-8459-0847-7, ISBN 0-13-066943-1

УДК 004.056.57

ИССЛЕДОВАНИЕ МЕТОДОВ И АЛГОРИТМОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

Богиня И. Г., Масальская Е. А.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: big94@ua.fm

В данной статье рассматриваются основные методы и алгоритмы обнаружения сетевых аномалий и атак, проводится сравнительный анализ данных алгоритмов, а также рассматривается применимость этих алгоритмов в качестве базы для создания системы обнаружения сетевых аномалий.

Ключевые слова – сетевые аномалии; системы обнаружения аномалий.

ВСТУПЛЕНИЕ

Одной из актуальных задач в сфере информационной безопасности является создание системы обнаружения нестандартной сетевой активности. Реализацию данной задачи осложняет тот факт, что почти каждый день появляются новые виды сетевых атак и инструментов воздействия на объекты сетей, что приводит к ошибкам в работе систем обнаружения вторжений (СОВ) и обнаружения аномалий (СОА). При анализе состояния сети, для минимизации ошибок, генерируемых СОВ и СОА, привлекают экспертов в области ИБ. Однако, присутствие человека в системе в качестве звена, принимающего какие-либо решения, может приводить к повышению числа невзвешенных и импульсивных решений в виду особенностей человеческого поведения.

Для снижения влияния человеческого фактора на процессы почти любой производственной сферы внедряют автоматизацию данных процессов. В сфере информационной безопасности важными процессами, влияющими на состояние информации и рассматриваемой информационной системы, являются процессы мониторинга состояния всех информационных ресурсов, а также процессы реакции на обнаруженные аномалии. В данном случае, под аномалиями подразумеваются любые отклонения состояний объектов системы от эталонных для таковых.

ОСНОВНАЯ ЧАСТЬ

Обнаружение аномалий – динамический метод работы антивирусов, хостовых и сетевых систем обнаружения вторжений. Программное обеспечение, использующее этот метод, наблюдает определённые действия (работу программы/процесса, параметры сетевого трафика, работу пользователя), следя за возможными необычными и подозрительными событиями или тенденциями.

Одним из важных аспектов необходимости проведения мониторинга работы ИС является то, что наличие аномалии может указывать на проводимую в настоящем времени атаку на информационные ресурсы данной ИС. Рынок программных и программно-аппаратных продуктов, задачей которых являются мониторинг состояния ИС и осуществление реакций на возникновение аномалий, насчитывает немало позиций таких, как: Catchi, Zabbix, Nagios, Ganglia, Snort и другие [1].

В случаях, когда в ИС возникает аномалия и необходимо предпринять ответные действия, которые не могут быть просчитаны ни одной из имеющихся СОВ, привлекают экспертов в области ИБ. Но, если речь идет о реализации угроз для критической информации, время для ответных действий по защите сокращается практически до нуля, что накладывает существенные временные ограничения на процессы привлечения экспертов. Из-за этого возникает необходимость создания системы, способной реагировать на возникающие в ИС аномалии в режиме реального времени. Некоторые из вышеприведенных продуктов справляются с задачей не только мониторинга, но и обнаружения и предотвращения вторжений и атак, но качество обнаружения атак напрямую зависит от вида проводимой атаки. Некоторые СОВ работают по сигнатурному принципу, что позволяет хорошо обнаруживать множество распространенных видов атак, для которых собрано много информации, описывающей данные атаки. Но недостатком таких систем является их неспособность дать адекватный ответ на атаку, для который в базе знаний СОВ нет никакой информации. В таких случаях используют СОВ, основанные на эвристических алгоритмах. Однако, такие системы также не могут работать в полном диапазоне возможных видов атак из-за самого определения эвристических методов поиска решений: данные алгоритмы не имеют доказанной правильной логики для всех возможных вариантов решаемых задач.

Одним из возможных вариантов построения данной системы является моделирование поведения эксперта в сфере ИБ в ситуации возникновения аномалии. В подавляющем большинстве случаев, логика мышления человека, который должен рассуждать рационально и взвешенно принимать решения, возможно описать математическими моделями такими, как деревья принятия решений [2].

В широком смысле, деревья принятия решений – средство поддержки принятия решений, использующееся в статистике и анализе данных для прогнозных моделей. Структура дерева представляет собой «листья» и «ветки». На ребрах («ветках») дерева решения записаны атрибуты, от которых зависит целевая функция, в «листьях» записаны значения целевой функции, а в остальных узлах – атрибуты, по которым различаются случаи. Чтобы классифицировать новый случай, необходимо спуститься по дереву до листа и выдать

соответствующее значение. Цель состоит в том, чтобы создать модель, которая предсказывает значение целевой переменной на основе нескольких переменных на входе.

Существуют различные реализации данной модели, такие как: алгоритмы CART, C4.5, CHAID, CN2, NewId, ITrule и т.д. Наиболее часто из них применяются алгоритмы CART и C4.5 [3].

Алгоритм CART принципиально отличается от некоторых других алгоритмов конструирования деревьев решений механизмом отсечения ветвей. В рассматриваемом алгоритме отсечение – это некий компромисс между получением дерева «подходящего размера» и получением наиболее точной оценки классификации. Также для применения алгоритма CART нет необходимости заранее выбирать переменные, которые будут участвовать в анализе: переменные отбираются непосредственно во время проведения анализа на основании значения индекса Джини (показателя неравномерности распределения некоторой величины на заданном интервале).

Однако, данный алгоритм не лишен недостатков. В случае, когда необходимо построить дерево со сложной структурой, лучше использовать другие алгоритмы, т.к. CART может не идентифицировать правильную структуру данных.

Алгоритм C4.5 является усовершенствованной версией алгоритма ID3. В частности, в новую версию были добавлены отсечение ветвей, возможность работы с числовыми атрибутами, а также возможность построения дерева из неполной обучающей выборки, в которой отсутствуют значения некоторых атрибутов.

В обучающей выборке количество примеров должно быть значительно больше количества классов, к тому же каждый пример должен быть заранее ассоциирован со своим классом. По этой причине C4.5 является вариантом машинного обучения с учителем.

Одним из алгоритмов, адаптированных для максимально гетерогенных входящих данных, является алгоритм Random forest – алгоритм машинного обучения, предложенный Лео Брейманом и Адель Катлер, заключающийся в использовании комитета (ансамбля) решающих деревьев. Алгоритм применяется для задач классификации, регрессии и кластеризации [4].

Классификация объектов проводится путём голосования: каждое дерево комитета относит классифицируемый объект к одному из классов, и побеждает класс, за который проголосовало наибольшее число деревьев.

Оптимальное число деревьев подбирается таким образом, чтобы минимизировать ошибку классификатора на тестовой выборке. В случае её отсутствия, минимизируется оценка ошибки «out-of-bag»: доля примеров обучающей выборки, неправильно классифицируемых комитетом, если не учитывать голоса деревьев на примерах, входящих в их собственную обучающую подвыборку.

Главными достоинствами данного алгоритма являются:

- способность эффективно обрабатывать данные с большим числом признаков и классов;
- нечувствительность к масштабированию (и вообще к любым монотонным преобразованиям) значений признаков;
- одинаково хорошо обрабатываются как непрерывные, так и дискретные признаки. Существуют методы построения деревьев по данным с пропущенными значениями признаков;
- существуют методы оценивания значимости отдельных признаков в модели;
- внутренняя оценка способности модели к обобщению (тест «out-of-bag»);
- высокая параллелизуемость вычислений и масштабируемость.

Учитывая вышеописанные особенности алгоритма Random forest, а также его способность воспринимать широкий диапазон входных данных, данный алгоритм является наиболее подходящим для реализации в качестве основы системы поиска и ответа на обнаруженные аномалии в ИС.

Применять данный алгоритм возможно на нескольких этапах формирования реакции на возникшую аномалию. Сначала необходима кластеризация данных, полученных от модуля мониторинга разрабатываемой СОВ. После этого возможно непосредственное создание набора ответных действий, которое также осуществляется при помощи данных, представляемых на выходе моделью «случайного леса».

Необходимо отметить, что адекватность создаваемых реакций будет напрямую зависеть от объема и достоверности данных, полученных от модуля мониторинга СОВ.

ЗАКЛЮЧЕНИЕ

В качестве базы для создания описанной системы реагирования на аномалии рекомендуется выбирать математические модели такие, как модель комитета деревьев решений Random forest, т.к. в сравнении с вышеперечисленными моделями данный алгоритм наименее требователен к типизации входных данных (что свойственно специфике работы системы обнаружения аномалий в случае обнаружения нового типа аномалии), а также является особо эффективным при обработке данных с большим количеством признаков, что, соответственно, существенно повышает точность выходных данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). 2-е изд. М.: КМК, 2016. – 223 с.

2. Паклин Н.Б., Орешков В.И. Бизнес-аналитика: от данных к знаниям: учебное пособие. 2-е изд. СПб: Питер, 2013. – 704 с.

3. Толстова Ю.Н. Анализ социологических данных. М.: Научный мир, 2000. - 352 с.

4. Проталинский О.М. Применение методов искусственного интеллекта при автоматизации технологических процессов. АГТУ, 2004. – 183 с.

УДК 004.056

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ВЫМОГАТЕЛЬСТВА И МЕТОДЫ БОРЬБЫ С НИМ

Кот Л.Л., Кручинин А.В.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/,E-mail: leon.k91@yandex.ua

В данных тезисах рассматривается вредоносное программное обеспечение для вымогательства, особенности его функционирования, способы его проникновения в систему и методы борьбы с ним.

Ключевые слова – вредоносное программное обеспечение для вымогательства, ransomware, cerber, teslacrypt, cryptxxx, malvertising.

ВВЕДЕНИЕ

Программное обеспечение (ПО) для вымогательства или Ransomware – такой вид вредоносного ПО, который при попадании в компьютер или мобильное устройство блокирует доступ или шифрует хранящиеся файлы, а для восстановления управления компьютером или файлами пользователю необходимо отправить требуемую сумму на указанный счет.

Средняя сумма выкупа – 679 долларов США [3]. Распространенный способ оплаты выкупа – в биткоинах.

Среди общего количества обнаруженного ПО для вымогательства 64% составляет криптографическое ПО [1].

Между 2013 и 2014 годами количество видов криптографического ПО для вымогательства увеличилось на 250% [1].

Согласно данным Лаборатории Касперского, статистика по этому виду угрозы выглядит следующим образом [2]:

- процент пострадавших от программ, шифрующих файлы, вырос на 25%, с 6.6% в 2014 – 2015 гг. до 31.6% в 2015 – 2016;
- количество пользователей, столкнувшихся с программами блокировки компьютера снизился на 13.03%, с 1836673 в 2014-2015 годах до 1597395 в 2015-2016 годах;
- количество пользователей, столкнувшихся с ПО для вымогательства при пользовании мобильными устройствами, выросло в 4 раза: с 35413 пользователей в 2014-2015 до 136532 в 2015-2016 гг.

ВИДЫ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА

На данный момент существуют 2 вида программного обеспечения для вымогательства [1], [2]:

- блокирующее ПО (computer locker);
- вредоносное ПО с криптографическими функциями (data locker).

БЛОКИРУЮЩЕЕ ВРЕДОНОСНОЕ ПО ДЛЯ ВЫМОГАТЕЛЬСТВА (COMPUTER LOCKER)

Данный вид ПО разработан с целью блокировки доступа пользователя к компьютеру. Как правило, функциональность заблокированного компьютера ограничена, мышь может быть отключена, а на клавиатуре могут работать только цифровые клавиши для ввода платежного кода [1].

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С КРИПТОГРАФИЧЕСКИМИ ФУНКЦИЯМИ

Данный тип вредоносного ПО разработан с целью поиска и шифрования файлов, хранящихся на атакуемом компьютере.

Доступ к файлам возможен только в случае использования ключа расшифрования, который можно получить только после оплаты суммы, указанной в всплывающем окне при работе компьютера.

Количество пользователей, атакованных криптографическим ПО для вымогательства в Украине в 2014 - 2015 году составило 1.34%, в то время как в 2015 – 2016 году было зарегистрировано уже 28.86% атак [2].

Для шифрования используются такие алгоритмы шифрования, как RSA – 1024, 3DES, AES [1].

СЕМЕЙСТВА ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА

На данный момент самыми распространенными семействами вредоносного ПО для вымогательства являются: Teslacrypt, Cerber, CryptXXX [2], [3];

Для контактов с жертвами злоумышленники используют сеть Tor, предоставляющую анонимное сетевое соединение, защищённое от прослушивания.

Некоторые семейства вирусов имеют дополнительные функции. CryptXXX способен добавить инфицированный компьютер в ботнет, и этот компьютер может быть затем использован для осуществления DDoS – атак [3].

СПОСОБЫ ПРОНИКНОВЕНИЯ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА В СИСТЕМУ

Существуют следующие способы проникновения данного вредоносного ПО в систему:

- спам и социальная инженерия (письма электронной почты от Интернет-провайдера, счет по коммунальным платежам, письмо от банка, при переходе по ссылке, указанной в письме или загрузке

прикрепленного файла, вирус попадает в систему [3], [4]).

- через уязвимости операционной системы [4];
- скачивание вредоносного контента с заражённых веб-сайтов (вредоносное ПО, встроенное в бесплатное ПО, аудио и др. файлы) [1];
- malvertising – распространение через рекламные сети Yahoo!, YouTube, Skype [4].

СПОСОБЫ ПРЕДОТВРАЩЕНИЯ ПРОНИКНОВЕНИЯ ВРЕДОНОСНОГО ПО ДЛЯ ВЫМОГАТЕЛЬСТВА В СИСТЕМУ И МЕТОДЫ БОРЬБЫ С НИМ

1. Включение в настройках системы отображения расширения файлов, это поможет определить, например, не был ли загружен файл аудиозаписи .mp3 с расширением .exe [2].
2. Использование обновляемого антивирусного ПО.
3. Регулярное обновление ОС и установленного ПО (Adobe Flash, Java, Chrome, Firefox, Internet Explorer, Microsoft Windows, Office) [2].
4. Создание образа системы средствами ОС или с помощью специализированных программ.
5. Регулярное создание резервных копий ценных файлов или на внешнем носителе, или с помощью OneDrive for Business компании Microsoft [5].
6. Не открывать письма электронной почты от незнакомых отправителей.
7. Компании Лаборатория Касперского, Intel, Symantec разработали инструменты для определения типа угрозы и ее устранения [6], [7].

ВЫВОДЫ

В данных тезисах представлена информация о вредоносном ПО для вымогательства, способах его проникновения в систему, способах предотвращения проникновения и методах борьбы с ним.

Среди указанных в тезисах способов предотвращения проникновения вредоносного программного обеспечения и борьбы с ним следует выделить основные: использование антивирусного программного обеспечения, резервное копирование файлов на съемный носитель. Антивирусными средствами, обладающими функциями обнаружения и удаления вредоносного ПО для вымогательства являются: Kaspersky Internet Security, Kaspersky Anti-Ransomware Tool for Business, Bitdefender Total Security Multi-Device (предоставляет защиту для Windows, Mac OC и Android), Norton Power Eraser.

Резервное копирование может быть организовано:

- стандартными средствами в системе;
- программой Acronis True Image;

Учитывая увеличение разнообразия устройств, подключаемых к Интернет, все они могут быть подвержены атакам вредоносного программного обеспечения, следовательно, уязвимыми могут оказаться: часы, системы Smart Home (Умный дом), телевизоры, кондиционеры, стиральные машины, холодильники и другая бытовая техника, транспортные средства. Это влечет за собой необходимость в создании и применении дополнительных методов, способов и средств защиты от вредоносного ПО для вымогательства, ориентированных на конкретное защищаемое устройство.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Kevin Savage, Peter Coogan, Hon Lau - «Эволюция вредоносного программного обеспечения для вымогательства» [Электронный ресурс] – [Веб-сайт] - Режим доступа: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
2. Securelist.com - «Отчет сетевой безопасности Касперского: Вредоносное программное обеспечение в 2014 – 2016 годах» [Электронный ресурс] – [Веб-сайт] – Режим доступа: https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
3. Symantec.com - «Специальный отчет об угрозах безопасности в Интернет: Ransomware и бизнес» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
4. Владимир Безмалый: «Деньги или данные? Что такое Ransomware.» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.pcweek.ru/security/article/detail.php?ID=175237
5. Alexs Pena – «Как справиться с Ransomware» [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://blogs.technet.microsoft.com/office365security/how-to-deal-with-ransomware/
6. Проект «Больше никакого выкупа» инструменты для расшифрования файлов [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.nomoreransom.org/decryption-tools.html
7. Программы для расшифрования файлов, разработанные Лабораторией Касперского [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://noransom.kaspersky.com

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Амиров Николай Гурамович, Кручинин Александр Владимирович
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, E-mail: kenobi@ukr.net

В работе проведен сравнительный анализ методик тестов на проникновение. Целью является выявления сильных и слабых сторон каждой методики. Сформулирована задача разработки методики, соотносящейся с требованиями, выдвигаемыми законодательством Украины.

Ключевые слова – тест на проникновение, пентест, методология.

ВВЕДЕНИЕ

С увеличением зависимости компаний любого направления деятельности от ИТ технологий, остро встает вопрос обеспечения информационной безопасности [1]. Одним из ключевых мероприятий в обеспечении информационной безопасности компании является тестирование на проникновение. Это позволяет удостовериться в надежности защиты от НСД и прочих угроз ИБ [4]. В Украине отсутствует единая утвержденная методика тестов на проникновение. В связи с этим предлагается провести анализ имеющихся методик для последующей разработки новой методики, подходящей для Украинских стандартов.

ОБЗОР МЕТОДИК ПРОНИКНОВЕНИЯ

1. Методология OSSTMM – The Open Source Security Testing Methodology Manual.

Является достаточно формализованным и хорошо структурированным документом для тестирования сети. Документ имеет так называемую «Карту безопасности» – визуальный показатель безопасности. На карте указываются основные области безопасности, которые включают в себя наборы элементов, которые должны быть протестированы на соответствие методике.

В документе присутствует подпункт «Методология» / «Тестирование технологии интернет-безопасности» / «Обзор сети» / «Тестирование Межсетевого экрана», где перечислена ожидаемая информация, которую может получить взломщик в результате удачной атаки или отсутствия нужной функции у средства защиты. Также описываются конкретные корректные реакции сети на атаки и их наличие, например, измерение времени отклика на пакет или проверка наличия потерь пакетов на маршруте к цели. Минусами методики считается формализованность и отсутствие дополнительного описания к требованиям [2].

2. Методология NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment.

Создана и поддерживается подразделением NIST – CSRC, центром по компьютерной безопасности, объединяющий специалистов федеральных служб, университетов, крупнейших ИТ-компаний США.

В разделе «Техники оценки уязвимостей цели», в качестве одной из техник описываются Тесты на проникновение, а именно Фазы и Логистика тестов. По данному документу тесты на проникновение, в дополнение к стандартным их возможностям, можно применять для определения:

- насколько хорошо система переносит реально существующие модели атак;
- примерного уровня сложности, который необходимо преодолеть атакующему;
- дополнительных мер противодействия, которые могли бы ослабить угрозы в адрес системы;
- способности защищающего систему на обнаружение атак и обеспечение соответствующей реакции на них [2].

3. Методология BSI – Study A Penetration Testing Model.

Разработана немецким подразделением «Federal Office for Information Security». В документе описывается проведение корректных испытаний системы на прочность. Подробно описываются не только сама методология тестов, но и необходимые требования, правовые аспекты применения методологии и процедуры, которые необходимо выполнить для успешного проведения тестов.

Приводится классификация тестов на прочность и определены ее критерии. В приложениях содержатся описание ПО, которое можно использовать для тестирования объектов, описанных в методике. Методика является достаточно подробной и старается предусмотреть все аспекты тестов на прочность, как технические, организационные, так и правовые [2].

4. Методология ISSAF – Information System Security Assessment Framework.

Разработан OISSG (Open Information Systems Security Group) для внутренних контрольных проверок.

Документ охватывает огромное количество вопросов, связанных с информационной безопасностью. Присутствуют главы, описывающие оценку безопасности межсетевых экранов, маршрутизаторов, антивирусных систем и много другого [2].

5. Методология OWASP (Open Web Application Security Project) Testing Guide.

OWASP (Open Web Application Security Project) – международное открытое сообщество, нацеленное на улучшение безопасности программного обеспечения. Каждый имеет право участвовать в OWASP, и все их материалы свободно распространяемы. OWASP Testing Guide представляет собой более широкую

методологию по сравнению с другими, т.к. дает указания не только по тестам на проникновение, но и по анализу вэб-приложений в целом (к примеру – исходного кода), поскольку эта методика фокусирует свое внимание именно на обнаружениях уязвимостей вэб-приложений [3].

6. Обзор методологии PTES – Penetration Testing Execution Standard – Technical Guidelines.

Стандарт, разработанный для объединения как бизнес требований, так и возможностей служб безопасности, и масштабирования тестов на проникновение. На первом подготовительном этапе подробно рассматриваются устанавливаемые каналы коммуникаций, правила взаимодействия и контроля, конкретные способы реагирования и мониторинга инцидентов. Далее выделены следующие этапы:

- сбор информации;
- моделирование угроз;
- методы анализа уязвимостей;
- эксплоитация – обеспечение обхода контрмер и обнаружение наилучшего пути атаки;
- пост-эксплоитация – анализ инфраструктуры, последующее проникновение в инфраструктуру, зачистка и живучесть.

Определена структура отчетов, составляемых по результатам тестирования [2].

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ПРОНИКНОВЕНИЯ

В таблице 1 приведен фрагмент сравнительной таблицы методик по подробности описания и раскрытию каждого этапа проникновения по шкале от 0 до 10, где 0 – не раскрыто совсем, 10 – раскрыто максимально точно.

Для общей сравнительной оценки методик были предложены следующие критерии:

- описание информации, которую может получить взломщик – насколько четко в рамках методологии определены типы информации, которую возможно получить в результате взлома;
- описание целей тестирования на проникновение – насколько точно отражен ожидаемый результат при применении методологии;
- подробность описания методики;
- подробность описания пунктов;
- подробность описания классификации тестирования на проникновение;
- наличие классификаций уязвимости;
- подробность классификации уязвимостей;
- наличие списка рекомендуемых утилит для тестов;
- подробность описания использования утилит;
- восприятие;
- общая оценка методологии.

Фрагмент общей сравнительной таблицы методик приведен в таблице 2.

Таблица 1. Фрагмент сравнительной таблицы методик по подробности описания

Методологии / Этапы	OSSTMM	NIST SP 800-115	BSI	ISSAF	OWASP	PTES
Подготовка						
1. Утверждение с заказчиком режимов тестирования	7	1	0	5	0	7
2. Оформление и подписание договора	7	1	0	5	0	7
Выполнение тестов						
1. Сбор информации об объекте	1	4	8	8	8	7
2. Идентификация уязвимостей	1	3	8	8	8	8

Таблица 2. Фрагмент общей сравнительной таблицы методик

Методологии / Критерий	OSSTMM	NIST SP 800-115	BSI	ISSAF	OWASP	PTES
1. Описание информации, которую может получить взломщик	8	1	0	2	5	0
2. Описание целей тестирования на проникновение	4	5	10	1	10	5
3. Подробность описания методики	4	9	7	6	10	10

ВЫВОД

Используя результаты анализа можно приступить к разработке единой методики, удовлетворяющей требованиям украинского законодательства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уязвимости веб-приложений [Электронный ресурс]:[https://habrahabr.ru/company/pt/blog/268779/].
2. Сравнительный анализ методик оценки межсетевых экранов [Электронный ресурс]: [http://ojs.ifmo.ru/index.php/IMS/article/viewFile/34/35].
3. OWASP Testing Guide v4.0 [Электронный ресурс]: [https://www.owasp.org/index.php/Category:OWASP_Testing_Project].
4. Тест на проникновение – Агентство Активного Аудита [Электронный ресурс]: [http://auditagency.com.ua/?r=blog&p=Pentest]

УДК 004.421

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РОБОТИ ПРОТОКОЛУ КРИПТОВАЛЮТИ ETHEREUM

Масальська Олена Олександівна [1], Мєшков Вадим Ігорович [2]
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: elmasalskaya@yandex.ua [1], local@i.ua [2]

В роботі розглянуто особливості роботи протоколу криптовалюти Ethereum. Розглянуті вразливості та недоліки роботи алгоритму ДАО (децентралізована автономна організація Ефіріума).

Ключові слова – криптовалюта, Ефіріум, Ethereum, Біткойн, Bitcoin, вразливості криптовалюти, децентралізована автономна організація

ВСТУП

На сьогоднішній день широкого застосування набувають ідеї відходу від традиційних грошей та розвитку грошей електронних. Найвідомішою електронною валютою (або криптовалютою) є Біткойн (Bitcoin). Але через особливості свого алгоритму, Біткойн зараз знаходиться на фінальній стадії генерації монет і із часом поступиться в популярності більш новим криптовалютам, таким як, наприклад, Ефіріум (Ethereum) [1].

Ефіріум позиціонує себе як принципово нова платформа для додатків. Це відразу і платформа, і мова програмування, яка дозволяє розробнику створювати і публікувати розподілені додатки наступного покоління. Ефіріум є різновидом Біткойн, що використовує повну за Тюрінгом мову програмування замість простої мови сценаріїв. Причина цього полягає в тому, що Ефіріум підтримує смарт-контракти. Ефір, внутрішня валюта Ефіріума, діє як «знак обміну» всередині цієї децентралізованої мережі. Мережа може використовуватися для шифрованої і безпечної передачі будь-яких видів інформації: результатів голосування, доменного імені, процесів управління компанією, договорів та угод, а також для спрощення обороту смарт-власності, операцій на фінансових біржах і «краудфандінга» [2].

ОСОБЛИВОСТІ РОБОТИ АЛГОРИТМУ ЕФІРІУМ

Децентралізована Ефіріума концепція запозичена у мережі Біткойн. Однак, протокол Ефіріума є відкритим. Його скриптова мова (на відміну від безальтернативного розрахунку хеш-функції та застосування сценаріїв в Біткойн) може використовуватись для побудови будь-якої програми. При цьому, оригінальну програму можна описати будь-якою мовою програмування з подальшим виконанням в «хмарі». Ефіріум об'єднує переваги технології «блокчейн» і переваги Тюрінг-повних мов програмування.

Окремі облікові одиниці, кожна з яких має назву «1 Ефір» (1 Ethereum – ринкова ціна складає 9,97119548$ – дані на 13 листопада 2016р.), виступають будівельними блоками. Блоки функціонують всередині загальної мережі. Кожен з них являє собою комп'ютерну програму, у якій є свій власний баланс, пам'ять і код. На їх основі будуються додатки з відкритим вихідним кодом.

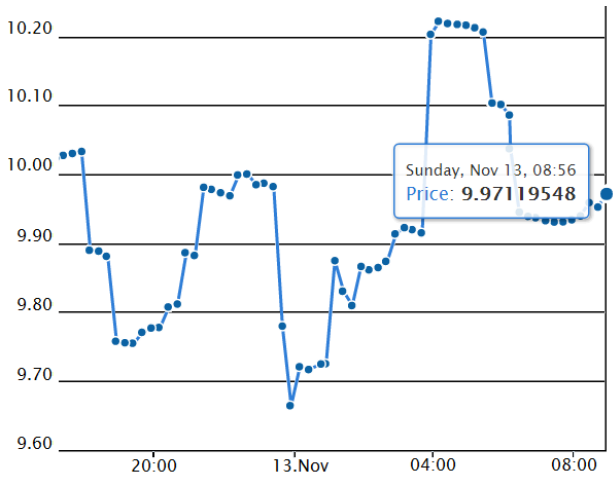


Рисунок 1. Ринкова ціна 1 Ethereum / 1 US Dollar (джерело: https://www.coingecko.com).

На алгоритмі Ефіріума заснований відомий проект «ДАО» (децентралізована автономна організація) - краудфандінговий проект, який позиціонує себе як організація, заснована на хмарному коді, яка не є юридичною особою і керована колективно усіма її інвесторами. Тобто, ДАО закрита і сама керує собою: її програмний код здійснює свою діяльність автономно, а внутрішні правила є невід'ємною і незмінною частиною Ефіріум-блокчейна [3]. ДАО володіє наступними характеристиками:

- по-перше, слід зазначити абсолютну неупередженість у відборі учасників. Використовуючи реалізацію розумних контрактів від Ефіріум, ДАО дозволяє бажаючим з усього світу брати участь в управлінні загальним фондом коштів. Учасники, що підтримали проект, отримують DAO-токени для подальшого їх використання в голосуванні та іншої діяльності компанії.
- по-друге, ДАО – це гнучка структура. Це проявляється в тому, що принцип роботи організації дозволяє підтримувати пропозиції будь-якого характеру, будь то створення корисного для неї продукту, вкладення коштів у венчурні проекти для отримання прибутку або їх спрямування на

благодійні потреби (порятунок китів, наприклад). Учасники можуть проголосувати за виділення коштів на пропозиції інноваційного характеру, за подальшу практичну реалізацію яких візьмуться залучені виконавці.

- по-третє, ДАО може отримувати прибуток з розроблюваних в рамках проекту продуктів або послуг. З клієнтів стягується плата, а потенційний прибуток може бути спрямований на подальше зростання організації або просто конвертований в ДАО-токени і розподілений серед учасників проекту.

ВРАЗЛИВОСТІ ТА НЕДОЛІКИ АЛГОРИТМУ

При всій своїй зовнішній привабливості Ефіріум не позбавлений деяких недоліків. Наприклад, є одна частина системи, яка не захищена криптографічно. Припустимо, за товар відправлено 100 монет, і нехай це цифровий товар з миттєвою доставкою. Далі зловмисник переводить ті ж монети собі, і намагається переконати мережу, що друга угода повинна знаходиться на першому місці, і саме вона є справжньою. Для цього йому буде потрібно роздвоїти ланцюжок блоків. А, так як найдовший ланцюжок за замовчуванням є правдою, зусилля зловмисника в кінцевому рахунку приречені на невдачу. Але це звичайно, до тих пір, поки він не зосередить 51% потужності мережі в одних руках [4].

Також у червні 2016 року, в коді ДАО (платформи для автономного управління інвестиційним капіталом), був виявлений несподіваний «баг», який дозволив хакеру витонченими методами вивести деяку кількість коштів. Ця вразливість була експлуатована невідомою стороною, якій вдалося перемістити близько однієї третини валюти Ефіріум, наявної в ДАО (на той час на суму близько 50 мільйонів доларів США), в одну з дочірніх ДАО, контроль над якою був тільки в атакуючої сторони. Однак, завдяки особливості реалізації ДАО всі ці кошти були недоступні для виведення протягом місяця. Розглянемо більш докладно принцип атаки [3].

Припустимо учасник ДАО хочу вийти з інвестиційної схеми та вивести свої кошти з проекту. Для цього йому необхідно надати ДАО частину свого власного коду з транзакцією для передачі йому Ефіріум-монет. Код Ефіріум є рекурсивним, що означає, що функція, що реалізує Ефіріум, може визивати сама себе.

На цьому етапі може виникнути помилка, що полягає в тому, що, коли викликається функція Ефіріума, вона буде викликати код одержувачів для передачі Ефіріум-монет, після чого код одержувачів буде викликаний ще раз, перш ніж закінчити процес. Це змушує процес повторюватися, передаючи більше Ефіріум-монет, ніж потрібно насправді (рисунок 2).

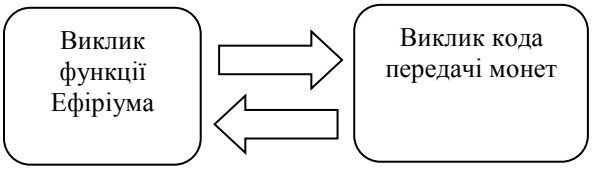


Рисунок 2. Рекурсивний виклик функції Ефіріума

Цей процес може тривати нескінченно, поки не дістане всі монети ДАО, що зможуть бути використані зловмисником за місяць.

Тобто, Ефіріум має вразливості, що закладені самим математичним алгоритмом (навіть, не його програмною реалізацією), усунути які на сьогоднішній день не представляється можливим. Але великим полем для діяльності є часовий проміжок в місяць, в який зловмисник ніяк не зможе використати монети, отримані в процесі атаки. Тобто, актуальним напрямком наукових досліджень є пошук методів «відкату» операцій зловмисника з метою повернення нелегально здобутих коштів законному власникові. Але не треба забувати й про правовий аспект питання: всі дії з повернення коштів повинні проводитися тільки після однозначної ідентифікації факту порушення, що само собою являю нетривіальний процес.

ВИСНОВКИ

Протокол Ефіріума був задуманий як модернізована версія криптовалюти, що забезпечує розширені функції за допомогою вельми узагальненої мови програмування. Він дозволяє підтримувати довільні контракти, що теоретично можуть бути створені для будь-якого типу транзакцій або додатків. Протокол Ефіріума сьогодні вийшов далеко за межі тільки валюти. Поняття довільної функції стану переходу, що реалізована протоколом Ефіріума, забезпечує платформу з унікальним потенціалом, що це дуже добре підходить в якості основного шару для дуже великого числа фінансових і нефінансових протоколів в наступні роки за умови знаходження ефективного алгоритму нейтралізації розглянутих вразливостей.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ethereum. Вікіпедія [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Ethereum

2. Ethereum. Блог [Електронний ресурс]. – Режим доступу: https://blog.ethereum.org/

3. Bitcoin конференція [Електронний ресурс]. – Режим доступу: https://bitcoinconf.com.ua/ru/news/4-samie-prodavaemie-knigi-o-bitcoin-obzor/

4. О Биткоине и блокчейне. Форум [Електронний ресурс]. – Режим доступу: https://forum.bits.media/index.php?/topic/21907-piat-neobkhodimykh-knig-o-bitkoine-i-blokcheine/

УДК 004.056:004.087.2

ВІДНОВЛЕННЯ ДАНИХ НА ФЛЕШ-НОСІЯХ В КОМПЛЕКСНІЙ СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ

Автор: Гроссман Юлія Олександрівна,
Керівник – співавтор: Кручінін Олександр Володимирович
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail: mohyr_ulchic@mail.ru

Розглянуто процес відновлення даних на флеш-носіях та його вплив на захист інформації в автоматизованих системах (АС).

Визначені критерії, які пов'язані з задачею відновлення даних на флеш-носіях. Виконано аналіз методів та засобів по відновленню інформації на флеш-носіях.

Ключові слова – Відновлення даних на флеш-носіях, флеш-пам'ять, пошкодження інформації, способи відновлення, критерії захищеності інформації, структура файлової системи, повторне використання об'єктів.

ВСТУП

За останні роки пристрої із застосуванням технології флеш-пам'яті є невід'ємною частиною життя сучасної людини. Завдяки своїй компактності і високій щільності запису, цей тип носія інформації міцно зайняв положення на ринку цифрових пристроїв – фото і відеокамер, диктофонів, MP3-плеєрів, КПК, мобільних телефонів, а також смартфонів і комунікаторів. Крім того, зовнішня флеш-пам'ять активно застосовується для зберігання і резервування інформації та використовується в якості ідентифікатора в АС. Тому порушення цілісності або обмеження доступу до інформації, що зберігається на флеш-носіях, може привести до втрати важливих даних або до призупинення роботи АС.

Можливі причини втрати даних на флеш-носіях:

1. Вірусна атака на комп'ютер.
2. Випадковість. Видалення файлів з флеш-носія, комп'ютера або ноутбука ненавмисним чином.
3. Форматування диска або карти пам'яті.
4. Апаратні і механічні ушкодження.

Усі ці чинники можуть вивести флеш-пам'ять з ладу повністю або частково.

ОБГРУНТУВАННЯ ВИБОРУ КРИТЕРІЇВ ЗАХИСТУ

Для формалізації оцінки впливу на рівень захисту інформації в АС порушень функціонування флеш-носіїв, необхідно виконати аналіз критеріїв захищеності.

Різні відмови флеш-носіїв впливають на окремі критерії.

В наслідок помилкового форматування, дій вірусів та випадкового видалення будуть порушені критерії цілісності. В першу чергу це послуга ЦО – відкат. Особливо небезпечно, якщо флеш-накопичувач використовувався для резервного копіювання. якщо флеш-накопичувач використовувався як основний носій, або імпорту/експорту інформації, то будуть порушені і ЦА/ЦД.

Апаратних ушкодження контролера або стабілізатора напруги впливатимуть на реалізацію послуги ДВ – відновлення після збоїв, яка відноситься до критеріїв доступності.

Крім того, особливості технології та схемо технічних рішень, які використовуються в флеш-накопичувачах, не гарантують видалення інформації при її перезаписі. Це порушує послугу КО – повторне використання об'єктів, яка відноситься до критеріїв конфіденційності. Це, в свою чергу, спричиняє невиконання послуги КК – аналіз прихованих каналів.

Таким чином, відмови флеш-накопичувачів, при використанні їх в АС, можуть привести до невиконання цілої групи послуг, які є обов'язковими майже в кожній комплексній системі захисту інформації.

Відновлення даних на флеш-носіях є достатньо складною технічною задачею. В деяких випадках відновлення інформації можливе без застосування спеціалізованого обладнання. В інших випадках доводиться звертатись в спеціалізовані центри. Використання таких центрів, як правило, не можуть гарантувати повну конфіденційність відновлюваних даних**,** до того ж це віднімає немало часу і засобів.

Для аналізу методів та засобів по відновленню даних на флеш-носіях, необхідно враховувати особливості технологій створення та організації флеш-накопичувачів.

АЛГОРИТМ РОБОТИ ФЛЕШ-ПАМ'ЯТІ

Флеш пам'ять – є таким типом пам'яті, що може працювати без живлення довготривалий час зберігаючи необхідну інформацію.

Флеш пам'ять зберігає інформацію в масиві «комірок», кожна з яких традиційно зберігає по одному біту інформації. Кожна комірка – це транзистор із плавним затвором.

До флеш – пам'яті типу NAND-Flash відносять такі накопичувачі як: USB Flash, SSD-диски, карти пам'яті SD, miniSD, microSD, xD, MS, M2, Compact Flash.

Найбільш розповсюджені технічні несправності флеш-носіїв:

1. Логічні несправності (можливо відновити дані за допомогою програм для відновлення даних).
2. Механічні пошкодження (можливо замінити несправний компонент або відновити порушений

контакт, чи зчитати дані безпосередньо з чипа пам'яті, використовуючи спеціальне устаткування).

3. Електричні пошкодження (заміна компонентів або читання з чипів пам'яті).

Відновлення даних на носіях пам'яті – процедура зчитування інформації з запам'ятовуючого пристрою у деяких ситуаціях, коли вона не може бути прочитана звичайним способом. Відновлення може здійснюватися з будь - якого комп'ютерного носія.

Існує три методи доступу до мікросхеми:

1. Звичайний доступ (Conventional). (Використовується при зчитуванні невеликої кількості інформації з мікросхеми пам'яті, асинхронний доступ).

2. Пакетний (Burst). (Швидке послідовне читання даних, повільний доступ при читанні певних осередків пам'яті, синхронний доступ).

3. Сторінковий (Page). (Дуже швидкий довільний доступ в межах поточної сторінки, відносно повільне перемикання між блоками, асинхронний доступ).

В загальному випадку є два основних способу відновлення:

1. Програмний спосіб – це вміння відновити інформацію без фізичного втручання в пристрій носія, а також у функціонування мікропрограми і структуру модулів службової інформації.

2. При фізичному пошкодженні накопичувача необхідно використовувати програмно-апаратний спосіб для різних видів інформаційних накопичувачів.

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВІДНОВЛЕННЯ ДАНИХ НА ФЛЕШ-НОСІЯХ

Самий надійний, простий і дешевий спосіб відновлення інформації – це раніше зроблені резервні копії. Для створення резервних копій використовується спеціалізоване програмне забезпечення, яке в тому числі може виконувати відновлення даних.

PC-3000 SSD Flash Edition – програмно-апаратний комплекс, призначений для відновлення інформації з усіх типів накопичувачів на основі NAND флеш пам'яті (USB Flash, SD, MS, xD, MMC, CF, Voice Recorder, iPhone, SSD), у випадках, коли доступ до даних за допомогою штатного інтерфейсу накопичувача неможливий. PC-3000 SSD Flash Edition дозволяє відновлювати дані флеш носіїв з фізичними ушкодженнями, з руйнуваннями службової інформації, з логічними руйнуваннями структур файлової системи.

Комплекс PC-3000 SSD Flash Edition включає в себе спеціалізований пристрій PC Flash Reader для зчитування мікросхем пам'яті NAND Flash і програмне забезпечення для збирання (відновлення) вихідного образу флеш накопичувача.

Основні особливості PC-3000 SSD Flash Edition: наявність автоматичних і ручних режимів відновлення даних; підтримка алгоритмів корекції даних ECC; велика база даних підтримуваних флеш і SSD носіїв; можливість поповнення внутрішньої бази даних мікросхем NAND Flash; підтримка мікросхем в корпусах LGA-52; підтримка ОС Windows x64.

Крім того, на практиці, використовують ще такі програми по відновлюванню даних: Undelete 360, CardRecovery, PhotoRec і Recuva.

Після проведення аналізу програмно-апаратних засобів по відновленню даних на флеш-носіях можна виділити переваги та недоліки методів та засобів.

Переваги:

- великий процент відновлення.
- можливість роботи з безліччю типів носіїв.
- великий набір функцій.
- багато програм з наявністю безкоштовної версії по відновленню даних.

Недоліки:

- у деяких випадках не відновлює вміст файлу.
- деякі програми мають обмеження за розміром відновлюваних файлів.
- не завжди можливо напряму добратися до флеш-пам'яті, так як причиною поломки може бути спалений контролер, або зношені комірки пам'яті.
- є програми з високою вартістю платної версії.

Зворотною задачею відновлення даних є гарантоване знищення інформації з флеш-носія при збереженні його робочого стану. Задача гарантованого знищення інформації з жорстких дисках, розглянута в багатьох джерелах. Для знищення інформації з жорстких дисках розроблені відповідні методи та засоби. Відносно флеш-носіїв, при вирішенні цієї задачі необхідно враховувати особливості алгоритмів читання та запису, фізичної структури, наявності контролера та ін.

ВИСНОВОК

Щоб забезпечити спостережливість, цілісність та конфіденційність інформації при застосуванні флеш-носіїв, після програмного чи програмно-апаратного збою на пристрої, треба використовувати відповідні методи та засоби по відновленню даних. При виконанні цих процедур, необхідно застосовувати додаткові організаційні міри.

Задача гарантованого знищення інформації з флеш-носія при збереженні його робочого стану вимагає додаткового аналізу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стаханов С. Відновлення даних з флеш-носіїв. [Електронний ресурс]. – Режим доступу: http://www.stahanov-rdc.ru/povrejdenie-flash.html

2. Програмне забезпечення комплексу PC-3000 Flash. [Електронний ресурс]. – Режим доступу: http://www.acelab.ru/dep.pc/pc3000.flash.php

3. Відновлення даних з накопичувачів на основі NAND флеш-пам'яті. [Електронний ресурс]. – Режим доступу: http://www.ixbt.com/storage/faq-flash-p0.shtml

УДК 004.7:004.056.5

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ТА ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ WI-FI МЕРЕЖ

Автор: Шовкута Володимир Андрійович
Керівник – співавтор: Флоров Сергій Володимирович
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail: v.shovkuta@gmail.com

Сьогодні все більше користувачів надають перевагу бездротовим мережам Wi-Fi, що міцно посіли важливе місце в нашому житті. Вони дозволяють отримати широкосмуговий доступ до мережі Інтернет, дають можливість обміну файлами у локальній мережі, не застосовуючи кабелі передачі даних. Перебуваючи в громадському місці чи в колі друзів, багато хто починає шукати найближчу точку доступу Wi-Fi, ні на хвилину не замислюючись про питання безпеки при користуванні бездротовими мережами. Слабке уявлення користувачів про загрози в бездротових мережах дозволяють зловмиснику отримати доступ до інформації користувачів, адже завдяки особливостям середовища передачі бездротові мережі не можуть забезпечити розмежування доступу до даних, тому пакети, що передаються клієнтом або точкою доступу, можуть бути отримані будь-яким пристроєм в зоні дії мережі.

Ключові слова – Wi-Fi; бездротові мережі; шифрування, автентифікація, точка доступу, мережеве обладнання, WEP, WPA, WPA2, WPS, WDS.

ВСТУП

За прогнозом компанії Cisco, наведеним у звіті «Наочний індекс розвитку мережевих технологій: повний прогноз на період 2015-2020 рр.» (Cisco Visual Networking Index™ (VNI) Complete Forecast for 2015 to 2020), число точок доступу Wi-Fi в світі (включаючи домашні) виросте семикратно і до 2020 року досягне 432 млн (так, наприклад, показник 2015 року – 64 млн), а на Wi-Fi та мобільні пристрої буде припадати близько двох третин IP-трафіку [1].

А, наприклад, за даними, наведеними в інфографіці для сайту BotRevolt.com, 49 відсотків всіх мереж Wi-Fi є незахищеними, з яких 89 відсотків є мережами, розташованими у громадських місцях, а на маршрутизаторах 80 відсотків сімей у світі досі встановлені паролі за замовчанням [2].

Все це, з огляду на неминуче розповсюдження бездротових мереж та зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки, наприклад:

- розголошення конфіденційної або внутрішньої інформації;
- несанкціонований доступ до інформації;
- вірусна атака;
- компрометація облікових записів;
- перевищення повноважень;
- моніторинг інформаційної системи;
- атаки на мережеве обладнання та інше.

ОРГАНІЗАЦІЯ WI-FI МЕРЕЖ

Організацію бездротових мереж Wi-Fi можна поділити на 2 групи:

1. Ad-hoc (бездротові самоорганізовані мережі);
2. Hot-spot (бездротові керовані мережі).

У бездротової локальної мережі типу Ad-hoc зв'язок встановлюється безпосередньо між пристроями, обладнаними Wi-Fi-адаптерами, і в цьому випадку точка доступу взагалі не використовується.

У бездротової локальної мережі, що функціонує в режимі Hot-spot, бездротові пристрої спілкуються між собою через точку доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але й доступ до зовнішніх мереж. Точка доступу передає ідентифікатор мережі SSID (Service Set ID) за допомогою спеціальних сигнальних пакетів. Бездротові пристрої підключаються до точки доступу, використовуючи її ідентифікатор мережі SSID, і обмінюються інформацією один з одним. У цьому випадку точка доступу використовується в якості центральної точки підключення бездротових пристроїв.

З точки зору захисту інформації Hot-spot має більше значення, оскільки, отримавши доступ до точки доступу, зловмисник може мати змогу отримати інформацію не тільки зі станцій, розміщених у цій бездротовій мережі, а й зі станцій розміщених у дротовій мережі, до якої підключена ця точка доступу [3].

МЕХАНІЗМИ ЗАХИСТУ WI-FI МЕРЕЖ

Механізми захисту Wi-Fi мереж передбачають автентифікацію (клієнт та точка доступу представляються один одному і підтверджують права на обмін даними) та шифрування (обрання алгоритму шифрування інформації та даних, що передаються по бездротовій мережі, генерація та зміна ключів).

Методи автентифікації клієнтів.

1. Відкрита автентифікація (Open Authentication).

Відкрита автентифікація передбачає захист бездротової мережі на основі MAC-фільтрації. Клієнт робить запит автентифікації, надсилаючи точці доступу свою MAC-адресу, точка доступу відповідає або підтвердженням (у разі знаходження MAC-адреси клієнта у таблиці дозволених адрес) або відмовою у автентифікації.

Порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес підтримується більшістю виробників мережевого обладнання та може

застосовуватися як додатковий захід захисту разом з наступними методами.

2. Автентифікація із загальним ключем (Shared Key Authentication).

Клієнт надсилає запит на автентифікацію точці доступу, отримуючи у відповідь підтвердження, що містить випадкову інформацію довжиною 128 біт. Клієнт шифрує отримані дані за допомогою алгоритму WEP (Wired Equivalent Privacy) за допомогою побітового додавання за модулем 2 (операція XOR) отриманої випадкової послідовності та послідовності ключа й відправляє зашифрований текст разом із запитом на асоціацію. Впевнившись у відповідності, точка доступу надсилає клієнту підтвердження асоціації. Після цього клієнт вважається підключеним до мережі.

Для використання автентифікації із загальним ключем необхідно попередньо налаштувати статичний ключ шифрування алгоритму WEP [4].

3. WPA (Wi-Fi Protected Access).

Внаслідок перших успішних атак на метод WEP було випущено проміжний стандарт WPA, що включає у собі нову систему автентифікації на базі 801.1x та новий метод шифрування TKIP (Temporal Key Integrity Protocol) – протокол перевірки цілісності ключа, який використовує вдосконалений спосіб керування ключами і покадрову зміну ключа.

Існують два варіанти автентифікації: за допомогою зовнішнього серверу, якому користувачі надають свої дані для автентифікації (WPA-Enterprise), та з використанням завчасно наданого ключа, що встановлюється на точці доступу (WPA-Pre-Shared Key) [5].

4. WPA2 (Wi-Fi Protected Access2, IEEE 802.11i).

WPA2 або IEEE 802.11i є варіант стандарту безпеки бездротових мереж, у якому в якості основного алгоритму шифрування було обрано стійкий блоковий шифр AES, а для зберігання зворотної сумісності з WPA може використовуватися TKIP. Алгоритм автентифікації у порівнянні з WPA зазнав незначних змін, але зберіг два варіанти автентифікації: WPA-Enterprise та WPA-Pre-Shared Key [5].

Методи шифрування даних.

1. WEP-шифрування.

WEP – один з перших алгоритмів, що забезпечує захист інформації, яка циркулює у бездротовій мережі. У якості основи для WEP було обрано потоковий шифр RC4 з ефективними довжинами ключів 40 чи 104 біт. На практиці використовують ключі довжиною 64 чи 128 біт, 24 біта з яких використовуються у якості вектору ініціалізації (Initialization Vector, IV), що містить дані для розшифрування повідомлення.

WEP-шифрування полягає у наступному: в першу чергу передані в пакеті дані перевіряються на цілісність за допомогою алгоритму CRC-32, після чого отримана контрольна сума додається в службове поле заготовки пакету даних. Далі генерується вектору ініціалізації довжиною 24 біти, до якого додається статичний 40 чи 104 бітний секретний ключ. Отриманий таким чином ключ довжиною 64 чи 128 біти є ключем для генерації псевдовипадкового числа, що використовується для шифрування даних. Наступним кроком алгоритму є виконання операції XOR між даними, що передаються, та отриманою псевдовипадковою послідовністю. Використаний вектор ініціалізації додається у службове поле кадру [4].

2. WPA-шифрування.

Головною особливістю наступного стандарту безпеки – WPA – стала технологія динамічної генерації ключів, побудована на протоколі TKIP, що використовує вектор ініціалізації довжиною 48 біт, замість 24 біт у WEP, та реалізація правила зміни його бітової послідовності для виключення повторного застосування ключа. Використання протоколу TKIP передбачає те, що для кожного пакету даних відбувається генерація нового ключа довжиною 128 біт. Крім цього контрольні криптографічні суми розраховуються за методом MIC (Message Integrity Code): у кожний кадр вкладається спеціальний код цілісності повідомлення довжиною 8 байт, перевірка якого дозволяє попередити атаки з використанням підміни пакетів. Якщо протягом хвилини буде відправлено більше двох пакетів, що не пройшли перевірку, то клієнта буде заблоковано на одну хвилину [5].

3. WPA2-шифрування.

Впровадження WPA2 істотно підвищило захищеність бездротових Wi-Fi мереж у порівнянні з попередніми технологіями. Новий стандарт передбачає обов'язкове використання стійкого блочного шифру AES – CCMP (Advanced Encryption Standard – Counter CBC-MAC Protocol). У режимі WPA-Pre-Shared Key з уведеного у вигляді відкритого тексту паролю генерується ключ PSK (PreShared Key) довжиною 256 біт. Цей ключ сумісно з SSID та ще чотирма параметрами використовується для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key) для взаємодії бездротових пристроїв. Режим WPA2-Enterprise дозволяє більш гнучко організувати роботу мережі за допомогою інтеграції із зовнішнім сервером, що здійснює керування доступом. Робота в цьому режимі потребує реєстраційних даних, таких як ім'я та пароль користувача, сертифікат безпеки чи одноразовий пароль, а автентифікація виконується між клієнтом і центральним сервером автентифікації [5].

Також, окремо варто згадати протокол WPS (Wi-Fi Protected Setup), що використовується для напівавтоматичного налаштування бездротової мережі для користувачів, які мають складнощі з самостійним налаштуванням точки доступу. При першому підключені користувачу буде запропоновано ввести 8 цифр з етикетки точки доступу; за умови правильного набору цього паролю, користувач створює SSID мережі, обирає ключ, протокол безпеки (WPA чи WPA2) та необхідний тип шифрування (TKIP чи AES) у діалоговому вікні операційної системи. При наступних підключеннях за допомогою WPS користувачу буде запропоновано або ввести пароль з етикетки пристрою, або натиснути на відповідну клавішу на точці доступу, після чого клієнт підключиться до точки доступу.

ВРАЗЛИВОСТІ ПРОТОКОЛІВ БЕЗПЕКИ WI-FI МЕРЕЖ

Варто розуміти, що до мережі з відкритою автентифікацією може підключитись будь-хто в зоні покриття, адже точка доступу не обов'язково має налаштований MAC-фільтр. Та навіть у разі налаштованого MAC-фільтру ніщо не заважає підібрати MAC-адресу авторизованого клієнта.

Використання режиму прихованого ідентифікатора мережі дозволяє приховати SSID мережі в списку доступних мереж, а підключення до неї стає можливим за умови, що клієнт знає її ідентифікатор та заздалегідь створив профіль підключення. У разі використання режиму приховання SSID точка доступу, так само, як і в звичайному режимі, надсилає службові кадри-маячки (beacon frames) з інформацією для підключення, але залишає пустим поле з SSID. Але це не захистить від можливості дізнатися SSID мережі за допомогою утиліт сканування ефіру, бо всі клієнти в мережі, що підключені до дочки доступу, знають SSID цієї мережі та при підключені надсилають кадри типу Probe Request, вказуючи ідентифікатор мережі з профілю підключення. Це дає хибні сподівання на захист мережі від зловмисника.

Через відсутність шифрування в таких мережах весь трафік може бути проаналізовано зловмисником на наявність конфіденційних даних. При користуванні такими мережами слід використовувати допоміжні технології, такі як, наприклад, HTTPS та VPN, для забезпечення певного рівня захищеності.

Протокол WEP фактично передає кілька байт свого тимчасового ключа разом з кожним пакетом даних. Відповідно, не залежно від складності паролю, проводячи перехоплення пакетів у бездротовій мережі з WEP-шифруванням, можна отримати ключ від цієї мережі. Так, наприклад, кількість пакетів, які треба перехопити для успішного злому мережі з WEP-ключем довжиною 64 біти, – близько півмільйона пакетів, а в багатьох випадках і менше, для злому мережі з ключем довжиною 128 біт вже буде потрібно близько двох мільйонів пакетів. Швидкість зламу прямо пропорційна інтенсивності трафіку між клієнтом та точкою доступу [4].

Незважаючи на застарілість та відносно легкі способи зламу, WEP шифрування й досі використовується при побудові розподілених бездротових мереж WDS (Wireless Distribution System), що дозволяють використовувати другу точку доступу як бездротовий міст для поєднання двох дротових мереж або як повторювач для розширення зони покриття першої точки доступу.

Протоколи WPA та WPA2, на відміну від WEP, шифрують дані кожного клієнта окремо за допомогою тимчасового PTK-ключа, що генерується після підключення клієнта до точки доступу. Для отримання PTK-ключа необхідно знати п'ять параметрів мережі, які можна вільно перехопити при прослуховуванні пакетів мережі, а головною перепоною на шляху зловмисника стає отримання Pre-Shared Key за допомогою перебору всіх можливих комбінацій паролю чи з використанням словника.

Для спроби підбору паролю зловмиснику потрібно перехопити «рукостискання» (handshake) між клієнтом і точкою доступу. Швидкість підбору залежить від швидкодії комп'ютера зловмисника та ємності словника паролів [5].

Протокол WPS дозволяє клієнту підключитись до точки доступу за допомогою PIN-коду, що складається лише з восьми цифр, остання з яких є контрольною сумою. Через реалізацію у алгоритмі двоетапної перевірки PIN-коду спочатку перевіряються перші чотири цифри; якщо вони підібрані невірно, точка доступу відправить пакет M4, якщо ж перші чотири цифри підібрані вірно, а цифри на позиціях 5-7 – ні, то точка доступу відправить пакет M6. Для отримання доступу до мережі потрібно перебрати перші чотири цифри, що дорівнює 10000 комбінацій та цифри на 5-7 позиціях, що дорівнює 1000 комбінаціям. Отже для підбору PIN-коду достатньо перебрати 11000 комбінацій.

ВИСНОВОК

Розглянуті методи захисту та вразливості протоколів бездротових Wi-Fi мереж наочно демонструють їх вразливість.

Такі заходи, як MAC-фільтрація і приховання ідентифікатора мережі, не є перепоною на шляху зловмисника, тому їх доцільно використовувати лише у комплексі з іншими заходами.

Протоколи WEP і WPS, маючи відповідні програмні засоби, можна зламати за короткий проміжок часу, тому за можливістю потрібно відмовитись від їх використання.

Успіх атаки на WPA/WPA2 у кінцевому результаті залежить від наявності паролю в словнику, оскільки повний перебір паролю довжиною від 8 до 63 символів займає значний час.

Для забезпечення безпеки бездротових мереж розроблено відносно багато методів. Так, наприклад, можна використовувати віртуальні приватні мережі VPN (Virtual Private Network) чи протокол SSL (Secure Sockets Layer).

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. White paper: Cisco VNI Forecast and Methodology, 2015-2020 [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html#wp9001447 (дата звернення 10.11.2016), вільний.
2. Wifi Network Security Statistics/Graph [Електронний ресурс]. – Режим доступу: http://graphs.net/wifi-stats.html (дата звернення 10.11.2016), вільний.
3. Владимир Антонович Ткаченко. Технологии стандарта 802.11x [Електронний ресурс]. – Режим доступу: http://www.lessons-tva.info/articles/net/003.html (дата звернення 10.11.2016), вільний;
4. Дмитрий Бугрименко. Проблемы безопасности в беспроводных ЛВС IEEE 802.11 и решения Cisco Wireless Security Suite [Електронний ресурс]. – Режим доступу: https://www.cisco.com/web/RU/downloads/WLANSecurity-1.2a.pdf (дата звернення 10.11.2016), вільний;
5. Василий Леонов. Как ломаются беспроводные сети [Електронний ресурс]. – Режим доступу: http://citforum.ru/nets/wireless/crack/ (дата звернення 10.11.2016), вільний;

УДК 004.056

ЗАЩИТА АКУСТИЧЕСКОЙ РЕЧЕВОЙ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКОМУ КАНАЛУ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Потоцкий С.В.,
Научный руководитель: Войцех С.И.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, E-mail: s90992p@uandex.ua

Проанализированы методы и средства несанкционированного получения акустической речевой информации с использованием мобильных телефонов и средств мобильной связи, технические устройства противодействия утечке информации.

Ключевые слова – сотовая связь, мобильный телефон, канал утечки, блокиратор.

Защита информации с ограниченным доступом от утечки по техническим каналам на объекте информационной деятельности достигается при применении совокупности организационных, инженерных и технических мероприятий и средств. При озвучивании информации в ходе закрытых совещаний, показов видеоматериалов со звуковым сопровождением особое внимание требует защита от утечки информации по прямому акустическому каналу.

Серьезную угрозу представляет использования возможности сотовой связи путем непосредственного применения мобильных телефонов, характеристики которых постоянно расширяются и модифицируются, и различных технических устройств на базе сотовой связи.

Простейший способ использования мобильного телефона в качестве закладного устройства - набор перед заходом в выделенное помещение номера абонента, который будет вести запись разговора.

Прослушивание также может осуществляться с использование специального приемника, настроенного на частоту стандарта GSM, с последующей записью и расшифровкой трафика.

Широкое распространение смартфонов привело к использованию программного способа прослушивания. Программа может быть установлена удаленно. В программе за ранее записан номер, при входящем звонке по которому мобильный телефон без видимых признаков включает микрофон, и передача информации происходит, как при обычном разговоре.

Возможно применение активного комплекса перехвата GSM-сигнала, представляющего собой ложную базовую станцию, которая становится посредником между реальной базовой станцией и мобильным телефоном. Ложная базовая станция перехватывает параметры соты и аутентифицируется мобильными телефонами в качестве обычной базовой станции. С этого момента возможно управление мобильным телефоном виртуальной базовой станцией, вплоть до перевода телефона в режим передачи без какой-либо индикации и без ведома его владельца (т. н. «полицейский режим»).

Для предотвращения утечки акустической информации через мобильный телефон могут использоваться пассивные и активные средства. К пассивным средствам относятся специальные чехлы, стаканы, сейфы, исключающие возможность воздействия акустического сигнала на телефон. Этот метод не обеспечивает защиту в случае, когда мобильный телефон скрыто установлен или занесен в выделенное помещение.

К активным средствам относится использования различных типов блокираторов, делающих невозможным установления связи с базовыми станциями. Классификация блокираторов представлена на рис. 1. Одной из основных характеристик блокираторов является радиус действия, который зависит от мощности блокиратора и от расстояния до базовой станции. Блокираторы по режиму работы можно разделить на три группы.

Блокираторы с ручным управлением создают шумовую помеху на диапазонах частот соответствующего стандарта работы базовых станций, делающую невозможным прием сигнала мобильными телефонами от базовых станций. Такие блокираторы обычно содержат от двух до четырех генераторов помех, охватывающих различные стандарты с возможностью включения в разных сочетаниях. Выходная мощность каждого генератора варьируется от 0,5 Вт до 2 Вт для портативных блокираторов и от 8 до 10Вт для стационарных. Основной недостаток - непрерывная работа вне зависимости от рабочего или нерабочего состояния мобильных телефонов.

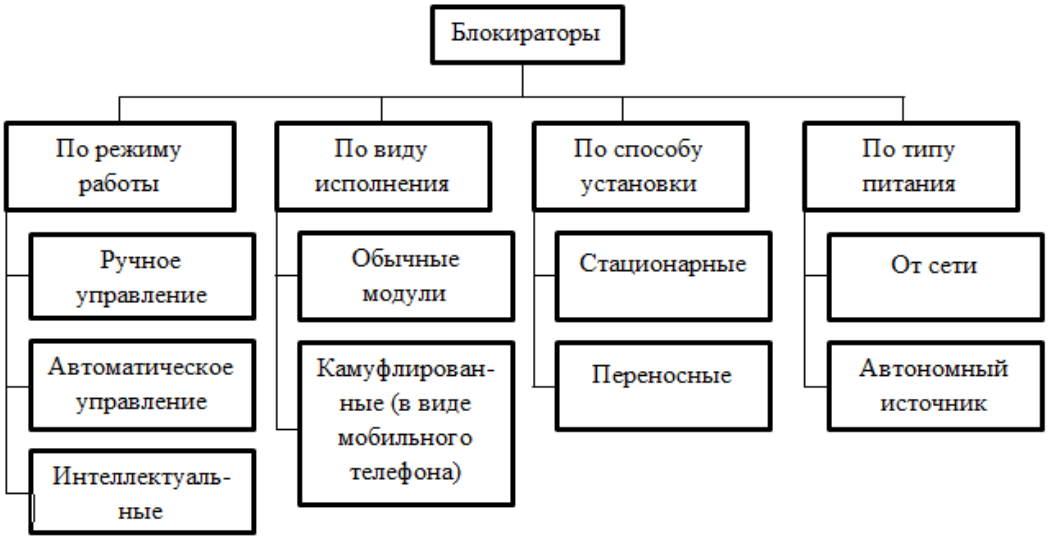


Рисунок 1. Классификация блокираторов

Подавители с автоматическим режимом работы содержат многоканальный приемник, который управляет включением генераторов блокиратора при появлении опасного сигнала. На входе приемника стоят полосовые фильтры, настроенные на частоты определенного стандарта сотовой связи. После выделения сигнала включается соответствующий генератор помех на несколько секунд, срывая установления сеанса связи. Такие блокираторы могут работать в режиме выявления опасного сигнала с постановкой или без постановки помех.

Интеллектуальные блокираторы содержит блок цифровой обработки. Приемник в коротком промежутке времени обнаруживает сигнал от мобильного телефона и вычисляет номер частотного канала и временной слот, выделенный конкретному телефону. Затем формируется заградительная помеха на частоте ответа базовой станции.

ВЫВОД

Постоянное расширения функциональных возможностей мобильных телефонов и технических средств на основе сотовой связи создает новые возможности для перехвата акустической речевой информации, циркулирующей в выделенных помещениях и делает актуальным проведения работ по совершенствованию блокираторов различных видов.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

2. Хорев А.А. Подавители средств сотовой связи и беспроводного доступа Журнал «Защита информации Инсайд» 2012 г.- №1 - с. 8-19.

УДК 004.056.52.001.362:57.087.1

БІОМЕТРИЧНІ ЗАСОБИ ІДЕНТИФІКАЦІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дем’янюк Максим Юрійович, Мартиненко Андрій Анатолійович
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua,
E-mail: jozephpalka@gmail.com

Однією з головних проблем захисту інформації в сучасних комп'ютерних системах є несанкціонований доступ до ресурсів ІТС. Саме тому, коректна ідентифікація авторизованих користувачів відіграє дуже важливу роль у інформаційній безпеці ІТС.

Ключові слова – доступ; авторизація; методи; біометрія.

ВСТУП

Біометричні системи ідентифікації дуже добре зарекомендували себе на ринку інформаційної безпеки, але так і не набули широкого розповсюдження окрім дактилоскопічних методів ідентифікації. Це пов'язано з розповсюдженню думкою про високу вартість подібних систем, та відсутністю бажання керівників підприємств зіткатися зі змінами у існуючих системах безпеки. Але, переваги біометричних систем ідентифікації користувачів – незаперечні. Швидкість обробки даних, постійність авторизаційної інформації в поєднанні з доступною ціною, все це беззаперечно повинно схилити підприємців до впровадження біометричних систем ідентифікації.

Дактилоскопія – найбільш відомий та поширений метод встановлення особистості за біометричними параметрами, відмінно зарекомендував себе у криміналістиці 20-го століття і допоміг розкрити не одну сотню злочинів. Проте, технології не стоять на

місці і відбитки пальців перестали буди єдиним ключом ідентифікації.

Сучасна техніка навчилася визначати користувачів за сітківкою та рогівкою ока, формую обличчя та рук, і низкою динамічних характеристик, голосу, біологічною активністю серця, рукописному і клавіатурному почерку.

ІДЕНТИФІКАЦІЯ ЗА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА

Подібно до відбитку пальця малюнок райдужної оболонки ока е унікальною характеристикою людини, а метод встановлення особистості за цим біометричним параметром, за думкою експертів, перевершує в надійності звичну дактилоскопію.

Для того, щоб зафіксувати малюнок на райдужці потрібна фотокамера з високим розширенням. Отримане зображення збільшується і перетворюється в унікальний код який присвоюється людині.

Малюнок райдужки який остаточно формується на другому році життя дитини, практично не змінюється протягом життя, якщо людина не отримує травм і не страждає від серйозних офтальмологічних патологій. В той же самий час, папілярний малюнок відбитку пальця вразливий до змін навіть в результаті дрібних побутових ушкоджень – опіків, або порізів, що робить цей метод ідентифікації менш ефективним ніж аналіз райдужної оболонки.

Перевагою методу є і простота в скануванні. Людині не обов'язково зосереджено дивитися в одну точку, бо пляма на сітківці знаходиться прямо на поверхні очного яблука і легко считується на відстані, що не перевищує 1м. Використати даний метод зручно в банківських організаціях або громадському транспорті. Зацікавились технологією і виробники смартфонів – у 2015 році в Японії до продажу поступила перша модель із сканером райдужної оболонки.

За думкою розробників впровадження технології ідентифікації за райдужкою ока допоможе захистити особисті данні власників смартфонів.

ІДЕНТИФІКАЦІЯ ЗА СІТКІВКОЮ

Просканувати сітківку – внутрішню оболонку очного яблука, що реагує на світло, важче: для цього до кровоносних судин задньої стінки ока, через зіницю посилають низько інтенсивні інфрачервоні світлові промені. Подібний метод встановлення особистості вважається високоефективним, та активно використовується на державних і військових об'єктах.

Капілярний малюнок сітківки відрізняється навіть, у близнюків, що знижує вірогідність помилки ідентифікації. Але, у 2012 році вчені із Університету Нотр-Дам в США виявили похибку у визначенні особистостей людей чиї данні були внесені в базу раніше 2008 року, і довели що на відміну від малюнка на райдужній оболонці малюнок сітківки схильний до ряду вікових змін.

І знову виробники мобільних гаджетів не залишились осторонь. Цілий ряд компаній працює над створенням комбінованих технологій ідентифікації за сітківкою і райдужкою.

РОЗПІЗНАВАННЯ ЗА "ГЕОМЕТРІЄЮ" ОБЛИЧЧЯ

Метод встановлення особистості за рисами здається експертам одним із найбільш перспективним завдяки своїй звичності: люди з легкістю ідентифікують один одного за обличчям, так чому не навчити цьому комп'ютер?

В основі технології – створення двомірних або тримірних "карт" людських рис – система запам'ятовує і опізнає контури носу і губ, форму брів, відстань між окремими рисами.

Розробники систем біометричного аналізу компанія Biolink називають розпізнання за обличчям другою за поширеністю і популярністю біометричною технологією, але "упізнання" за геометрією обличчя – задача трудомістка бо на сприйняття машини впливає освітлення, кут нахилу голови, наявність макіяжу.

Найбільш ефективно техніка розпізнає статичні зображення – фотографії. Так, система штучного інтелекту facenet створена Google, "визначила" 99,63% фото користувачів інтернету.

РОЗПІЗНАВАННЯ ЗА БІОЛОГІЧНОЮ АКТИВНІСТЮ СЕРЦЯ

Одна із новітніх технологій динамічної біометричної ідентифікації – встановлення особистості на основі даних про роботу серцево-судинної системи.

У 2014 році Канадська компанія Bionim представила світу пристрій який дозволяє використати ЕКГ людини в якості персонального ідентифікатора. "В науковому суспільстві існує ідея про те, що унікальність і сталість людського серцевого ритму дозволяє використати його в якості біометричного ідентифікатора", – зауважив генеральний директор компанії Bionim Карл Мартін.

В сутності, необхідно зробити наступне: взяту форму ЕКГ і піддати її машинному аналізу, щоб виявити унікальні і сталі особливості".

Високу ефективність технології оцінили спеціалісти з безпеки. "Кардіограма, як виявилось, також може бути досить перспективним засобом біометричної аутентифікації" – відмітили експерти Лабораторії Касперського.

АНАЛІЗ ГОЛОСУ

Біометричний метод ідентифікації за голосом простий у використанні – досить забезпечити аналітичний пристрій мікрофоном і записати "звучання" конкретної людини. Широке розповсюдження даного метода обумовлено наявністю мікрофону і можливістю запису звуку на більшості сучасних гаджетів і комп'ютерів. Але, технологія має низку суттєвих недоліків: голос однієї і тієї людини може звучати по-різному в залежності від її психологічного і фізичного стану, рівня шуму, якості мікрофону.

ДОДАТКОВІ МОЖЛИВОСТІ СИСТЕМ БЗІ

Всупереч розповсюдженій думці, системи біометричної ідентифікації

впроваджуються не тільки заради забезпечення безпеки охороняємих об'єктів або протидії злочинності.

Наприклад, ряд систем ідентифікації застосовуються в навчальних закладах. Деякі сучасні школи впроваджують сканування райдужної оболонки учнів з метою контролю відвідування і навіть для спрощення процедури оплати шкільних сніданків і обідів – учень приходить до їдальні, його сітківка сканується, з рахунку батьків списується конкретна сума за харчування дитини.

Використовуються і системи, що сканують відбитки пальців. На виробництві подібні системи дозволяють відмічати час проведений співробітником на робочому місці.

ВИСНОВОК

Вищевказані засоби ідентифікації користувачів надають змогу підвищити захищеність інформаційних ресурсів. Зокрема біометричні системи не виключають використання класичних засобів надання доступу а лише доповнюють їх при розумному впровадженні та налаштуванні, що в комплексі приведе до покращення ситуації з безпекою інформації.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Інформаційний ІТ-портал "Хабрахабр" [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://habrahabr.ru/ (дата звернення 15.11.2016) – Назва з екрана.

УДК 004.083.72+ 004.239

ОЦЕНКА ЗАЩИЩЕННОСТИ НАКОПИТЕЛЯ НА ЖЕСТКОМ МАГНИТНОМ ДИСКЕ ОТ УТЕЧКИ ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ КАНАЛАМИ

Автор: Цыбульников Артем Андреевич
Руководитель – соавтор: Кручинин Александр Владимирович
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: artem111artem@gmail.com

Выполнен обзор современных накопителей на жестких магнитных дисках (НЖМД, HDD) и интерфейсов, которые они используют. Выполнен комплексный анализ информационных сигналов, возникающих при работе HDD. Сформулированы предложения по совершенствованию методов и средств специальных исследований HDD.

Ключевые слова - накопитель на жестких магнитных дисках, интерфейс, излучение, опасный сигнал, кодирование, тестовая программа, специальные исследования.

ВВЕДЕНИЕ

HDD – является неотъемлемой частью многих автоматизированных систем (АС). Поэтому актуальными является задачи обеспечение защиты информации и оценка уровня защищенности от утечки ее техническими каналами, за счет побочных электромагнитных излучений (ПЭМИ) от HDD и интерфейса, через который он подключен.

Для решения этих задач необходимо выполнить анализ структуры HDD и спецификаций интерфейсов, которые используются в настоящее время. На сегодняшний день, распространёнными являются интерфейсы SATA.

КЛАССИФИКАЦИЯ СИГНАЛОВ

Как известно, все сигналы, которые циркулируют в элементах вычислительной системы разделяются на: информативные, слабо информативные и не информативные. Опасность представляет перехват информативных и, в некоторых случаях, слабо информативных сигналов. Поэтому существует необходимость классификации основных электрических сигналов, которые циркулируют в самом HDD и его интерфейсе.

На основе анализа структурных, функциональных и принципиальных схем HDD можно сделать следующие выводы.

К информативным можно отнести сигналы, циркулирующие в:

- управляющем микроконтроллере (обеспечение взаимодействие всех блоков накопителя и связь с внешним интерфейсом);
- канале чтения-записи и цепи (выделение из сигнала, принятого от предусилителя, импульсы синхронизации и данных и формирующие сигналы записи);
- контроллере HDD (запись и считывание данных).

К мало-информативным можно отнести сигналы, циркулирующие в:

- блоке управления позиционированием (формирование импульсов управления соленоидом для перехода с цилиндра на цилиндр по команде микроконтроллера);
- внутренней ОЗУ (используется для считывания и записи секторов и локального кэширования);

К не информативным можно отнести сигналы, которые циркулируют в:

- детекторе сервометок (выделение сервометок из потока сигналов, принимаемых с головок считывания);
- блоке управления шпиндельным двигателем (обеспечивает запуск и остановку шпинделя по команде от микроконтроллера и поддерживающие заданную скорость вращения по сигналам от датчиков индекса, специальных датчиков вращения или/и сервометок);

• коммутаторе головок (улучшение отношения сигнал/шума при считывании).

Параметры этих сигналов зависят от многих факторов. В технической документации на HDD, как правило, приведены общие сведения о сигналах. Поэтому существует необходимость в более подробном их изучении.

Следует отметить, что интерфейсы, которые используются для подключения HDD, являются стандартизированными и параметры их сигналов достаточно подробно описаны в документации.

Рассмотрим, для примера, интерфейс SATA (Serial ATA), который является развитием интерфейса IDE. Его особенностью является не параллельная передача данных, а последовательная, что хотя и медленнее, но позволяет использовать более высокие частоты без необходимости синхронизации сигнала. Кабель интерфейса состоит из двух пар проводов (одной передачи и одной на прием) и несколько нулевых. Всего семь. Однако, этот факт является причиной того, что этот интерфейс является более уязвимым, с точки зрения перехвата информации каналом ПЭМИ.

Первый стандарт SATA 1.x мог работать на частоте 1.5 ГГц с пропускной способностью 1.2 Гбит/с (потери за счет передачи большого количества служебной информации). Стандарт 2.x работает на частоте 3 ГГц с пропускной способностью до 2.4 Гбит/сек и стандарт 3.0 на частоте 6.0 Гбит/с, с пропускной способностью 4.8 Гбит/с.

Тем не менее, авторы исследований утверждают, что частоты, на которых возможен съем информации находится в пределах от 1кГц до 3 ГГц. Однако Частота рассматриваемого сигнала составляет 1500 МГц, ширина сигнала порядка 5 МГц. Необходимо отметить, что уровни отличаются незначительно и частоты около 1500 МГц, на которых происходят излучения от SATA интерфейса, не оптимальны для передач данных – электромагнитная волна быстро затухает. Данный фактор играет против злоумышленника, но при грамотной настройке перехватывающей аппаратуры и последующей цифровой обработке сигнала возможен такой перехват со значительных расстояний [1].

СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ

Для оценки уровня защищенности проводят, специальные исследования, основными этапами которых являются:

1) обнаружение излучения от объекта;

2) классификация излучений;

3) измерение параметров информативных излучений.

На практике наибольшую сложность представляют собой первые два этапа.

Для их реализации используются тестовые программы для формирования тестовых сигналов. Эти программы позволяют определять параметры тактовых сигналов элементов вычислительной системы, которые исследуются, и «подкрашивать» информативные сигналы.

Так, многие тестовые программы для определения тактовой частоты при исследовании HDD, производят запись-чтение файла достаточно большого размера. После определения времени, которое было затрачено, определяется тактовая частота. Однако данный способ не учитывает особенности логической структуры диска накопителя, равномерность его заполнения и другие факторы, которые оказывают влияние на время доступа к диску, а, следовательно, и на время чтения-записи файла. В результате этого, погрешность, при определении тактовой частоты, может составлять 100%. Кроме этого, не вполне понятно тактовая частота чего при этом определяется? Каким образом учитывается наличие блоков работающих с разными тактовыми частотами, использование буферов FIFO, пакетная передача данных?

При формировании тестовых последовательностей, оператор задает их типы. Наиболее распространенными являются «меандр» (101010….), «нули» (00000…) и «единицы» (11111…). Однако при этом не учитываются те преобразования данных, которые возникают в процессе обращения к HDD.

Так в интерфейсе SATA для кодирования передаваемой информации используется потенциальный код без возвращения к нулю (Non Return to Zero, NRZ). Он является одним из самых простых в реализации, благодаря двум резко различающимся потенциалам обладает хорошей распознаваемостью ошибок, но не обладает необходимым свойством самосинхронизации.

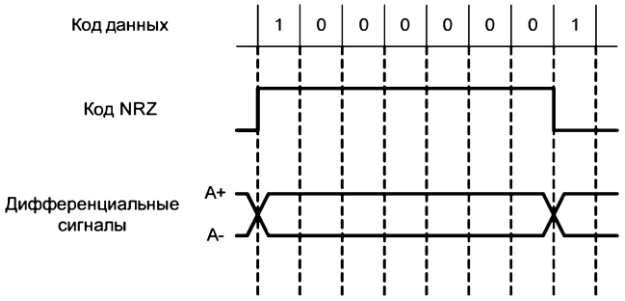


Рисунок1. Диаграмма формирования сигналов кода NRZ

Для обеспечения самосинхронизации применяется скремблирование. Перемешивая данные, подлежащие передаче определенным образом так, чтобы вероятность появления единиц и нулей на выходе была приблизительно одинаковой. Эта задача решается с помощью кодирования 8/10 (аналогия с кодами CD 8/14). При кодировании 8/10 байты заменяются 10-битными кодами, дающими 1024 возможные комбинации, из которых выбираются 256 двоичных кодов с ограниченным числом нулей. [4]

Кроме этого, на различных этапах передачи данных используются и другие способы модуляции и кодирования:

• частотная модуляция (FM);

• модифицированная частотная модуляция (MFM);

• кодирование с ограничением длины поля записи (RLL).

При выполнении специальных исследований, могут возникать сложности при идентификации

источника сигнала: интерфейс, контроллер HDD и др. Локализовать источник можно используя специальный набор антенн. Однако их использование в малом объеме может быть затрудненно. Частично решить эту проблему могло бы разделение во времени работы различных потенциальных источников сигналов.

ВЫВОДЫ

На основании проведенного анализа современных HDD и их интерфейсов, были определены их особенности, которые необходимо учитывать при проведении специальных исследований. Это обуславливает необходимость совершенствования существующих тестовых программ и методик проведения специальных исследований HDD для оценки уровня защищенности информации от утечки каналами ПЭМИ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Гук Михаил Юрьевич “Аппаратные средства IBM PC” Санкт-Петербург, 2006. - 1034 с.[Електронный ресурс]. – Режим доступа: http://royallib.com/book/guk_mihail/apparatnie_interfeysi_pk_entsiklopediya.html, свободный;

2. Антясов И. С., Сафонов А. В., Соколов А. Н. «ПРОГРАММНО-ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ «МЯГКИЙ» ПЭМИН. 2015 — 4с. [Електронный ресурс]. Режим доступа: http://www.info-secur.ru/is_17/Antyasovsafonov.pdf, вільний;

3. Кенін А.М. Практичне керівництво системного адміністратора. – СПБХ. БХВ – Петербург, 2010. – 464 с.: ил. – (Системний адміністратор);

4. Вадим Авдеев «Периферийные устройства: интерфейсы, схемотехника, программирование» Москва, 2009 - 847 с.

Секція «Телекомунікації та радіотехніка»

Голова секції: к.ф.-м.н., доцент кафедри безпеки інформації та телекомунікацій Гусєв О.Ю.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Масальська О.О.

УДК 621.391

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ GPON В СУЧАСНІЙ УКРАЇНІ

Москаленко А.Б., научний керівник: доц. Гусєв О.Ю.
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail: skipper06@gmail.com

У статті розглянуті перспективи впровадження технології GPON в Україні для надання доступу інтернет. Проаналізовані переваги технології. На основі моделювання GPON мережі підтверджується, що ці мережі запроваджують задовільну якість передачі і є одним з найкращих шляхів розвитку мережевої структури систем зв'язку.

Ключові слова – GPON; хвилеводне спектральне ущільнення; оптоволокно; мультиплексор.

ВСТУП

На даний момент технологія GPON має широке поширення по світу і є одним з найдешевших способів реалізації технології FTTH. У нинішніх умовах ця технологія є дуже перспективною для організації широкосмугового доступу інтернет та до мультисервісних мереж в Україні.

ТЕОРИТИЧНІ ДАННІ

GPON складається з OLT (optical line terminal), який знаходиться на стороні оператора і ONT (optical network terminal), які знаходяться у абонентів. Між ними немає активного обладнання, тільки пасивні оптичні розгалужувачі і оптоволокно. Передача з OLT ведеться на довжині хвилі 1490 нм зі швидкістю 2,5Гбіт/с, а прийом – на довжині хвилі 1310 нм зі швидкістю 1,25 Гбіт/с [1, с.5]. Таким чином забезпечується робота системи по одному волокну за принципом хвилеводного спектрального ущільнення (WDM).

У низхідному потоці (від OLT до ONT) за принципом широкомовлення – усі кадри передаються усім абонента у зашифрованому 128-бітним ключем вигляді, і кожен ONT має доступ до своїх кадрів, [1, с.6].

У висхідному потоці працює принцип мультиплексуванням з поділом за часом. Кожен з ONT веде передачу тільки у своєму проміжку часу, [1, с.6]. Стабільна та гнучка робота досягається завдяки повній синхронізації мережі разом з динамічним розподілом смуги перепуску.

До переваг GPON можна віднести:

- ефективне використання кожного волокна;
- широку смугу пропускання (2.5 Гбіт/с);
- відсутність необхідності інсталяції активних мультиплексорів в точках розгалуження, що полегшує обслуговування таких мереж і мінімізує енергоспоживання. Замість активних пристроїв в таких точках PON використовує невеликі оптичні розгалужувачі;
- оптичну прозорість по всій довжині, що дозволяє легко переходити на велику швидкість обміну (10Гбіт/с) або застосовувати додаткові довжини хвиль.

РОЗРАХУНКИ ДЛЯ МОДЕЛІ ДСЛІДЖЕННЯ

Для перевірки можливостей GPON була промодельована робота мережі для 48 абонентів на одному волокні. Відстань від OLT до ONT 8 км; використовуються подільники: один 1х4 (внесене згасання 7,4 дБм) і три 1х16 (внесене згасання 13,5 дБм). Загасання на з'єднаннях становить 0,8 дБм, загасання на волокні 1,68 дБм.

Трансмітер в OLT має лазер з потужністю випромінювання $P_{л1}$ = 5 мВт (7 дБм) і приймач з чутливістю 27 дБм, загальний бюджет – 34 дБм для низхідного потоку. Трансмітер в OMT - лазер з потужністю випромінювання $P_{л2}$ = 3 мВт (5 дБм) і приймач з чутливістю 32 дБм, загальний бюджет – 37 дБм для висхідного потоку.

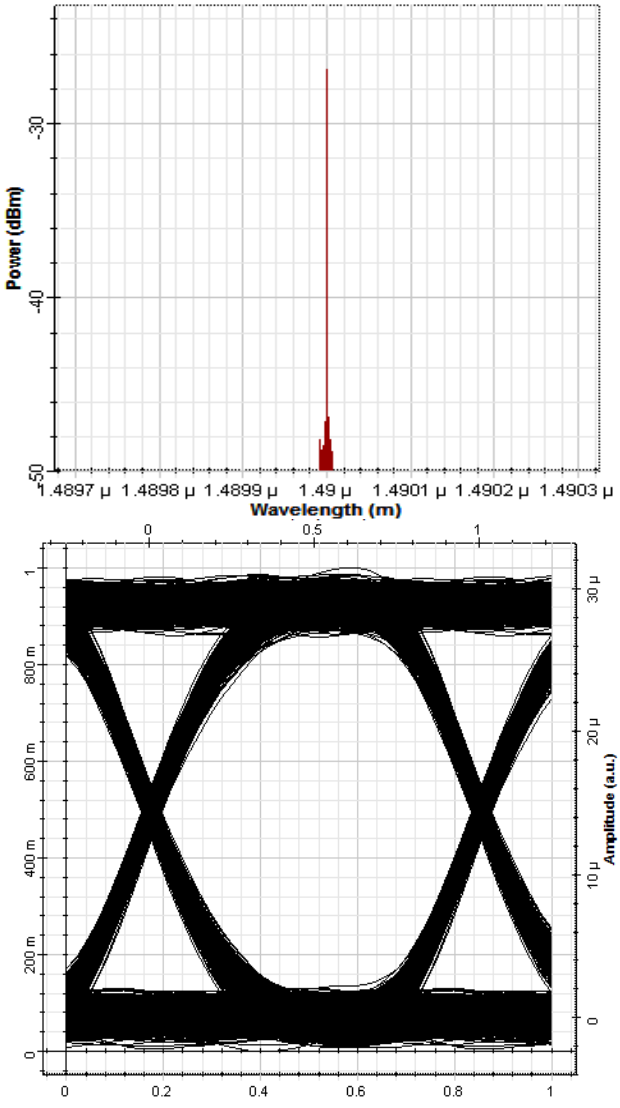
Загальне згасання для низхідного потоку дорівнює 23,2 дБм, а для вісхідного – 24,26 дБм. Отже розрахований запас згасання для низхідного потоку – 10,8 дБм, та для висхідного – 12,74 дБм. Результати моделювання надані на рисунку 1.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведений модельний експеримент показав достатньо високу ефективність системи передачі, що підтверджується наступними результатами:

- відношення сигнал/шум досить велике в обох напрямках: 27,2 дБм для низхідного та 15,34 дБм для висхідного потоків;
- коефіцієнт помилкового прийому дорівнює 10^{-116} для низхідного та 10^{-10} для висхідного потоків, при мінімальній допустимій величині – 10^{-10}.

Max. Q Factor	22.9123
Min. BER	1.75089e-116
Eye Height	2.51588e-005
Threshold	1.44902e-005
Decision Inst.	0.46875



Max. Q Factor	5.85814
Min. BER	2.30313e-009
Eye Height	4.22821e-006
Threshold	8.00538e-006
Decision Inst.	0.53125

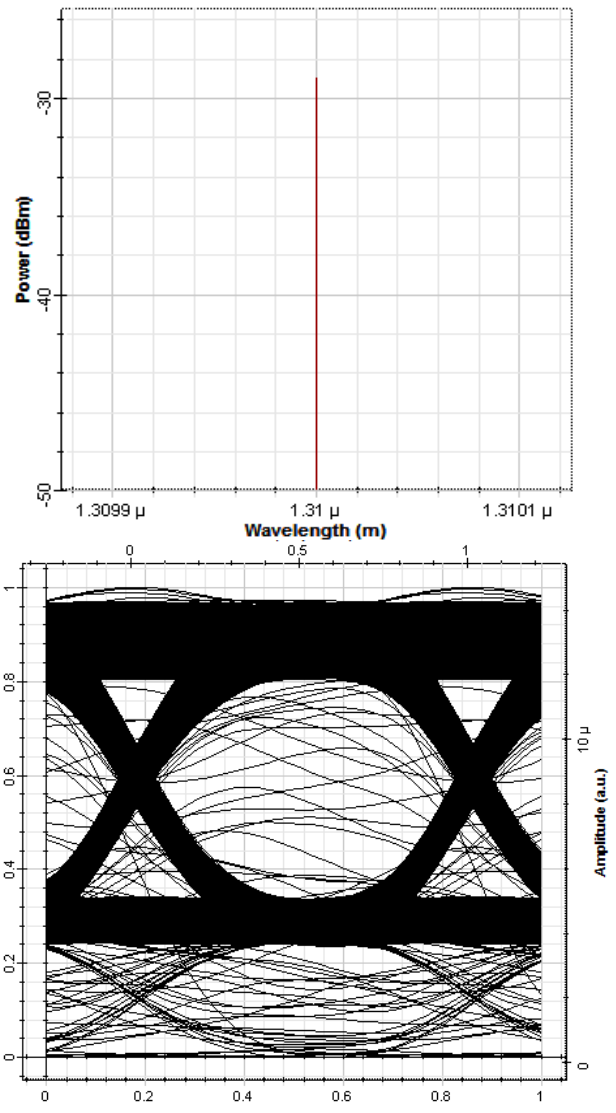


Рисунок 1 – Спектр прийнятого сигналу, індикаторна діаграма, числові результати аналізу відповідно, низхідного потоку (3 верхні діаграми) висхідного потоку (3 нижні діаграми).

ВИСНОВКИ

Отже за допомогою моделі з'ясовано, що GPON може впровадити передавання на даних на відстані 8 км із 48 абонентами на одному волокні та швидкістю 50 Мбіт/с. Це задовільний результат для використання в Україні.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 ITU-T Recommendation G.984.2 – Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification – approved by ITU-T Study Group 15 (2001-2004) under the ITU-T Recommendation A.8 procedure on 16 March 2003. – 38 c

VIII ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

24 листопада 2016 р.

Підписано до друку 15.11.16. Формат 30 х 42/2.
Папір офсетний. Ризографія. Ум. друк. арк. 3,73
Обл.-вид. арк. 3,65. Тираж 25 прим. Зам. № __

Підготовлено до друку у Державному ВНЗ
«Національний гірничий університет»
49005, м. Дніпро, просп. Д. Яворницького, 19

Надруковано у ТОВ «САЛВЕЙ»
Свідоцтво № 233689904636
49000, м. Дніпро, вул. ак. Чекмарьова, 10 / 7