• *Функціональне*: рішення повинно бути достатньо функціональним, а це означає, що воно повинне бути здатним зменшити вплив атаки незалежно від того, наскільки потужною є атака.

• *Прозоре*: рішення має бути простим у здійсненні, тобто не повинно вимагати змін існуючої мережі та її інфраструктури.

• *Легке*: рішення не повинно перекривати систему.

• *Точне*. Вибране рішення не повинно видавати помилкові результати. Ряд методів вимагають зменшення трафіку, але рішення для захисту від DDoS-атак не має впливати на трафік.

Висновок

Оскільки кількість DDoS-атак у хмарних сервісах зростає, подано короткий опис DDoS-атак, таксономію атак, їх види та заходи протидії пом'якшенню впливу. Описані методи виявлення і запобігання атак, визначені принципу вибору рішень для захисту.

1. Denial of Service Attack, http://en.wikipedia.org/wiki/Denial-of-serviceattack
2. DDoS attack tool time line, http://staff.washington.edu/dittrich/talks/sec2000/timeline.html
3. History of DDoS, http://www.timetoast.com/timelines/history-of-ddos
4. DoS and DdoS Evolution, http://users.atw.hu/denialofservice/ch03lev1sec3.html
5. CERT Coordination Center, Over view of attack trends, Feb.2002. http://www.cert.org/archive/pdf/attacktrends.pdf.

http://doi.org/10.5281/zenodo.3860778

Поступила 3.10.2019р.

УДК 009.4

Б.М. Гавриш [1], к.т.н., доцент
Б.В. Дурняк [1], д.т.н., професор
О.Б. Полусин [1], аспірант
О.Є. Семенова [2], асистент

ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Abstract. Methods of protection by encryption, implementation of authentication system and use of electronic signature algorithms are considered and compared. The structural division of encryption algorithms is given.

[1], Українська академія друкарства, Львів

[2] Національний університет «Львівська політехніка»

Вступ. На сьогодні первинним чинником, що впливає на політичну і економічну складові національної безпеки, є ступінь захищеності інформації та інформаційного середовища. Ось чому важливе значення набувають питання забезпечення захисту інформації в автоматизованих (інформаційних) та телекомунікаційних системах під час обробки в різних сферах діяльності.

Стрімкий розвиток засобів обчислювальної техніки і відкритих мереж передачі даних зумовило їхнє поширення в повсякденному житті і підприємницькій діяльності. Потужні обчислювальні можливості і оперативність передачі інформації не тільки вплинули на принципи ведення бізнесу, що склалися в більшості традиційних галузей, а й відкрили нові напрямки розвитку підприємницької діяльності [1]. Однак останні досягнення людської думки в області комп'ютерних технологій пов'язані з появою не тільки персональних комп'ютерів, мереж передачі даних і електронних грошей, а й таких понять, як гакер, інформаційна зброя, комп'ютерні віруси тощо.

Основна частина

Шифрування даних – процес давно відомий і досить зрозумілий. Навіть якщо в процесі передачі інформації від відправника до одержувача дані будуть перехоплені зловмисником, прочитати їх без ключів шифрування неможливо. Таким чином, перехоплення зашифрованої інформації стає позбавленим сенсу. Незважаючи на те, що шифрування даних, як ідея, – це просто, реальне втілення задуму в життя пов'язане зі значними труднощами доступу. У шифрування є дві сторони. Постійно використовувати суперскладне шифрування даних, яке неможливо зламати, недоцільно, тому що це створює великі труднощі одержувачу. У разі, якщо шифрування даних проводиться з використанням занадто простих ключів шифрування, теж зле: зусиль багато, але результат мінімальний, тоді вже простіше обійтися взагалі без шифрування. Будь-яка хороша система повинна бути збалансована. Шифрування даних – не виняток: інформація і дані повинні відправлятися швидко, але, при цьому, дані повинні залишатися в безпеці. В даний час, віртуальна приватна мережа – VPN, яка застосовує шифрування даних, є хорошим прикладом швидкого і безпечного інтернет з'єднання. VPN в основному займається виявленням слабких місць в системі безпеки інтернет користувачів та маскування IP адреси для великої кількості людей.

Шифрування даних – це видозміна інформації для того, щоб вона стала нерозпізнаваною для сторонніх.

Одним з початкових методів шифрування періоду античності є код перестановки. Більшість людей знайомі з цим типом кодування, під час якого шифрування даних проходить за допомогою перестановки літер алфавіту. Це дуже просте симетричне шифрування, однак функціональне.

З плином часу шифрування і криптоаналіз стають щораз поширенішими, процес шифрування – набагато складнішим. У якийсь момент ефективність використання букв алфавіту для шифрування повідомлень була вичерпана, і

люди звернулися до математики. Просте обчислення перетворилося в просунуту математику, потім в ірраціональну математику, і тепер воно досягло точки, в якій в цих обчисленнях знову переважають букви, але ці букви – це інші, не менш складні обчислення.

Зазвичай, шифрування даних відбувається за допомогою будь-якого методу шифрування або ключа (пароля) шифрування/дешифрування, який відомий лише двом сторонам: відправнику і одержувачу. Цифрове шифрування даних складніше, ніж шифрування рукописне, але воно засноване на тих самих принципах.

Рано чи пізно перед кожною інформаційною системою постає важливе питання забезпечення захисту даних шляхом приховування інформації від осіб, для яких вона не призначена. Виконати це завдання в рамках самої системи можна за рахунок впровадження системи аутентифікації, завдяки чому доступ зможуть отримати виключно авторизовані користувачі. Однак якщо зловмисникові вдасться отримати фізичний доступ до даних, то аутентифікація стане марною. Буде порушена конфіденційність даних (доступні тільки тим, кому призначені), вони можуть бути змінені, що також ще й порушить їхню цілісність. Для запобігання подібного результату застосовується шифрування даних. Простими словами, шифрування даних полягає в поданні інформації у вигляді, відмінному від початкового, з якого неможливо визначити, як виглядає вихідна інформація, не знаючи спеціального ключа шифрування. Використовуючи цей ключ, дані можна спокійно розшифрувати. Варто також відзначити, що шифрування даних використовується не тільки для фізичного захисту даних - його також можна використовувати, наприклад, для запобігання несанкціонованого доступу в систему, ускладнивши процедуру аутентифікації.

Шифрування є важливою частиною криптографії – науки про захист інформації. Протягом останніх кількох десятків років ця наука переживає бурхливий розвиток [1], викликаний, в першу чергу, повсюдним використанням електронно-обчислювальних машин, а також бажанням власників цієї техніки захистити свої особисті дані (або даної організації) від сторонніх очей. Для того щоб вирішити таку серйозну проблему, були розроблені спеціальні алгоритми шифрування. Структурно ці алгоритми можна розділити на три групи: безключові, одноключеві та двоключові (рис. 1) [1]. Безключові алгоритми не використовують ключі в процесі шифрування, одноключові використовують один ключ, а двоключові – два ключі. Двоключові алгоритми вважаються найбільш надійними, проте вони більш складні і трудомісткі у використанні. Як видно з рисунка 1, деякі типи алгоритмів можуть відноситися відразу до декількох груп. Наприклад, хеш-функції (виконують контрольне підсумовування даних) можуть виконуватися як з ключем (причому із одним), так і без нього. Хеш-функції набули широкого поширення через свою відносну простоту і низької потреби ресурсів і використовується, наприклад, тоді, коли необхідно підтвердити цілісність даних. Також до двох груп відносяться і алгоритми аутентифікації,

які можуть бути як одноключовими, так і двоключовими. Подібні алгоритми замінюють стандартну схему парольної аутентифікації, коли користувач може потрапити в систему при правильному введенні імені користувача та пароля. Ці алгоритми помітно знижують шанси зловмисника потрапити в систему. Наприклад, можлива наступна реалізація використання алгоритму аутентифікації:

- кожен користувач володіє унікальним ключем шифрування, який також знає і система;
- під час спроби входу в систему сервер генерує випадкове число, яке після генерації відправляє користувачу;
- використовуючи свій унікальний ключ шифрування, користувач шифрує отримане число і відправляє серверу вже зашифроване число.
- сервер розшифровує отримане число (або зашифровує вихідне), використовуючи ключ шифрування користувача, що зберігається в системі;
- якщо результати збігаються, то користувач отримує доступ до системи, в іншому ж випадку він отримає відмову на отримання доступу.

Рис.1. Структурний поділ алгоритмів шифрування

Генератори випадкових чисел, хоч і є безключовими алгоритмами, проте використовують ключі шифрування, просто вони створюють їх самі. Такі ключі є абсолютно випадковими, що помітно зменшує можливість розшифрувати дані. Алгоритми симетричного шифрування є базовими, оскільки в них шифрування і дешифрування проводиться за одним ключем

(або один ключ можна легко отримати з іншого). Ці алгоритми діляться на ті, що використовують блочне шифрування і ті, що використовують потокове шифрування. Під час блокового шифрування весь масив даних ділиться на блоки певної фіксованої довжини (найчастіше використовуються блоки по 64 або 128 біт), яка дорівнює довжині ключа шифрування. Відповідно, кожен отриманий блок шифрується окремо ключем, причому цей ключ може змінюватися для різних блоків, наприклад, в залежності від результату шифрування попереднього блоку. У свою чергу, під час потокового шифрування шифрується окремо кожен біт даних. Можна сказати, що потокового шифрування як такого не існує – воно всього лише є окремим випадком блочного шифрування, коли довжина блоку дорівнює одному біту. Варто зазначити, що алгоритми симетричного шифрування це найбільша категорія алгоритмів шифрування. Генератори псевдовипадкових чисел використовуються тоді, коли немає можливості розробити якісний генератор випадкових чисел. Псевдовипадкові числа створюються на основі певного алгоритму симетричного шифрування. Алгоритми асиметричного шифрування використовують два ключа шифрування відкритий для зашифровування інформація і секретний для її дешифрування, причому відкритий ключ досить просто обчислюється з секретного, а обчислити секретний ключ з відкритого практично неможливо (для цього потрібен тривалий час і величезні ресурси). Інформацію, зашифровану відкритим ключем, можна розшифрувати виключно секретним ключем. Наприклад, можлива наступна реалізація алгоритму асиметричного шифрування при спілкуванні двох користувачів:

- один користувач має відкритий ключ шифрування, а інший – секретний;
- перший користувач шифрує повідомлення, використовуючи відкритий ключ, і передає його другому;
- другий користувач дешифрує отримане повідомлення, використовуючи секретний ключ.

Останніми на черзі є алгоритми електронного підпису, які «використовують секретний ключ для обчислення електронного цифрового підпису даних, а який той, що вираховується з нього відкритий – для її перевірки» [1].

Висновки

Таким чином, існує величезна кількість хороших і якісних алгоритмів шифрування, однак навіть їхнє використання, на жаль, ніяк не виключає можливості несанкціонованого доступу до даних, однак вони серйозно ускладнять життя зловмисникові і, можливо, навіть змусять його відмовитися від спроби доступу. Саме в цьому, на сьогодні і складається завдання захисту інформації.

1 *Блінцов В.С.* Математичні основи криптології + CD : Навчальний посібник для студ. вищих навч. закл. / В.С. Блінцов, Л. Пальчевський. – Миколаїв: Національний ун-т кораблебудування ім. адмірала Макарова, 2006. – 232 с.: іл.

2 Безпека інформаційних систем і технологій: Навч. посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с. : іл
3 *Горбенко І.Д.* Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво "Форт", 2012. – 880 с.: іл
4 Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.: іл.
5 *Мукачев В.А*. Методы практической криптографии / В.А. Мукачев, А.А. Хорошко. – К.: ООО "Полиграф-Консалтинг", 2005. – 215 с.: ил
6 *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. – СПб: БХВ-Петербург, 2009. – 576 с.: ил
7 *Б. Шнайер*, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Москва: Изд-во Триумф, 2002. -816 стр
8 *Menezes, P. van Oorschot, S.* Vanstone Handbook of Applied Cryptography. – CRC Press, Inc. – 1997.
9 *Фороузан Б.А.* Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин – Курс лекций.

http://doi.org/10.5281/zenodo.3860780

Поступила 3.10.2019р.

УДК 621.372:376.56

О.В. Тимченко [1,2]
О.В. Шевчук [2]

ДОСЛІДЖЕННЯ ПЕРЕХІДНИХ І ЧАСТОТНИХ ХАРАКТЕРИСТИК СИСТЕМИ СУМІЩЕННЯ ФАРБ РУЛОННОЇ РОТАЦІЙНОЇ МАШИНИ

Abstract. The influence of technological parameters on the ink displacement in a roll printing machine is investigated. It is shown that the largest dynamic deviation is observed for the first paint, and the method of measuring the errors of combining paints for the last paint provides more efficient filtering of high-frequency noise.

Вступ

Системи автоматичного регулювання фарб на багатофарбових рулонних друкарських машинах є дискретними системами. Дискретність систем обумовлена способом вимірювання зміщення фарб за допомогою рівновіддалених міток, які друкуються на рухомій стрічці. Аналіз впливів зміни технологічних параметрів на зміщення фарб вимагає складних

[1] University of Warmia and Mazury Olsztyn, Poland
[2] Українська академія друкарства, Львів