В таблиці 2 наведені порівняння витрат часу і об'єму алгоритмами дерева і середніх значень. Але слід зазначити, що витрати часу для алгоритму дерева змінюються залежно від побудованого дерева.

Висновок

В роботі проведений аналіз найбільш відомих алгоритмів знаходження нормалізуючої константи. Встановлено, що найбільш доцільно буде використовувати алгоритм у формі дерева, що дозволить значно скоротити час і витрати пам'яті для знаходження вихідних даних в комп'ютерних мережах.

Література

1. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. - Москва : Техносфера, 2003. - 512 с.

2. Simon S. A tree convolution algorithm for the solution of queueing networks / S. Simon, Y. Luke Lien. // - Communications of the ACM. - 1983. - pp. 203-215.

Надійшла до редакції
7.2.2013 р.

УДК 004:004.65

О.Ю. ХМЕЛЬНИЦЬКИЙ, Ю.В. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

ЦІЛІСНІСТЬ ТА КОНФІДЕНЦІЙНІСТЬ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖАХ

Досліджено та виділені типові загрози інформації – потенційно несприятливі дії на інформацію, що призводить до порушень хоча б одної з її властивостей. Аналіз загроз інформації є одним з найбільш важливих питань при побудові захищених мереж. Такий аналіз має виявити можливі загрози інформації та показати з якого боку мережі нам слід чекати атаки.

Ключові слова: загроза інформації, технології захисту,цілісність та конфіденційність передачі даних, захищеність мереж.

Investigated and identified common threats to information - a potentially adverse effect on the information that leads to violations of at least one of its properties. Analysis of threats to information is one of the most important issues in building secure networks. This analysis should identify possible threats and information show which side of the network, we should expect an attack.

Keywords: threat information technology security, integrity and confidentiality of data, security networks.

Вступ

Для захисту інформації у мережах необхідно витрачати сили і кошти. Очевидно, що витрати на захист інформації у мережах не повинні перевищувати можливих збитків при втраті інформації. Необхідно ввести міру цінності інформації. На базі відомих витоків сформулюємо властивості інформації, що визначають її цінність. Такими основними властивостями захищеної інформації є конфіденційність, цілісність, доступність [1]. Конфіденційність визначається як властивість інформації, яка полягає в тому, що вона не може бути доступною користувачам, які не мають на це відповідних повноважень. Цілісність інформації – це властивість інформації коли вона не може бути доступною для модифікації користувачам, які не мають на це відповідних повноважень. Цілісність інформації може бути фізичною та логічною. Доступність інформації – це властивість інформації, що полягає в можливості використання за вимогами користувача, який має відповідні повноваження. Під загрозами розуміються шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза зняття інформації і перехоплення випромінювання з дисплею веде до втрати секретності або конфіденційності, загроза пожежі веде до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності. В [1] констатується, що загрози інформації розглядаються з точки зору їх будь-якої небажаної дії на будь-яку з цих властивостей і можливого їх порушення. З цієї точки зору в автоматизованих системах (АС) розрізняють наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;

Тому загроза – це потенційно можлива несприятлива дія на інформацію, що призводить до порушень хоча б одної з наведених властивостей. Аналіз загроз інформації є одним з найбільш важливих питань при побудові захищених мереж. Такий аналіз має виявити можливі загрози інформації та показати з якого боку мережі нам слід чекати атаки. Загрози інформації можуть реалізуватися внаслідок причин, серед яких [2]:

- кількісна недостатність - нестача компонентів мережі для протидії можливим порушенням безпеки інформації;
- якісна недостатність – недосконалість конструкції, організації компонентів мережі, внаслідок чого не забезпечується протидія можливим порушенням безпеки інформації у мережі;

- відмови елементів мережі – порушення працездатності елементів мережі, яке призводить до неможливості виконання своїх функцій;
- збої елементів мережі – тимчасове порушення працездатності елементів мережі, яке призводить до неправильного виконання своїх функцій;
- помилки елементів мережі – неправильне виконання елементами мережі функцій внаслідок їх стану;
- зловмисні дії – дії користувачів спрямовані на порушення безпеки інформації мережі;

Постановка задачі

Мережі стандарту 802.11 працюють у не ліцензованому діапазоні частот та доступні для прослуховування, тому саме в них розгортання й обслуговування віртуальних мереж VPN здобуває особливу важливість, якщо необхідно забезпечити високий рівень захисту інформації.

Захищати потрібно як з'єднання між комп'ютерами у бездротовій локальній мережі, так і канали між мостами. Для забезпечення безпеки особливо секретних даних не можна покладатися на якийсь один механізм чи на захист лише одного рівня мережі. У випадку кількох каналів простіше та дешевше розгорнути VPN, що покриває дві мережі. Користуватися реалізацією стандарту на базі попередньо розділених ключів (PSK) та протоколу 802.1x при наявності високошвидкісного каналу між мережами - не самий безпечний метод. VPN - це повна протилежність дорогій системі власних або орендованих ліній, які можуть використатися тільки однією організацією. Завдання VPN - надати організації ті ж можливості, але за набагато менші гроші. Загалом VPN та бездротові технології не конкурують, а доповнюють один одного. VPN працює поверх поділюваних мереж загального користування, забезпечуючи у той же час цілісність та конфіденційність передачі даних за рахунок спеціальних мір безпеки і застосування тунельних протоколів. Це забезпечує шифрування даних на кінці, що відправляє та дешифрування на приймаючому, тобто протокол організує "тунель", у який не можуть проникнути дані, не зашифровані належним чином. Додаткову безпеку може забезпечити шифрування не тільки самих даних, але й мережних адрес відправника та одержувача. Бездротову локальну мережу можна зрівняти з поділюваною мережею загального користування.

Загалом VPN мережа відповідає трьом умовам: конфіденційність, цілісність та доступність. Хоча ніяка VPN не є стійкою до DDoS-атак та не може гарантувати доступність на фізичному рівні просто в силу своєї віртуальної.

Основна частина

Дві найбільш важливі особливості VPN, особливо в бездротових середовищах, де є лише обмежений контроль над поширенням сигналу - це цілісність та конфіденційність даних. У ситуації, коли зловмисникові вдалося обійти шифрування по протоколі WEP та приєднатися до бездротової локальної мережі, то якщо VPN відсутній, то він зможе прослуховувати дані та втручатися у роботу мережі. Проте якщо пакети розпізнані то атака стає практично неможливою, хоча перехопити дані як і раніше легко. Включення у VPN елементу шифрування зменшує негативні наслідки перехоплення даних. VPN забезпечує не повну ізоляцію всіх мережних взаємодій, а здійснює такі взаємодії у більше контрольованих умовах із визначеними групами допущених учасників.

Розглянемо систему виявлення вторгнення. (Intrusion Detection System - IDS) - це пристрої, за допомогою яких можна виявляти та вчасно запобігати вторгненню в мережу. Вони діляться на два види: на базі мережі та на базі хоста. Мережні системи (Network Intrusion Detection Systems - NIDS) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил. Інший вид систем виявлення вторгнень представляють системи на базі хоста (Host Intrusion Detection Systems - HIDS). Вони встановлюються безпосередньо на вузлах та здійснюють спостереження за цілісністю файлової системи, системних журналів тощо. NIDS діляться у свою чергу на дві більші категорії: на основі сигнатур та на основі бази знань. Сигнатурні IDS найпоширеніші та простіше реалізуються, проте їх легко обійти і вони не здатні розпізнавати нові атаки. У таких системах події, що відбуваються у мережі, рівняються із ознаками відомих атак, які й називаються сигнатурами. Хоча якщо інструмент злому модифікувати з метою зміни якої-небудь частини сигнатури атаки, то така атака може залишитись непоміченою. Крім того, бази даних, що містять сигнатури, необхідно надійно захищати та часто обновляти. Інші IDS на основі бази знань стежать за мережею, збирають статистику про її поводження в нормальних умовах, виявляють різні особливості й позначають їх як підозрілі. Тому такі IDS ще називають заснованими на поводженні або статистичними. Для ефективної роботи статистичної IDS необхідно мати надійну інформацію про те, як поводиться мережа в нормальних умовах і це буде точкою відліку. Таку IDS обійти складніше, хоча і у неї є свої слабкі місця - помилкові спрацьовування та труднощі при виявленні деяких видів комунікацій по закритому каналі. Помилкові спрацьовування особливо ймовірні у бездротових мережах через нестабільність передавального середовища. Також атаки, проведені на ранніх стадіях періоду фіксації точки відліку, можуть спотворити процедуру навчання статистичної IDS, тому ризиковано розгортати її у промислових мережах. IDS для бездротової мережі повинна бути одночасно сигнатурною та статистичною. Частина програм для проведення атак на бездротові мережі мають чітко виражені сигнатури. Якщо вони виявляються у базі даних, то спрацьовує тривога. Проте у багатьох атак очевидних сигнатур немає, хоча

вони викликають відхилення від нормальної роботи мережі на нижніх рівнях стеку протоколів. Ці відхилення або аномалії можуть бути малопомітними. Виявлення таких аномалій - непросте завдання, по скільки практично не існує двох однакових бездротових мереж. Це відноситься і до провідних локальних мереж, хоча там немає радіоперешкод, відбиття, рефракції та розсіювання сигналу. Тому ефективне застосування IDS у бездротових мережах можливо тільки після тривалого періоду детального дослідження конкретної мережі. Загалом при розгортанні системи необхідно чітко розуміти, що, як і навіщо хочемо аналізувати і тільки тоді сконструювати потрібну систему IDS. Зібравши значний обсяг статистичних даних про роботу конкретної мережі, можна вирішити, що є аномальним поводженням, а що – ні та ідентифікувати проблеми зі зв'язком, помилки користувачів і атаки. Розглянемо проблеми та події які виникають на різних рівнях взаємодії у мережі.

Події на фізичному рівні [3]:

- наявність додаткових передавачів у зоні дії безпровідної мережі;
- використання каналів, які не повинні бути задіяні у системі захисту мережі;
- використання каналів, що перекриваються;
- раптова зміна робочого каналу одним або декількома пристроями, за яких ведеться спостереження;
- погіршення якості сигналу, високий рівень шуму тощо.

Такі події можуть свідчити про наявність проблем зі зв'язком або із мережею, про помилки допущені при конфігуруванні мережі, про появу невідомих пристроїв, про навмисне глушіння або про атаки.

Події, пов'язані з адміністративними або керуючими фреймами у мережі [3]:

- підвищена частота появи деяких типів фреймів;
- фрейми незвичайного розміру;
- фрейми невідомих типів;
- неповні, зіпсовані або неправильно сформовані фрейми;
- потік фреймів із запитами на від'єднання й припинення сеансу;
- часта поява фреймів із запитом на повторне приєднання в мережах, де не включений роумінг;
- фрейми з неправильними порядковими номерами;
- часта поява пробних фреймів;
- фрейми, у яких SSID відрізняється від SSID даної мережі;
- фрейми із широкомовним SSID;
- фрейми із часто змінюються або випадковими SSID;
- фрейми зі значеннями в поле SSID або інших полях, типовими для деяких інструментів вторгнення;
- фрейми з Mac-адресами, відсутніми в списку контролю доступу;
- фрейми з Mac-адресами, що дублюються;
- фрейми із часто змінюються або випадковими Mac-адресами.

Такі події можуть вказувати на неправильну конфігурацію мережі, проблеми зі зв'язком, сильні перешкоди, спроби застосування інструментів активного сканування мережі, підробку Mac - адресів, присутність у мережі сторонніх клієнтів, спроби вгадати або підібрати методом повного перебору закритий SSID тощо.

Події, пов'язані із фреймами протоколів 802.1x/EAP [3]:

- неповні, зіпсовані або неправильно сформовані фрейми протоколу 802.1x;
- фрейми з такими типами протоколу EAP, які не реалізовані в даній бездротовій мережі;
- багаторазові фрейми запиту та відповіді процедури аутентифікації EAP;
- багаторазові фрейми з повідомленням про невдалий аутентифікації EAP;
- затоплення фреймами початку й завершення сеансу EAP;
- фрейми EAP аномального розміру;
- фрейми EAP з некоректним значенням довжини;
- фрейми EAP з неправильними "вірчими грамотами";
- фрейми EAP, що приходять від невідомих аутентифікаторів (фальшива точка доступу);
- незавершена процедура аутентифікації по протоколі 802.1x/EAP.

Такі події можуть вказувати на спроби прорватися через процедуру аутентифікації, описану в протоколі 802.1x, у тому числі й шляхом розміщення фальшивого пристрою та проникнення у мережу за допомогою атаки методом повного перебору або проведення витонченої DoS-атаки, спрямованої на вивід з ладу механізмів аутентифікації.

Події, пов'язані із загальними проблемами зв'язки [3]:

- втрата зв'язку;
- раптовий сплеск навантаження на мережу;
- раптове зменшення пропускної здатності мережі;
- раптове збільшення затримок у каналі;
- підвищений рівень фрагментації пакетів;
- часті повторні передачі.

Такі події заслуговують більш пильного вивчення для виявлення причин помилок.

Інші події [3]:

- атаки на верхні рівні стека протоколів, що викликають спрацьовування "традиційної" IDS;
- сторонній адміністративний трафік, адресований точці доступу;
- постійне дублювання або повтор пакетів з даними;
- пакети з даними, у яких зіпсовані контрольні суми або MIC, формовані на канальному рівні;
- багаторазові спробами одночасного приєднання до мережі.

Такі події можуть свідчити про успішну або невдалу атаку, про наявність хоста з некоректними настроюваннями безпеки, про спроби одержати контроль над точкою доступу та змінити її конфігурацію, про застосування інструментів для впровадження свого трафіка, про DoS-атаку проти хостів із включеним протоколом 802.11i тощо.

Висновки

В результаті проведеної роботи проаналізовано, досліджено та виділені типові загрози інформації – потенційно несприятливі дії на інформацію. Проведений аналіз загроз інформації є одним з найбільш важливих питань при побудові захищених безпровідних мереж. Такий аналіз має виявити можливі загрози інформації, аномалії та показати з якого боку мережі нам слід чекати атаки на безпровідні мережі. Виявлення таких аномалій - непросте завдання, по скільки практично не існує двох однакових бездротових мереж. Тому ефективне застосування IDS у бездротових мережах можливо тільки після тривалого періоду детального дослідження конкретної мережі. При розгортанні системи необхідно чітко розуміти, що, як і навіщо хочемо аналізувати і тільки тоді сконструювати потрібну систему безпеки. Зібравши значний обсяг статистичних даних про роботу конкретної мережі, можна вирішити, що є аномальним поводженням, а що – ні та ідентифікувати проблеми зі зв'язком, помилки користувачів і атаки.

Література

1. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2004. – 992 с.

2. Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньган. - М.: ДМК Пресс, 2004. - 616 с.: ил.

3. Норткатт С. Обнаружение вторжений в сеть / С. Норткатт, Д. Новак, Д. Маклахлен. – Изд-во "ЛОРИ", 2001. - 384 с.

Надійшла до редакції
24.1.2013 р.

УДК 004

Є.С. ГРИЦАЮК, В.М. ЧЕШУН
Хмельницький національний університет

ПРОБЛЕМНІ АСПЕКТИ АВТОМАТИЗАЦІЇ В ПІДВИЩЕННІ НАДІЙНОСТІ РОБОТИ СИСТЕМИ КЛІЄНТ-БАНК

Досліджено проблеми забезпечення надійної роботи системи “Клієнт-банк” в умовах ризику спроб несанкціонованого доступу до приватної інформації та спроб крадіжок коштів. На сьогоднішній день в банківській сфері, з впровадженням автоматизованих технологій обробки інформації та розширенням спектру послуг, які надаються, і прискоренням оборотності коштів ці проблеми значно загострюються та потребують негайного вирішення. Визначено основні напрямки автоматизованого розв’язання виявлених проблем.

Ключові слова: інформація, система “Клієнт-банк”, захист інформації, засоби криптографії.

Investigated the problems to ensure reliable operation of the system "Client-Bank" at risk of unauthorized access to personal information and attempted theft of funds. To date, with the introduction of automated information processing technologies, expanding the range of services provided and to accelerating the turnover of funds greatly exacerbated these problems and require urgent attention in the banking industry. Defined the main directions of automatic decision of problems.

Keywords: information, system "Client-Bank", protection of Information, means of cryptography.

Вступ

Спосіб дистанційного надання послуг клієнтам у сфері банківського обслуговування перетворився на цілком самостійну форму ведення бізнесу. Технологія дистанційного банківського обслуговування “домашній банкінг” (home banking) або “віддалений банкінг” (remote banking), що дає змогу клієнту отримувати банківські послуги без відвідин офісу банку, існує вже більше двадцяти років.

Як видно із самої назви, “віддалений банкінг” є формою надання банківських послуг не в банківському офісі при безпосередньому контакті клієнта і банківського службовця, а в офісі клієнта, в його будинку і скрізь, де це допускається системою і є зручним.

Технологія “home banking” була розроблена на початку 80-х років XX ст., коли банки Західної