телефонного апарату. В даний час жоден з скремблерів, що працюють на міських телефонних лініях, не обладнаний надійною системою запобігання перехопленню мовної інформації з приміщення по телефонній лінії, що перебуває у відбої [3].

Не дивлячись на великий асортимент приладів пропонованих на ринку використовування тільки одного приладу не забезпечує надійного захисту телефонної лінії від несанкціонованого зняття інформації. Для надійного захисту необхідно застосовувати декількох приладів.

Література:

1. Быков С.В. Классификация устройств съема информации в телефонной линии - Новосибирск. Сборник научных трудов НГТУ №2 1999г.

3. Лагутин В.С. Петраков А.В. Утечка и защита информации в телефонных каналах - М.: Энергоатомиздат 1996г

4. Лысов А.В. Остапенко А.Н. Телефон и безопасность (Проблемы защиты информации в телефонных сетях) - Санкт-Петербург: Политехника, 1997г.

УДК 004.681

Довлад О.А.
Західноукраїнський національний університет імені Володимира Даля

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛІ ПРОЦЕСУ АТАКИ НА ТРАФІК ЛОКАЛЬНОЇ МЕРЕЖІ

Актуальність теми: Інформатизація є характерною рисою сучасного життя. Новітні технології активно впроваджуються в усі сфери діяльності суспільства та відіграють важливу роль. Актуальність зазначеної теми обумовлено високими темпами зростання парку персональних комп'ютерів та об'ємів обробляємої інформації; об'єднання їх в локальні мережі та підключення до Інтернету; розширенням кола користувачів, що мають безпосередній доступ до ресурсів та масивів даних; зосередження в єдиних базах даних інформації різної за призначенням та приналежністю; зростання обчислювальної потужності сучасних комп'ютерів при одночасному спрощенні їх в експлуатації.

Метою роботи є забезпечення необхідного рівня захисту інформації, що обробляється у локальних мережах, шляхом розробки моделі процесу атаки на мережевий трафік.

Для досягнення зазначеної мети необхідно вирішити декілька задач, серед яких:

- дослідити фактори, які впливають на рівень інформаційної захищеності локальної мережі;
- проаналізувати можливі причини, що приводять до зниження необхідного рівня захищеності мережі;
- розробити математичну модель процесу атаки на мережевий трафік;
- запропонувати методику, здатну забезпечити потрібний рівень захищеності мережі від атак на її трафік;

Найчастіше термін «локальні мережі» або «локальні обчислювальні мережі» розуміють буквально, тобто це такі мережі, які мають невеликі, локальні розміри, з'єднують близько розташовані комп'ютери. Проте досить подивитися на характеристики деяких сучасних локальних мереж, щоб зрозуміти, що таке визначення не точно. Наприклад, деякі локальні мережі легко забезпечують зв'язок на відстані декількох десятків кілометрів. З іншого боку, по глобальній мережі можуть зв'язуватися комп'ютери, що знаходяться на сусідніх столах в одній кімнаті, але її чомусь ніхто не називає локальною мережею. Невірно і визначення локальної мережі як малої мережі, яка об'єднує невелику кількість комп'ютерів. Дійсно, як пра-

вило, локальна мережа зв'язує від двох до декількох десятків комп'ютерів. Але граничні можливості сучасних локальних мереж набагато вищі: максимальне число абонентів може досягати тисячі.

Інколи локальну мережу визначають як «систему для безпосереднього з'єднання багатьох комп'ютерів». При цьому мається на увазі, що інформація передається від комп'ютера до комп'ютера без яких-небудь посередників і по єдиному середовищу передачі. Але в межах однієї мережі можуть використовуватися як електричні кабелі різних типів (вита пара, коаксіальний кабель), так і оптоволоконні кабелі. Визначення передачі «без посередників» також не коректно, адже в сучасних локальних мережах використовуються репітери, концентратори, комутатори, маршрутизатори, мости, які іноді здійснюють досить складну обробку переданої інформації.

Найточніше було б визначити як локальну таку мережу, яка дозволяє користувачам не помічати зв'язки. По суті, комп'ютери, зв'язані локальною мережею, об'єднуються в один віртуальний комп'ютер, ресурси якого можуть бути доступні всім користувачам, причому цей доступ не менш зручний, чим до ресурсів, що входять безпосередньо в кожен окремий комп'ютер. Під зручністю в даному випадку розуміється висока реальна швидкість доступу, швидкість обміну інформацією між додатками.

З даного визначення виходить, що швидкість передачі по локальній мережі обов'язково повинна зростати по мірі зростання швидкодії найбільш поширених комп'ютерів. Таким чином, головна відмінність локальної мережі від будь-якої іншої — висока швидкість передачі інформації по мережі. Також принципово необхідний низький рівень помилок передачі, викликаних як внутрішніми, так і зовнішніми чинниками. Тому локальні мережі обов'язково використовують високоякісні, що спеціально прокладаються, і добре захищені від перешкод лінії зв'язку.

Особливе значення має і така характеристика мережі, як спроможність роботи з великими навантаженнями, тобто з високою інтенсивністю обміну (з великим трафіком). Механізм управління обміном може гарантовано успішно працювати тільки у тому випадку, коли наперед відомо, скільки комп'ютерів (абонентів, вузлів) допустимо підключити до мережі. Інакше внаслідок перевантаження забуксує будь-який механізм управління. Нарешті, мережею можна назвати тільки таку систему передачі даних, яка дозволяє об'єднувати до декількох десятків комп'ютерів.

Таким чином, можна сформулювати характерні ознаки локальної мережі:

- висока швидкість передачі інформації, велика пропускна спроможність мережі;
- низький рівень помилок передачі;
- ефективний, швидкодіючий механізм управління обміном по мережі;
- наперед чітко обумовлена кількість комп'ютерів.

Правда, зараз вже не можна провести чітку межу між локальними і глобальними мережами. Більшість локальних мереж мають вихід в глобальну. Але характер переданої інформації, принципи організації обміну, режими доступу до ресурсів усередині локальної мережі, як правило, сильно відрізняються від тих, що прийняті в глобальній мережі.

При наявності багатьох переваг та зручностей, які ми отримуємо при наявності та використанні локальних мереж, існують ряд недоліків, які слід врахувати:

- мережа вимагає додаткових матеріальних витрат на купівлю мережевого устаткування, програмного забезпечення, на прокладку кабелів і навчання персоналу;
- мережа вимагає наявність спеціаліста, який займатиметься контролем її роботи, модернізацією, управлінням доступу до ресурсів, усуненням можливих несправностей, захистом інформації і резервним копіюванням;
- мережа обмежує можливості переміщення комп'ютерів, підключених до неї, оскільки при цьому може знадобитися перекладання з'єднувальних кабелів;

- мережа є середовище для розповсюдження комп'ютерних вірусів, тому питанням захисту від них доведеться приділяти значно більше уваги, ніж у разі автономного використання комп'ютерів.
- мережа різко підвищує небезпеку несанкціонованого доступу до інформації з метою її крадіжки або знищення. Інформаційний захист вимагає проведення цілого комплексу технічних і організаційних заходів.

Серед основних загроз, найбільш небезпечних , слід зазначити наступні:

- доступ до мережевого трафіку з метою отримання доступу до інформації, що передається у відкритому вигляді;
- порушення цілісності переданої інформації. При цьому може модифікуватися як призначена для користувача, так і службова інформація, наприклад підміна ідентифікатора групи, до якої належить користувач;
- отримання несанкціонованого доступу до інформаційних ресурсів, наприклад з використанням підміни однієї із сторін обміну даними з метою отримання доступу до сервера від імені іншого користувача;
- спроба здійснення ряду дій від імені зареєстрованого користувача в системі, наприклад зловмисник, скомпрометувавши пароль адміністратора, може почати спілкування в мережі від його імені.

Причинами виникнення даних загроз в загальному випадку можуть виявитися:

- наявність слабких місць в базових версіях мережевих протоколів. Так, при використанні протоколів TCP/IP порушник може впровадити в мережу помилковий ARP-сервер;
- уразливості спеціалізованих захисних механізмів. Наприклад, причиною виникнення підміни сторони інформаційного обміну може служити уразливість процедур аутентифікації клієнтів при доступі до сервера;
- некоректне призначення рівня доступу;
- використання в якості каналів передачі даних загальнодоступного середовища, наприклад застосування топології побудови мережі із загальною шиною. В даному випадку зловмисник може використовувати програмне забезпечення, що дозволяє проглядати передані в мережі пакети;
- некоректне адміністрування ОС;
- помилки в реалізації ОС;
- помилки персоналу.

Забезпечення необхідного рівня захищеності інформації в локальних мережах є комплексним завданням і досягається при допомозі коректного адміністрування мережевих настройок, додаткових захисних механізмів (шифрування, аутентифікації сторін і др.), організаційних методів захисту і контролю за їх неухильним дотриманням (використанням системи аудиту).

Дієвим методом підтримки надійного функціонування системи безпеки в локальних мережах є використання системи аудиту. Його дієвість полягає не тільки в своєчасному реагуванні адміністратора безпеки на порушення вибраної політики безпеки, але і в можливості притягати зареєстрованих користувачів до відповідальності.

Застосування особливих топологій побудови локальних мереж дозволяє мінімізувати можливість застосування засобів, які дозволяють контролювати середовище передачі даних з метою отримання доступу до мережевих пакетів. Так, використання мережевої топології типу «зірка» ускладнює доступ порушнику до мережевих пакетів, що йому не належать, за умови впровадження організаційних заходів, або шифруванням трафіку.

Для виключення можливості неавторизованого входу в мережу можна використовувати комбінований підхід - пароль спільно з аутентифікацією користувача по персональному носію «ідентифікаційної інформації». Як носій може використовуватися пластикова карта, смарт-карта, ключові дискети або пристрої для ідентифікації особи за біометричною інформацією (по

радужній оболонці ока або по спеціальному програмному забезпеченню). За допомогою цих заходів можна підвищити ступінь захисту від несанкціонованого доступу.

Література

1. *Партыка Т. Л., Попов И. И.* Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. — М.: ФОРУМ: ИНФРА-М, 2002. - 368 с.: ил.
2. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты.-М.: ДМК, 2000. – 448с.: ил
3. http://www.intuit.ru

УДК 621.391:519.72

Н.Ф. Казакова
Міжнародний гуманітарний університет

СИНТЕЗ АЛГОРИТМУ РОБОТИ ТА ТЕХНІЧНА РЕАЛІЗАЦІЯ ДЕКОМПОЗИЦИОНОГО ГЕНЕРАТОРА ПОСЛІДОВНОСТІ GMW

Постановкою питання для дослідження в даному напрямку є завдання знаходження простого алгоритму генерації двійкових послідовностей GMW на основі генерації зрушених копій двійкової *m*- послідовності тієї ж довжини, а також освітлення переваг отриманого методу в порівнянні з відомими, які засновані на генерації *q*- та *m*- послідовностей [1]. Отже, метою є конструювання нового класу ПВП великого об'єму з близькою ідеальною автокореляцією і складною імітаційною структурою, а також розробка методу і структурної схеми пристрою їх генерації для захищених систем зв'язку. Рішення цієї проблеми розширює можливість вибору максимальної за об'ємом множини сигналів з заданою завадостійкістю і полегшує побудову пристроїв синхронізації абонентських приймачів, наприклад, для широкосмугових систем з CDMA, при заданому числі абонентів. На основі отриманої послідовності можуть бути синтезовані системи ортогональних кодових послідовностей великої лінійної складності та здійснене криптозахищене скремблювання передаваної інформації [2].

Пристрій, який розроблюється для формування двійкових ПВП GMW, дозволяє отримати одну або декілька форм ПВП при значно менших технічних витратах в порівнянні з відомими аналогічними пристроями. Значне зменшення витрат можна розглядати, як свого роду компенсацію за програш в числі форм, що генеруються [3]. Структурна схема пропонованого пристрою для генерації ПВП представлена на рис.1.

Робота пристрою полягає в наступному. Тактові імпульси, що поступають з генератора, з частотою f_T просувають записану в регістрі розподільника «одиницю», яка, проходячи через ту або іншу схему АБО комутатора, відкриває пов'язану з нею схему збігу, тим самим пропускаючи двійковий сигнал з виходу відповідного розряду регістра генератора базисної послідовності на вхід елементу АБО. Вихідні імпульси розподільника з частотою $\frac{f_T}{\varepsilon}$ поступають на тактовий вхід регістра зрушення генератора базисної послідовності, здійснюючи циклічне зрушення інформації в цьому регістрі. Таким чином, за тривалість періоду базисної послідовності на виході елементу АБО з'являться сигнали всіх 2^N-1 двійкових символів послідовності, що генерується пристроєм.