УДК 004.451.64

К.т.н., доцент Марченко О. І., магістрант Дмитришин Б.І.

Національний технічний університет України
«Київський політехнічний інститут»

СПОСІБ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ З АВТОМАТИЧНИМ ВИБОРОМ КАНАЛУ ЗВ'ЯЗКУ

Abstract

Oleksandr I. Marchenko, assoc. prof., PhD; Bohdan Dmytryshyn, student
Technique for protecting information in data transmission networks with automatic selection of a data channel

This paper is devoted to the development of some technique for protecting information which is transmitted in local area network which is divided into territorially separated segments and connected by several unreliable data channels. Special hardware and software is proposed for development and usage. The ways for further research are proposed as well.

Вступ

Широке використання інформаційно-телекомунікаційних систем, а також пов'язане з цим збільшення об'ємів інформації, яка обробляється, вимагають розширення кола користувачів, яким потрібен доступ до ресурсів і даних інформаційних систем.

Найдоступнішим методом організації такого доступу є створення локальних мереж. Але використання таких мереж у регіональному масштабі з можливістю доступу до глобальної мережі Інтернет породжує питання безпеки зберігання та передачі інформації. Тому, при експлуатації таких систем значна увага приділяється захисту інформаційних ресурсів від несанкціонованих користувачів, що бажають їх використати, модифікувати чи просто знищити.

Під захистом інформації мається на увазі підтримання цілісності, доступності та конфіденційності даних, що використовуються для введення, зберігання, обробки та передачі. Також важливою складовою захисту інформації є забезпечення її безпеки при передачі каналами зв'язку, оскільки саме на шляху передачі інформаційного контенту можливе її перехоплення, що, звичайно, ставить під загрозу конфіденційність даних.

Оскільки для зберігання, обробки та передачі даних використовується комп'ютерне та мережне обладнання, то, для вирішення

проблеми захисту інформації необхідне поєднання роботи програмних та апаратних засобів.

Постановка задачі

Задача полягає в розробці способу захисту інформації в локальних територіально розділених мережах передачі даних. Локальні територіально розділені мережі, як правило, мають складну топологію та будуються з використанням різних фізичних комутацій, для можливості створення мережі, яка функціонує з декількома каналами зв'язку.

Термінологія

MAC-адреса — унікальний ідентифікатор, що надається різному устаткуванню для комп'ютерних мереж. У таких мережах, як, наприклад, Ethernet-мережі, MAC-адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу.

BGAN – тип мережі супутникового зв'язку. Використовує три супутника, розміщені на геостаціонарній орбіті, що надають зону покриття практично на всій території земної кулі.

USB-токен – електронний пристрій, призначений для запису на нього параметрів алгоритму функціонування пристрою захисту інформації та параметрів конфігурування віртуальної приватної мережі.

Аналіз існуючих методів та способів

Для вирішення поставленої задачі проведено аналіз сучасних методів і засобів захисту інформації в мережах передачі даних, як програмних, так і апаратних. До програмних засобів захисту інформації можна віднести програмні шифратори інформації та брандмауери. Надійність таких методів захисту є сумнівною, оскільки ці програмні засоби працюють під керуванням операційних систем, в більшості випадків MS Windows, які легко піддаються зовнішнім атакам. Це може призвести до втрати цінної та конфіденційної інформації.

Апаратні засоби не мають таких суттєвих недоліків, оскільки їх головна ідея – реалізація у вигляді автономних пристроїв, в яких алгоритми шифрування виконуються або в модулях ПЛІС [1], або в захищених електронних модулях, побудованих на базі процесорів чи мікроконтролерів з використанням оригінальних операційних систем. Брандмауери можна віднести як до програмних, так і до апаратних засобів, в залежності від реалізації.

Проблемою обох видів засобів захисту інформації є те, що доступ до

інформації може відбуватися не шляхом атаки на робочі станції, а шляхом перехопленням інформації в каналі зв'язку. Такий тип атаки проконтролювати досить важко, що ставить під загрозу збереження конфіденційності інформації.

Опис способу

Виходячи зі сказаного вище, пропонується спосіб захисту інформації в мережах передачі даних, який може бути застосований для розробки апаратно-програмного комплексу захисту інформації з характеристиками, які мінімізують вразливість інформаційно-телекомунікаційної системи. Такий комплекс задовольняв би наступним вимогам:

- здійснювати апаратне шифрування інформації;
- мати засоби аутентифікації користувача;
- бути стійким до відмов каналів зв'язку;
- здійснювати автоматичний вибір каналу зв'язку.

Запропонований спосіб захисту інформації полягає в автоматичному виборі каналу з великого пулу можливих каналів, в яких використовуються різні фізичні протоколи передачі даних, що створює додаткові перешкоди на шляху перехоплення інформації. Крім того, способом передбачається можливість випадкового вибору каналу та його періодична зміна, що суттєво збільшує захищеність інформації при обміні між територіально віддаленими сегментами локальної мережі, а також передбачається використання USB-токенів.

Для підвищення рівня безпеки закритої мережі адміністрування пристроїв захисту здійснюється тільки через окремий USB-порт з використанням USB-токенів. Програмування USB-токенів відбувається на спеціалізованому комп'ютері – центрі генерації ключів, який є незалежним від інших комп'ютерів та не підключеним до будь-якого типу мереж з міркувань безпеки. Центр генерації створює конфігурацію для кожного з пристроїв захисту інформації враховуючи таблиці тунелів (в найпоширенішому варіанті – з використанням MAC-адрес), параметри мережевих інтерфейсів та унікальні номери кожного з пристроїв.

Апробація способу

На основі запропонованого способу розроблено апаратний комплекс, який здійснює криптографічні перетворення вмісту IP-пакетів з довіреної зони, проводить їх інкапсуляцію та відправляє вже нові пакети у зону ризику. Між двома модулями комплексу повинен бути організований тунель (програмне представлення допустимих маршрутів передачі

інформації), що заноситься до модулів за допомогою спеціальних ключів – USB-токенів. Модуль, який обслуговує приймаючий сегмент віддаленої локальної мережі, здійснює обернене криптографічне перетворення з використанням раніше узгоджених ключових параметрів та відправляє його адресату в цій довіреній зоні. Апаратна частина комплексу побудована на ПЛІС компанії ALTERA [2], що дало змогу збільшити кількість криптографічних перетворень та підняти продуктивність до 6% у порівнянні з іншими пристроями шифрування IP-пакетів.

При розробці комплексу була вирішена задача організації зв'язку віддалених сегментів локальної мережі з використанням декількох каналів зв'язку [3]. Як канал зв'язку може бути використаний орендований канал у мережі супутникового зв'язку Inmarsat BGAN чи довільній VSAT-мережі, канал з використанням високошвидкісного бездротового доступу до мережі Інтернет на базі технології 3G чи WiMax, канал короткохвильового зв'язку чи стаціонарне дротове підключення мережі PSTN.

Висновки

В роботі запропоновано спосіб захисту інформації, що дозволяє захистити інформацію в локальних мережах передачі даних на основі декількох ненадійних каналів зв'язку. Автоматичний вибір каналу зв'язку, що пропонується цим способом, надає додатковий рівень безпеки під час передачі. Чим більше каналів зв'язку є доступними, тим безпечнішою стає система.

На основі запропонованого способу був створений апаратно-програмний комплекс. Швидкість обробки IP-потоку досягає 1 Гбіт/с, максимальна кількість захищених з'єднань з клієнтами становить 8192.

Запропоноване рішення є новим та унікальним, дозволяє організувати обмін інформацією між декількома територіально віддаленими сегментами мережі з використанням довільних незахищених каналів зв'язку.

Література

1. Проектирование на ПЛИС. Архитектура, средства и методы. – М.: «Додэка-XXI», 2007. – 408 с.
2. *Комолов Д.А., Мальк А.В.* – Системы автоматизированого проектирования фирмы Altera Max+plusII и Quartus II. Краткое описание и самоучитель. – М.: ИП-РадиоСофт, 2002. – 352 с.
3. *Cyclone IV Device Handbook*. ver 1.5, Altera Corporation, 2010. – 641 с.