

количеством особых точек и идентификационных параметров синусоидальных решеток для повышения емкости внедрения, обеспечивает устойчивость к атакам типа «печать-сканирование», масштабирование (0,5...1,5 раза), поворот (300, 750, 1800), смещение (сдвиг на любое число пикселей).

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ОНЛАЙН-МАГАЗИНЕ ZORBASHOP.COM

В.А.Вишняков, Храйба Мохаммед

В докладе представлены используемые методы защиты информации в онлайн-магазине (zorbashop.com). Выделены следующие направления защиты: метод шифрования с цифровой подписью, использование брандмауэра, защищенный протокол Secure Sockets Layer (SSL), разрешение доступа.

Метод шифрования: использован алгоритм MD5 и кэш для хранения паролей, MD5 - это алгоритм, который, использует в качестве входных данных сообщение произвольной длины и выдает на выходе 128-битовое значение. Вводимые данные последовательно разбиваются на блоки по 512 бит. В алгоритме MD5 используются массив значений $T[i]$, $i=1, 2, \dots, 64$. Кэш содержит случайные данные, которые используются как дополнительный вход в систему. Хэш-функция, которая хэширует пароль. Основная функция кэша — защита от символьных атак против списка хэш-паролей и против заранее вычисленных в таблице атак.

Брандмауэр создает дополнительный слой безопасности по всему Интернет-магазину. С помощью правила брандмауэра, он будет блокировать нападавших или вносить их в черные списки и запрещать им доступ к сайту. Он имеет сканер для предоставления рекомендации о установке в нашем магазине.

Защищенный протокол: Secure Sockets Layer (SSL) используя протокол защищенных Сокетов (SSL) с ключом шифрования длиной 128-бит (самый высокий уровень, имеющихся в продаже).

Капча (CAPTCHA) — это визуальное средство, которое гарантирует, что человеческое существо, а не компьютер взаимодействует с сайтом. Капча может быть использован как для администратора так и для клиентов.

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ МЕЖСЕТЕВОГО ЭКРАНА CISCO ASA 5520

Р.М. Горбуль

Корпоративная сеть является неотъемлемой частью любой современной компании. Корпоративная сеть требует высокого уровня защиты, которую может обеспечить межсетевой экран Cisco ASA 5520. Данный межсетевой экран является аппаратным средством обеспечения защиты. Произведен анализ функций и возможностей межсетевоего экрана. Межсетевой экран обеспечивает пропускную способность 450 Мбит/с для не зашифрованного трафика и 225 Мбит/с для зашифрованного. Опытным путем было выявлено, что межсетевой экран выдерживает документированную пропускную способность как для не зашифрованного, так и зашифрованного видов трафика, что является отличным показателем для такого класса устройств. При помощи средств виртуализации были смоделированы режимы работы Active/Active и Active/Standby двух межсетевых экранов в связке для тестирования отказоустойчивости. Была смоделирована конфигурация с использованием нескольких контекстов или другими словами, несколькими виртуальными брандмауэрами, каждый со своей конфигурацией и логическими интерфейсами. Также была исследована функция глубокого анализа протоколов прикладного уровня и проверена поддержка протоколов динамической маршрутизации OSPF и EIGRP. Межсетевой экран Cisco ASA 5520 обеспечивает высокий уровень защиты для корпоративных сетей среднего и малого бизнеса.