УДК 681.325

СРЕДСТВА ЗАЩИТЫ ИНТЕРНЕТ ПОРТАЛОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Шмидт Д.Ю., – аспирант
Кубанский Государственный Технологический Университет

В статье излагаются основная модель защиты Интернет порталов от несанкционированного доступа. Некоторое распространенное программное обеспечение, их достоинства и недостатки, а также сильные и слабые стороны тех или иных программных продуктов защиты Интернет порталов от несанкционированного доступа.

In clause are stated the basic model of protection the Internet of portals from not authorized access. Some widespread software, their merits and demerits, and also strong and weaknesses of those or other software products of protection the Internet of portals from not authorized access.

В настоящее время большинство существующих сетей функционируют на давно существующем протоколе TCP/IP Версии 4.02 (IPv4),он имеет свои недостатки которые, тем не менее, не мешают ему быть одним из самых популярных протоколов пакетной передачи данных. Но в скором времени, его должен сменить более надежный и более защищенный протокол TCP/IP (IPv6) версии 6.0. Связано это в первую очередь с тем, что данный протокол расширит адресное пространство, которое на данный момент себя исчерпало и осталось мало свободных MAC- адресов (физический адрес, зарегистрированный для конкретного оборудования в конкретном месте) для регистрации новых порталов. По сравнению со старым TCP/IP 4.02, он более защищен от перехвата пакетов, которые так любят использовать взломщики.

Для разграничения доступа к Интернет порталу и защиты от несанкционированного доступа необходимо установить защиту портала. В этом отношении все существующие защиты можно классифицировать на два типа это **криптозащиты** (называемые также защита Кирхгофа) и **логические** защиты. Согласно правилу Кирхгофа стойкость криптозащит определяется стойкостью секретного ключа. Даже если становится

Отформатировано: Шрифт: 14 пт
Отформатировано: Междустр.интервал: одинарный
Отформатировано: Шрифт: 14 пт
Отформатировано: Шрифт: 14 пт
Удалено: -
Отформатировано: Шрифт: 14 пт
Отформатировано: Шрифт: 14 пт, курсив
Удалено: ,
Отформатировано: английский (США)
Удалено: ¶
Отформатировано: английский (США)
Удалено: IPv4)
Удалено: которые
Удалено: с
Удалено: адресо
Удалено: в
Удалено:
Удалено: (
Удалено: в
Удалено: адрес
Удалено: ,
Удалено: п
Удалено: пакетов
Удалено: в
Удалено: с
Удалено: е

известен алгоритм такой защиты, то это не сильно упрощает его взлом. При условии правильного выбора длины ключа, защиты Кирхгофа не ломаемы в принципе, конечно, если нет грубых ошибок в их реализации. Но криптозащиты с подобными ошибками в категорию защит Кирхгофа просто не попадают.

Стойкость логических защит, напротив определяется степенью секретности защищенного алгоритма, но отнюдь не ключа, вследствие чего надежность защиты держится на одном лишь предположении, что защитный код программы может быть или изучен или изменен. Рядовых пользователей абсолютно не интересует, что собой представляет механизм защищенного приложения портала. Для взломщика же наоборот, если исходный пароль используется для расшифровки критически важных модулей , то здесь есть несколько путей обхода защиты.

Возможно, исследуя программу с помощью дизассемблера или декомпилятора отыскать эталонный пароль и подставить его программе во время проверки, заставляя сравнивать его с самим собой. Можно пойти еще дальше и заставить защиту сравнивать введенный пароль не с эталоном, а с самим собой, или же найти ветвь программы, которая в процессе сравнение пароля не приведет к отказу, а откроет доступ на дальнейшую работу. Поэтому такой тип защит может быть очень быстро обезврежен и получен несанкционированный доступ к данным. Лишь особо сложным защитам удается выстоять перед попытками несанкционированного доступа один - два дня. Все происходит так, потому что большинство разработчиков программного обеспечения совершенно не разбираются в защитах и просто не представляют, во что именно компилятор перерабатывает исходный код. По этой причине с недавнего времени большинство разработчиков защиты комбинируют логическую защиту с криптографической, дополняя свои пакеты системами шифрования данных. Вследствие чего даже если и удастся

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: длинны

Удалено: конечно

Удалено: интересует

Удалено: из

Удалено: ебя

Удалено: программы

Удалено: ожно

Удалено: ,

Удалено:

снять логическую защиту, то с расшифровкой данных придется потратить не один месяц, все зависит от стойкости ключа, которым эта информация кодировалась.

Анализируя архитектурные решения, Система обеспечения безопасности информации (СОБИ) портала, начнем с цели защиты портала. Прежде всего, необходимо выделить объект защиты. Естественно, что защищаем информацию, причем не только конфиденциальную, как обычно полагают, - нет, в портальном решении должна защищаться и открытая информация. Вспомним такую распространенную цель хакерских атак, как искажение или замена главной страницы популярных порталов и Web-сайтов. Это означает, что в данном случае нужно предпринять контрмеры против нарушения целостности информации.

Система защиты портала должна обеспечивать конфиденциальность, целостность и доступность информации. Она должна устранять либо компенсировать угрозы (существует обобщающее понятие "парирование угроз"). Полный перечень угроз портальной информации, сгруппированный по трем базовым свойствам безопасности информации (конфиденциальность, целостность, доступность), выглядит следующим образом:

Конфиденциальность:

– хищение информации;

– незаконное копирование и распространение;

– утрата информации.

Целостность:

– модификация информации;

– отрицание подлинности;

– навязывание ложной информации.

Доступность:

– уничтожение информации;

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: всего

Удалено: -

Удалено: -

Удалено: -

Удалено: -

– блокирование доступа.

Ряд угроз можно предотвратить организационно-правовыми методами. Угрозу незаконного копирования и распространения, т. е. нарушения авторских прав можно эффективно устранить только с использованием правовых методов. Введение и практическая реализация более жестких правовых норм и законов, связанных с нарушением конфиденциальности, целостности, доступности информации, может уменьшить число вторжений на сайты и порталы.

Какие задачи с учетом оставшихся (после применения организационно-правовых методов) угроз должна решать СОБИ. Получается следующий список:

– защита от несанкционированного доступа к ресурсам портала (как пользователей, не имеющих соответствующих полномочий, так и посторонних лиц);

– контроль подлинности и целостности ресурсов портала;

– централизованное управление средствами СОБИ на основе политики безопасности портала;

– оперативный аудит безопасности портала, обеспечения полной подконтрольности всех совершаемых порталом операций;

– организация безопасного подключения портала к Интернету;

– обнаружение вторжений и антивирусная защита.

Анализ показывает, что на рынке имеются продукты, способные закрыть эти задачи по отдельности. Но эти продукты нужно интегрировать между собой. Следовательно, можно построить защищенный портал, но только путем интеграции существующих продуктов.

Как правило, хорошая система защиты бывает многоуровневой. Основную роль в решении поставленных задач играют **сетевой** и **прикладной уровни** обеспечения безопасности портала. Причем

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: -

Удалено: снизить

Удалено: -

Удалено: -

Удалено: -

Удалено: -

Удалено: -

Удалено: -

Удалено: Как можно догадаться,

Удалено: о

Удалено: ,

Удалено: п

прикладной уровень образуют, как правило, программные продукты, а сетевой - программно-технические.

Таким образом, **прикладной уровень** обеспечивает безопасность информации портала на более высоком иерархическом уровне. На прикладном уровне необходимы функции безопасности, недостижимые на более низких уровнях, а именно:

– идентификация пользователей;

– однократная аутентификация пользователей;

– ролевое управление доступом к информационным ресурсам портала;

– контроль подлинности и целостности некоторых ресурсов портала с применением технологии электронной цифровой подписи (ЭЦП);

– мониторинг и аудит.

На рынке не существует коробочного программного обеспечения для СОБИ портала, которое бы решало все эти задачи. Но существуют линейки продуктов, например, Tivoli от IBM, Sun One от Sun Microsystems, Dallas Lock ООО «Конфидент», которые после процесса интеграции могут быть использованы при разработке СОБИ портала.

Компания IBM со своим набором продуктов IBM Tivoli Identity Manager (ITIM) и IBM Tivoli Access Manager (ITAM) наиболее близко подошла к готовому решению прикладного уровня для СОБИ портала. Компания Microsoft для обеспечения безопасности портального решения использует как встроенные механизмы безопасности платформы Windows, так и отдельные продукты, например, прокси-сервер ISA 2003.

Сетевой уровень защиты портала обладает более насыщенным функционалом, возможно, потому, что любая внешняя атака, как правило, начинается на сетевом уровне. Добавим сюда еще вирусы и злонамеренный код, обычно проникающий через периметр корпоративной сети. Для противодействия существующим угрозам на сетевом уровне

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: -

Удалено: -

Удалено: -

Удалено: -

Удалено: -м

Удалено: -

Отформатировано: Шрифт: 14 пт

Удалено: ,

Удалено: как правило,

требуется организовать защиту от атак, как из внешней, так и из внутренней сети.

Для защиты от атак из внешней сети необходимы следующие функции безопасности:

- создание рубежа защиты по сетевому периметру;
- организация защищенного обмена информацией с внешними источниками;
- обнаружение и блокирование вторжений;
- обнаружение, блокирование распространения, уничтожение вредоносных программ.

Для защиты от атак изнутри требуется решать следующие задачи:

- устранение/уменьшение угроз, связанных с неправомочными действиями персонала, контрагентов, персонала внешних обслуживающих предприятий и прочих посетителей;
- выявление уязвимости и слабости программно-технических средств портала;
- сегментирование сети по уровням конфиденциальности, территориальному и функциональному признаку.

Данные функции в основном могут быть реализованы путем внедрения технологий Virtual Private Network- виртуальных частных сетей (VPN), межсетевого экрана на основе продуктов компаний Cisco, Check Point, обеспечивающих защиту сетевого периметра, создание и управление защищенными виртуальными сетями, сегментирование сетей по уровням безопасности, а также интеграцию систем антивирусной защиты, обнаружения вторжений и поиска уязвимостей.

В качестве базового варианта в состав функциональных подсистем СОБИ портала перечислим следующие подсистемы:

- управления безопасностью;
- идентификации и аутентификации;

Отформатировано: Положение: По горизонтали: справа, Относительно: поля
Отформатировано: Справа: 0,63 см
Удалено: атак
Удалено: -
Удалено: -
Удалено: -
Удалено: -
Удалено: -
Удалено: -
Удалено: -
Удалено: -

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: -

Отформатировано: Междустр.интервал: множитель 1,75 ин

Удалено: -

Удалено: -

Удалено: -

– управления доступом к информации;

– контроля целостности информации;

– регистрации и аудита;

– управления ключами и сертификатами.

Данные подсистемы охватывают как прикладной уровень, так и сетевой. Архитектурное решение СОБИ реализует эти подсистемы и интегрирует большинство из них в единое целое. Решаемую задачу можно сформулировать так: интеграция управления подсистем безопасности сетевого и прикладного уровня на базе общей политики безопасности, состоящей из совокупности формализованных правил доступа к сегментам сети, хостам, портам, сервисам, приложениям, правил аутентификации субъектов доступа, мониторинга состояния безопасности портала. Формализация и решение данной задачи может вывести на математические модели и методы, на новый интеллектуальный уровень всего направления.

Перейдем к решающей стадии - конструированию системы обеспечения безопасности, которая должна реализовать перечисленные выше функциональные подсистемы. В представленной на рисунке 1 архитектуре такой системы можно видеть комплекс средств защиты периметра, который можно создать на базе продуктов разных компаний. Отметим, что на данной схеме не показаны компоненты антивирусной защиты и обнаружения вторжений.

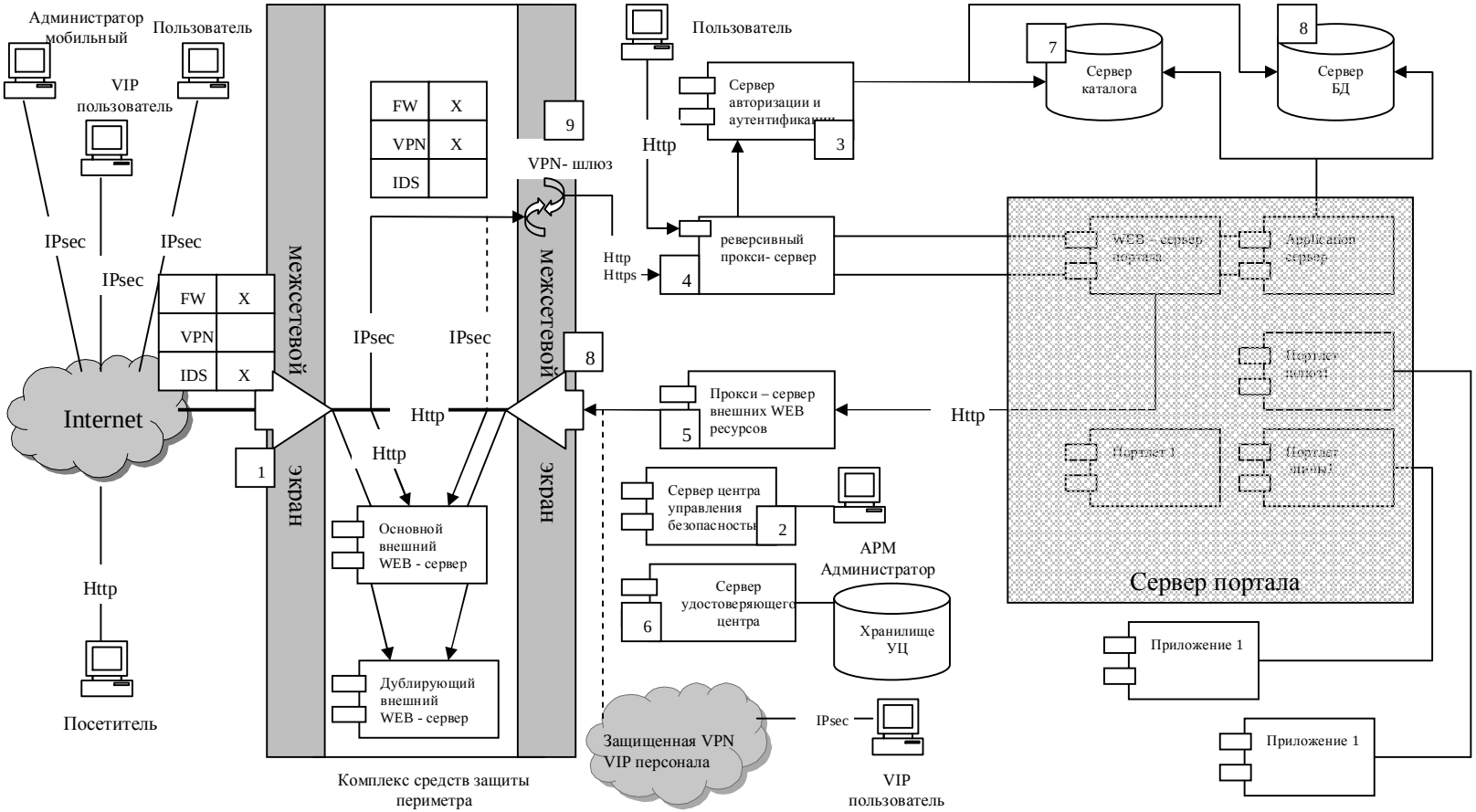

Рисунок 1. Архитектура программных компонентов СОБИ портала.

Удалено: ,

Следует подчеркнуть, что данная система контролирует доступ аутентифицированных (своих) пользователей и запрещает доступ посторонних в защищенную зону, лежащую справа. Система управления доступом построена на базе двух прокси-серверов, один из которых (реверсивный) разграничивает доступ зарегистрированных пользователей портала к его ресурсам, а второй (выходной) - доступ таких же пользователей в публичную сеть Интернет. Реверсивный прокси - сервер обеспечивает аутентификацию пользователей на основе сертификатов X.509 и PKI, а также механизм однократной регистрации. Прокси - серверы управляются сервером аутентификации и авторизации на основе ролей пользователей, связанных с корпоративной организационной структурой, и матрицы доступа, реализующей механизм ролевого доступа к ресурсам портала. Для посетителей портала (неавторизованных субъектов) доступен только Web-сервер, расположенный в неохраняемой зоне.

Удалено: .

Сервер управления безопасностью формирует общую политику безопасности в виде совокупности правил сетевого доступа к сегментам, хостам, портам, сервисам, и правил прокси-доступа к сервисам, портлетам-приложениям и статическим информационным ресурсам портала. Данная политика транслируется в локальные политики FW/VPN-агентов и прокси систем, а затем доставляется и исполняется на них.

Отсутствие выходного прокси-сервера в архитектуре портала объясняется тем, что в системе не ставилась задача защиты доступа к ресурсам среды Интернет, поскольку такой доступ из внутренней сети запрещен. Изменились и технологии защиты сетевого уровня - если раньше для формирования VPN использовался протокол SKIP (Simple Key management for Internet Protocol), то в настоящее время применяется протокол IP Security (IPSec). За прошедшие годы заметно усовершенствовались средства обнаружения вторжений, межсетевого

экранирования, определения уязвимостей и антивирусной защиты. На смену защищенным смарт-картам пришли более удобные защищенные USB-токены (ключи на основе USB флеш карт).

Какие программные продукты необходимы, чтобы реализовать все компоненты представленной архитектуры. Как видно из таблицы 1, все основные компоненты покрываются имеющимися на рынке продуктами известных компаний.

Таблица 1. Состав программных компонентов СОБИ портала

№ на рисунке	Компонент	Программные продукты
4	Реверсивный прокси - сервер	IBM WebSEAL/SunONE WebProxy/Microsoft ISA
5	Прокси - сервер внешних Web-ресурсов	Microsoft ISA/IBM WebSEAL/SunONE Web Proxy/
7	Сервер каталога	Microsoft AD/IBM Directory/SunONE DS
3	Сервер аутентификации и авторизации (АА)	ITIM+ITAM/SunONE IS/MS(Aspelle Everywhere) Dallas Lock ООО «Конфидент»
6	Сервер удостоверяющего центра	КриптоПро УЦ/RSA Keon
2	Сервер Центра управления безопасностью (ЦУБ)	Центр управления Застава
1	Межсетевой экран	PIX 5x5/FW-1
8	Межсетевой экран	PIX 5x5/FW-1
9	Шлюз VPN	Застава Офис

Остается только интегрировать отдельные продукты. Как показывает практика, затраты на интеграцию могут быть довольно велики, в сложных случаях они достигают 100-300% стоимости закупленных программно-технических средств. Еще раз отметим, что в состоянии наибольшей готовности для использования в качестве СОБИ портала находится пакет ITIM+ITAM компании IBM.

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Подводя итоги, сформулируем три основных преимущества рассмотренной архитектуры СОБИ портала.

– Решение может быть применено для широкого круга портальных систем и платформ.

Удалено: -

– Не требуется переработка кода портальных приложений.

Удалено: -

– Типовые протоколы сетевого уровня (IP/IPSec) и прикладного уровня (HTTP/HTTPS) улучшают интегрируемость средств защиты и реализуемость функций безопасности.

Удалено: -

Основное здесь то, что данное решение претендует на роль типового для разнообразных портальных систем, и что оно "разъемное", т. е. при интеграции с существующими порталами оно может быть встроено без переработки кода портальных приложений.

Сделаем следующий вывод. В данное время существует не мало продуктов Tivoli от IBM, Sun One от Sun Microsystems Dallas Lock ООО «Конфидент» и им подобных, но как показала практика единой системы решающей задачи комплексной защиты порталов и сайтов от несанкционированного доступа, не требующей переработки самого портала и легко интегрируемого на уже готовый портал просто нет. Создание подобного программного продукта стало просто первоочередной задачей, как для комплексной защиты самого портала, так и для массовой защиты других подобных объектов, которые могут быть подвержены несанкционированному доступу.

Удалено: м

Удалено: ,

Удалено: н

Отформатировано: Положение: По горизонтали: справа, Относительно: поля

Отформатировано: Справа: 0,63 см

Удалено: ¶ ¶ ¶ Л

Отформатировано: Шрифт: полужирный

Литература:

1. Крис Касперский Техника и философия хакерских атак – записки мыщ'а.- М.: Солон-Пресс 2005. – 272с.: ил. – (Серия Кодокопатель)

2. Столлингс Вильям. С81 Основы защиты сетей. Приложения и стандарты: Пер. с англ.. - М.: Издательский дом "Вильямс" 2002. - 432 с. :ил. – Парал. Тит. англ.

3. Жельников В. Криптография от папируса до компьютера, - М.: ABF 1997, ил 336 с.

4. Левин М. Л80 Руководство для Хакеров – Издание второе, дополненное и исправленное. – Москва, Оверлей - 2000. – 416 с.