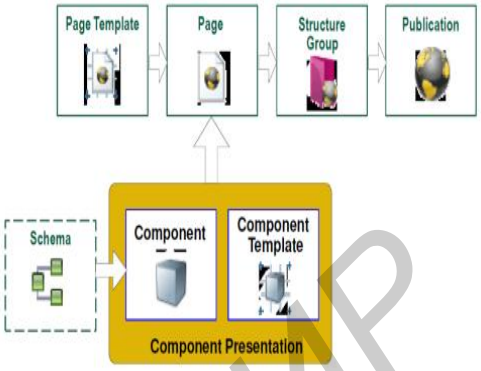
информация будет базироваться на одной из имеющихся схем, и сохранена в т.н. «компоненты», внешне похожие на файлы в папках.

Для того чтобы опубликовать страницу, потребуется также создать шаблон для самой страницы, а также шаблоны для схем. Для каждой схемы может быть создано неограниченное кол-во разных шаблонов в зависимости от потребностей. Это значит, что один раз создав компонент, основанный на определенной схеме, мы можем вставить его на разные страницы и применить разные шаблоны для того, чтобы представить на странице любую часть информации из этого компонента.



За счет четкого разделения информации и ее шаблонов, а также полного контроля за тем, что, когда и как будет публиковаться в «открытый» интернет, редактор получает свободу, которая редко встречается в других системах. Создание страницы похоже на собирание конструктора, где вы сами контролируете фигуру, которую хотите получить. Выходными форматами страниц или отдельных ее компонентов могут быть текст, HTML, XML, JS, CSS или даже бинарный код. Также важным преимуществом Tridion по сравнению с другими системами является то, что он не связан напрямую с сервером, на котором хранятся сгенерированные страницы вашего сайта, что позволяет использовать в них любое количество серверных языков — ASP, C#, Java или PHP, если сильно хочется. Для большинства из них есть написанные коннекторы, дающие доступ к объектной модели Tridion (COM+), а значит и ко всей опубликованной или не опубликованной информации.

Для простой рекомендуемой конфигурации Tridion требуется 4 отдельных сервера:

Один для самого Tridion.

Один для баз данных.

Один для копии сайта, называемой staging, т.е. предварительный просмотр.

Один для самого сайта в интернете.

Для оптимальной производительности к этому списку можно добавить 3-5 серверов:

Один для тестирования функциональных дополнений.

Один - два для публикации контента.

Один - два для распределения нагрузки между сайтами.

В завершении хотелось бы добавить, что Tridion выбрали такие компании как Kaspersky Lab, Honda, Toyota, Canon и более 600 других компаний по всему миру из совершенно разных сфер деятельности: производство, предоставление услуг, банки, туристические услуги, фармацевтика, образование, правительство, автоконцерны.

В докладе обсуждаются современное состояние и перспективы использования системы управления контентом сайтов SDL Tridion в Беларуси, указываются основные конкурирующие программные продукты, проводится сравнение SDL Tridion и конкурентов.

МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ РАБОТЫ ПРОТОКОЛА SHH

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Корнеев И. А.

Таболич Т. Г. – канд. техн. наук, доцент

Предлагаются мероприятия по повышению надёжности протокола для удаленного безопасного входа и других сетевых сервисов безопасности в недостаточно надежно защищенной сети. Мероприятия предлагается классифицировать по стоимости и длительности внедрения

В современных условиях из-за широкого распространения различных типов сетей большое распространение получили организация серверов (аппаратное обеспечение, выделенное и/или специализированное для выполнения на нём сервисного программного обеспечения). Сервера служат для большого диапазона задач: начиная от маршрутизации-фильтрации данных, заканчивая хранением активных приложений. В большинстве случаев физически сервер находится удаленно, и совершать над ним какие либо манипуляции крайне проблематично. Поэтому в большинстве серверов для решения данной проблемы используется протокол SSH (*Secure SHell*) [1]. **SSH** является протоколом для удаленного безопасного входа и других сетевых сервисов безопасности в недостаточно надежно защищенной сети. Он состоит из трёх компонентов. Первый компонент, протокол транспортного уровня (*SSH-TRANS*) обеспечивает аутентификацию сервера, конфиденциальность и целостность соединения. Второй компонент, протокол аутентификации пользователя (*SSH-USERAUTH*) аутентифицирует клиента для сервера. Он выполняется

поверх протокола транспортного уровня. Протокол соединения (*SSH-CONN*), мультиплексирует несколько логических каналов в один зашифрованный туннель. Этот компонент протокола SSH выполняется поверх протокола аутентификации пользователя.

Для аутентификации сервера в SSH-USERAUTH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA. Для аутентификации клиента также может использоваться ЭЦП RSA или DSA, но допускается также аутентификация при помощи пароля и даже ip-адреса хоста. Аутентификация по паролю наиболее распространена; она безопасна, так как пароль передаётся по зашифрованному виртуальному каналу. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают. Для создания общего секрета (сеансового ключа) используется алгоритм Диффи — Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью CRC32 в SSH1 или HMAC-SHA1/HMAC-MD5 в SSH2. Для сжатия шифруемых данных может использоваться алгоритм LempelZiv (LZ77), который обеспечивает такой же уровень сжатия, что и архиватор ZIP. Сжатие SSH включается лишь по запросу клиента, и на практике используется редко.

Для повышения надежности работы протокола можно принять несколько превентивных мер, заключающихся в проведении ряда организационно-технических мероприятий. К таким мероприятиям относятся:

Запрещение удалённого root-доступа (доступ в качестве администратора системы).

Запрещение подключения с пустым паролем или отключение входа по паролю.

Выбор нестандартного порта для SSH-сервера.

Использование длинных SSH2 RSA-ключей (2048 бит и более). Системы шифрования на основе RSA считаются надёжными, если длина ключа не менее 1024 бит.[6]

Ограничение списка IP-адресов, с которых разрешён доступ (например, настройкой файерволла).

Запрещение доступа с некоторых потенциально опасных адресов.

Отказ от использования распространённых или широко известных системных логинов для доступа по SSH.

Регулярный просмотр сообщений об ошибках аутентификации.

Установка систем обнаружения вторжений (IDS — Intrusion Detection System).

Использование ловушек, подделывающих SSH-сервис (honeypots).

При составлении плана организационно-технических мероприятий по повышению надёжности протокола SSH для конкретного предприятия все вышеперечисленные меры необходимо проанализировать, поскольку они резко отличаются друг от друга по величине капитальных затрат на их внедрение. Действительно, составление и внедрение инструкции или стандарта предприятия, предусматривающих «Отказ от использования распространённых или широко известных системных логинов для доступа по SSH» или «Регулярный просмотр сообщений об ошибках аутентификации», потребует мало денежных средств и времени, в то время как «Установка систем обнаружения вторжений» — это более дорогостоящее и длительное по срокам внедрения мероприятие.

Список использованных источников:

1. Корнеев И. А., Сечко Г.В., Таболич Т.Г. Постановка задачи разработки нового кроссплатформенного программного обеспечения (ПО) для работы с протоколом SSH // Современные средства связи: материалы XVII Междунар. науч.-техн. конф., 16–18 сент. 2012 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2012. – 332 с. – С. 199.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКИХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Королёв Я. П., Лысковец А. М., Масловская А. И.

Сечко Г. В. – канд. техн. наук, доцент

Для обеспечения информационной безопасности мобильных платежей предлагается начать в республике широкую стандартизацию при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт

Насколько нам известно, в настоящее время банки Беларуси только начинают внедрять приём мобильных платежей через интернет (почти во всех банках клиентам доступен SMS-банкинг). В то же время в России и на Украине этот вид услуг активно развивается. Например, санкт-петербургский банк ОАО АКБ «Балтика» внедрил первую в России России кастомизированную информационно-платежную систему на основе платежного сервиса MasterCard Mobile по модели White-lable при непосредственном участии MasterCard. Разработчиком и сервис-провайдером Baltica Mobile выступила группа компаний Intervale. Сервисом Baltica Mobile могут воспользоваться держатели карт MasterCard и Maestro, эмитированных ОАО АКБ «Балтика». Новый сервис предоставляет возможность оплачивать товары и услуги в режиме он-лайн на