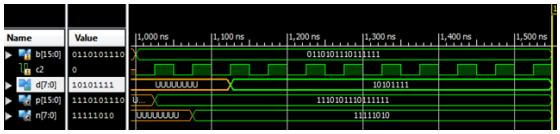

Рис. 2. Результат моделирования алгоритма сжатия по А-закону

Современные уровень развития технологий делает возможной и экономически оправданной реализацию различных методов обработки информации, применение их в технике связи, а именно в ЦСП и ЦЭАТС можно достаточно легко и быстро реконфигурировать структуру системы, а так же повышать производительность, что может удовлетворить требования к методам цифровой обработки сигналов.

Список литературы

1. Бернард Скляр Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.: ил. Парал. тит. англ.

2. Прокис Джон Цифровая связь. Пер. с англ. / Под ред. Д.Д. Кловского. М.: Радио и связь. 2000. 800 с.: ил.

3. Бабак В.П., Корченко А.Г., Тимошенко Н.П., Филоненко С.Ф. VHDL: Справочное пособие по основам языка. М.: Издательский дом «Додэка-XXI», 2008. 224 с.: ил. (Серия «Программируемы системы»).

WLAN СЕТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Бохан П.В.

Пензенский государственный технологический университет
Пенза, Россия, e-mail: los@pgta.ru

Сегодня всё шире распространяются локальные беспроводные сети (WLAN), использующие радиочастоты для передачи данных. Чаще их называют сетями Wi-Fi, хотя ранее это было наименование лишь одного из стандартов (802.11b).

Одно из основных преимуществ сетей WLAN, как следует из их названия, заключается в том, что они являются беспроводными. Это позволяет ускорить процесс создания сети и отказаться от использования кабелей. Кроме того, в отличие от сотовой связи, беспроводные сети Wi-Fi используют не лицензируемый (в большинстве стран) и, соответственно, бесплатный диапазон частот, а, следовательно, не требуют получения разрешения.

Стандарт IEEE 802.11 также предусматривает средства обеспечения безопасности. Сетям, в частности, присваивается уникальное имя, возможна фильтрация абонентов по MAC-адресам (физическим адресам устройств) и шифрование. При этом существуют два стандарта шифрования - Wired Equivalent Privacy (WEP) и Wi-Fi Protected Access (WPA). Первый, несмотря на то, что поддерживается всем сертифицированным оборудованием, имеет серьезные уязвимости и поэтому не обеспечивает должной защиты беспроводных каналов связи. Стандарт WPA считается намного более надежным. При этом сохраняется возможность одновременной работы в сети клиентов WPA и WEP, а также использующих другие, протоколы защиты. Часть старого оборудования можно модернизировать под WPA путем обновления микропрограммы («прошивки»).

Немаловажным достоинством сетей WLAN является возможность динамичной смены точек доступа. Современные устройства со встроенными контроллерами Wi-Fi начинают поиск нового хот-спота при ухудшении связи и автоматически переключаются на новую точку доступа. Это предоставляет пользователю возможность перемещаться, не отрываясь от работы.

Одной из основных проблем, характерных для сетей Wi-Fi, является, интерференция, то есть, пересечение зон приема от различных станций. По причине того, что передача сигнала ведется на свободной частоте, качество связи может значительно понижаться из-за помех от любительского радиооборудования и бытовых приборов, например, микроволновых печей. Кроме того, условия приема и передачи ухудшают стены, железобетонные перекрытия, металлические перегородки и пр.

Несмотря на появление стандарта безопасности WPA, на многих точках доступа применяется оборудование, совместимое исключительно с WEP. Такие потенциально уязвимые хот-споты теоретически могут представлять угрозу для пользователей, чья конфиденциальная информация может попасть в руки злоумышленников.

Нельзя не упомянуть проблему относительно высокого энергопотребления. Она особенно актуальна для владельцев ноутбуков и смартфонов, поскольку при активном использовании беспроводной связи существенно сокращается время работы портативных устройств от аккумуляторных батарей.

Наконец, к недостаткам WLAN можно отнести ограниченный радиус действия

Разработчики из Карлсруэвского Института Технологии (Германия) создали беспроводное Wi-Fi-соединение, передающее данные со скоростью более 40 Гб/сек на расстояние более 1,5 км. Этой скорости достаточно, к примеру, для того, чтобы за время меньшее секунды передать по сети обычный блюрей диск с фильмом. В оборудовании используется частота 240 ГГц вместо частотного диапазона от 2ГГц до 5 ГГц, используемого в обычных Wi-Fi устройствах. Переход на более высокие частоты решил проблемы и с дальностью передачи, а также размерами антенны. Необходимый размер антенны не превышает размеры самого чипа, отвечающего за передачу сигнала, и он не больше нескольких миллиметров.

Относительно новая функция, которая нашла широкое применение в как в офисной, так и в домашней цифровой технике, называется Wi-Fi Direct. Технология позволяет проводить беспроводное соединение между собой любых устройств, которыми поддерживается данная технология. Wi-Fi Direct – это возможность подключить к принимающему устройству, таких гаджетов, как камеры, принтеры, чтобы распечатать нужный файл, не используя провода. Те же возможности имеют игровые и любые сертифицированные мобильные устройства, в которых есть Wi-Fi адаптер.

В ближайшие годы развитие локальных беспроводных сетей пойдет по направлению массового внедрения так называемой технологии WiMAX (сокращенно от Worldwide Interoperability for Microwave Access). Сети WiMAX (стандарт IEEE 802.16a) предполагают использование частотного диапазона от 2 ГГц до 11 ГГц и обеспечивают скорость передачи данных до 70 Мбит/с на расстояние до 50 км. Новый стандарт позиционируется как средство подключения к интернету беспроводных локальных сетей WLAN и как замена DSL в качестве «последней мили». Пропускной способности одной базовой станции вполне хватит для обеспечения десятков бизнес-пользователей и сотен домашних подключений.

Список литературы

1. Беспроводные сети Wi-Fi / А.В. Пролетарский [и др.]. Интернет-университет информационных технологий, 2010.

2. Информационные основы средств вычислительной техники: учебное пособие / Е.В. Грачева [и др.]. Пензенская государственная технологическая академия, 2011.

3. Практика применения Wi-Fi – http://wi-life.ru/

4. Беспроводные технологии – http://wireless.ru/

5. Проектирование Wi-Fi сетей – http://www.getwifi.ru/

УЯЗВИМОСТЬ WEB-ПРИЛОЖЕНИЙ

Будников Е.А., Борисова С.Н.

Пензенский государственный технологический университет
Пенза, Россия, e-mail: romi_s@list.ru

При разработке приложений основные усилия разработчика обычно направлены на обеспечение требуемой функ-

циональности. При этом вопросам безопасности и качества программного кода уделяется недостаточно внимания. В результате подавляющее большинство веб-приложений содержит уязвимости различной степени критичности.

Простота протокола HTTP позволяет разрабатывать эффективные методы автоматического анализа веб-приложений и выявления в них уязвимостей. Это значительно упрощает работу нарушителя, позволяя ему обнаружить большое число уязвимых веб-сайтов, чтобы затем провести атаку на наиболее интересные из них.

Кроме того, уязвимости некоторых типов допускают не только автоматическое выявление, но и автоматическую эксплуатацию. Именно таким образом производится массовое внедрение в веб-ресурсы вредоносного кода, который затем используется для создания бот-сетей из рабочих станций обычных пользователей сети Интернет. Возможность использования веб-приложений в качестве платформы для атаки на рабочие места пользователей сама по себе делает эти приложения привлекательной целью для нарушителя.

Таким образом, при подготовке атаки на информационную инфраструктуру компании нарушители в первую очередь исследуют ее веб-приложения. Недооценка риска, который могут представлять уязвимости в веб-приложениях, доступные из сети Интернет, возможно, является основной причиной низкого уровня защищенности большинства из них.

OWASP (некоммерческой организации Open Web Application Security Project) после своего исследования представила список десяти наиболее опасных, но, в то же время, распространенных уязвимостей в программном обеспечении для интернета и веб-сервисах [1]. По мнению OWASP, на эти уязвимости стоит обратить самое пристальное внимание как государственным, так и коммерческим организациям, желающим обезопасить себя и своих клиентов от хакеров. Все указанные уязвимости достаточно широко распространены, а использовать их под силу даже малоквалифицированным хакерам, поскольку соответствующие средства взлома легко найти в сети Интернет.

1) Injection (всякого рода инъекции, в т.ч. SQL, LDAP и т.д.).

2) Cross Site Scripting (не потерявший актуальности XSS).

3) Broken Authentication and Session Management (ошибки в архитектуре аутентификации и управления сессиями).

4) Insecure Direct Object References (незащищенные ресурсы и объекты).

5) Cross Site Request Forgery (CSRF).

6) Security Misconfiguration (небезопасная конфигурация окружения, различных фреймворков, платформы).

7) Failure to Restrict URL Access (несанкционированный доступ к функционалу, требующему особых привилегий – например, обход проверки с помощью двойного «//» в URL для получения доступа к управлению блогом в WordPress).

8) Unvalidated Redirects and Forwards (открытые редиректы, которые ведут к фишингу, HTTP Response Splitting и XSS).

9) Insecure Cryptographic Storage (небезопасное хранение важных данных).

10) Insufficient Transport Layer Protection (недостаточная защита данных при их передаче на транспортном уровне, например по HTTP вместо HTTPS).

Опасность некоторых из указанных уязвимостей представлена ниже:

1) SQL-инъекции – встраивание вредоносного кода в запросы к базе данных – наиболее опасный вид атак [2]. С использованием SQL-инъекций злоумышленник может не только получить закрытую информацию из базы данных, но и, при определенных условиях, внести туда изменения. Уязвимость по отношению к SQL-инъекциям возникает из-за того, что пользовательская информация попадает в запрос к базе данных без должной обработке: чтобы скрипт не был уязвим, требуется убедиться, что все пользовательские данные попадают во все запросы к базе данных в экранированном виде.

2) PHP-инъекция (англ. PHP injection) – один из способов взлома веб-сайтов, работающих на PHP, заключающийся в выполнении постороннего кода на серверной стороне [3]. Потенциально опасными функциями являются: * eval(), * preg_replace() (с модификатором «e»), * require_once(), * include_once(), * include(), * require(), * create_function(). PHP-инъекция становится возможной, если входные параметры принимаются и используются без проверки.

3) Cross-Site Scripting – это вид уязвимости программного обеспечения (Web-приложений), при которой, на генерированной сервером странице, выполняются вредоносные скрипты, с целью атаки клиента. Сейчас XSS составляют около 15 % всех обнаруженных уязвимостей. Долгое время программисты не уделяли им должного внимания, считая их неопасными. Однако это мнение ошибочно: на странице или в HTTP-Cookie могут быть весьма уязвимые данные (например, идентификатор сессии администратора). На популярном сайте скрипт может устроить DoS-атаку.

4) CSRF (англ. Cross Site Request Forgery – «Подделка межсайтовых запросов», также известен как XSRF) – вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника).

Таким образом, уязвимости в Web-приложениях по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Проблема защищенности Web-приложений усугубляется еще и тем, что при разработке Web-приложений, зачастую не учитываются вопросы, связанные с защищенностью этих систем от внутренних и внешних угроз, либо не достаточно внимания уделяется данному процессу. Это в свою очередь порождает ситуацию, в которой проблемы ИБ попадают в поле зрения владельца системы уже после завершения проекта. А устранить уязвимости в уже созданном Web-приложении является более расходной статьей бюджета, чем при его разработке и внедрении.

Недооценка серьезности риска реализации угроз ИБ с использованием Web-приложений, доступных со стороны сети Интернет, возможно, является основным фактором текущего низкого состояния защищенности большинства из них.

Список литературы

1. Десять самых опасных уязвимостей в Web приложениях // http://www.securitylab.ru/news/212802.php.

2. SQL injection для начинающих. Часть1// http://habrahabr.ru/post/148151.

3. Основы php-инъекций для новичков // https://www.xaker.name/forvb/archive/index.php/t-13504.html

РАЗРАБОТКА И ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ С ВИРТУАЛИЗАЦИЕЙ

Валова О.О., Мартышкин А.И.

Пензенский государственный технологический университет, Пенза, Россия, e-mail: los@pgta.ru

Существующие в настоящее время математические модели вычислительных систем (ВС) не пригодны для исследования ВС с виртуализацией, из-за отсутствия