14. *Najgebauer A., Antkiewicz R., Chmielewski M., Kasprzyk R.* The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution // Journal of Telecommunications and Information Technologies. 2008. N 2. P. 14—20.
15. *Nazarova I. A.* Models and Methods for Solving the Problem of Network Vulnerability // Journal of Computer and Systems Sciences International. 2006. Vol. 45. № 4. P. 567—578.

А. А. Хейн, Б. А. Щукин

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ С ВЕБ-СЕРВИСОМ

В последнее время становится популярной покомпонентная сборка приложений на базе сервис-ориентированной архитектуры (SOA, Service-Oriented Architecture). Каждый такой компонент представляет собой сервис, являющийся модулем системы SOA. Использование данного подхода к программированию ИТ-инфраструктуры позволяет крупному предприятию получить преимущества при дальнейшем развитии.

Для эффективного контроля безопасности SOA-приложений должен быть установлен уровень требований к информационной безопасности (ИБ) составляющих сервисов, в частности веб-сервисов. ИБ — это состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних угроз, а также способность ИТ выполнять предписанные действия без нанесения ущерба субъектам информационных отношений. Так как SOA-приложения становятся все более популярны в бизнес-сообществе, консорциум W3C (World Wide Web Consortium) и OASIS (Organization for the Advancement of Structured Information Standards) прилагают значительные усилия для обеспечения гарантированного уровня их безопасности. Уровень требований устанавливается с помощью сертификатов (стандартов) безопасности. W3C и OASIS рекомендуют стандарты X.509, SPKI, XKMS, SSL/TLS, а также протоколы P3P и SAML в целях повышения информационной безопасности SOA-приложений.

Язык разметки подтверждения безопасности (SAML, Security Assertion Markup Language) (см. [1]) — основанный на языке XML стандарт, разработанный OASIS для обмена данными об аутентификации и авторизации между защищенными доменами, в рамках которых исполняются веб-сервисы. Стандарт SAML не зависит от платформы и состоит из утверждений, протоколов, привязок и профилей. Утверждения — это описания (высказывания) службы идентификации (identity authority) о конечном пользователе. Существуют три вида утверждений: авторизации, аутентификации и атрибута. Каждое в отдельности представляет собой набор общих элементов: предмет, условие и аутентификационное высказывание — и содержит информацию о типе сделанного запроса. Если запрашивается авторизация доступа к приложению, то утверждение SAML сообщает, разрешен ли пользователю вход в систему, и показывает набор его прав доступа. Если запрашивается аутентификация для сетевого ресурса или приложения, утверждение SAML указывает метод аутентификации, а также ее дату и время. В свою очередь, утверждения атрибута позволяют авторизовать пользователей для доступа к определенной информации на основании их статуса. В стандарте SAML хорошо то, что сервер управления идентификацией инкапсулирует, т. е. скрывает, реальные процессы авторизации и аутентификации, что позволяет сочетать решения безопасности от разных производителей. Одна из важных проблем, которую пытается решить SAML, — обеспечение сквозной аутентификации (технология единого входа, Single Sign On) при работе через браузер. Эта технология предполагает использование специального программного

решения, которое будет хранить пароли пользователя от всех приложений, требующих аутентификации, и автоматически вводить их, когда приложение того требует. Т. е. подобное решение замещает собой пользователя в процессе аутентификации. Доступ к хранимым паролям и настройкам происходит после аутентификации пользователя в подобной системе, совмещенной с аутентификацией в операционной системе: пользователь автоматически получает доступ ко всем системам, требующим аутентификации, введя однажды персональные данные аутентификации.

Спецификация XKMS (XML Key Management Specification) облегчает разработчикам создание безопасной связи между приложениями с помощью инфраструктуры открытых ключей (PKI). XKMS – это набор протоколов, разработанный W3C, который описывает распространение и регистрацию открытых ключей (Public Key), применимый для использования совместно со стандартом XML Signature (см. [3]), определенным W3C и IETF, в содружестве со стандартом XML Encryption (см. [4]). Эти протоколы не требуют отдельной инфраструктуры открытых ключей (такой, как X.509), но спроектированы так, чтобы быть совместимыми с такими инфраструктурами.

Веб-сервисы ослабляют безопасность, предоставляя посторонним лицам доступ к приложениям. Поэтому вопрос безопасности важен в плане контроля доступа к веб-сервисам. Для защиты взаимодействия с веб-сервисом на уровне сообщения и аутентификации применяется спецификация WS-Security (см. [2]), рекомендуемая консорциумом OASIS. Спецификация WS-Security описывает механизм безопасного обмена SOAP-сообщениями и обеспечивает следующую функциональность: целостность сообщения, пользовательскую аутентификацию и конфиденциальность. Используя спецификации XML Encryption и XML Signature, WS-Security определяет особенности безопасности в заголовке SOAP-сообщения.

В настоящее время в связи с быстрым распространением мобильных устройств стали весьма актуальны мобильные приложения, реализующие самые разнообразные функции. Рассмотрим приложение, предназначенное для координации действий сотрудников, выполняющих задания вне офиса. В исполнении каждого задания задействовано несколько сотрудников, последовательно решающих конкретные задачи. Для каждой задачи спланировано время начала работы, однако оно может быть скорректировано по факту ее реального выполнения. Предполагается, что сотрудники получают план работы на текущий день, не заезжая в офис, и сообщают в офис о начале работы по задаче, результатах работы и ее окончании.

Приложение предполагает интенсивный обмен сообщениями между офисом и сотрудниками, позволяющий оценить состояние исполнения каждого задания и выдать корректирующие распоряжения по задачам. Технически разработка сводится к построению приложения, которое состоит из веб-сервиса, выполняющего различные операции с базой данных, и мобильных клиентов, взаимодействующих с этим сервисом по GPRS. Очевидно, вопросы безопасности, хотя бы на элементарном уровне, должны быть решены.

Такое мобильное приложение было разработано с использованием технологии .NET (см. [5]). Оно связывает многочисленных мобильных клиентов с веб-сервисом, осуществляющим доступ к офисной базе данных. Следование стандартным подходам к обеспечению безопасности оказалось слишком сложным, поэтому для безопасного доступа к веб-сервису была реализована собственная процедура аутентификации. На листинге 1 показан формат SOAP-запроса, отправляемого мобильным клиентом к веб-сервису при вызове веб-метода. В заголовке SOAP-сообщения присутствуют учетные данные пользователя для доступа к веб-сервису (в настоящем примере примере номер мобильного телефона пользователя). Однако следует использовать защищенные каналы, например HTTPS (secure HTTP), потому что информация заголовка передается в виде открытого текста.

Листинг 1 Формат SOAP-запроса

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.
org/soap/envelope/">
<soap:Header>
<authenticationHeader xmlns="http://sc.bpc.ru">
<phoneNumber>string</phoneNumber>
</authenticationHeader>
</soap:Header>
<soap:Body>
<getInfo xmlns="http://sc.bpc.ru">
<jobID>int</jobID>
</getInfo>
</soap:Body>
</soap:Envelope>
```

При разработке веб-сервиса был реализован метод, который считывает идентификационную информацию запрашивающей стороны из этого SOAP-запроса и проверяет, разрешен ли этому пользователю вход в веб-сервис. Особенность данного решения в том, что этот метод не является веб-методом (т. е. он не декларирован в качестве операции WSDL) и, прежде всего, выполняет функцию аутентификации при вызове любого веб-метода данного веб-сервиса. Если запрашивающая сторона не зарегистрирована в базе офиса, то вызываемый веб-метод возвращает SOAP-ответ, содержащий сообщение о том, что доступ к веб-сервису запрещен, а в протокол нарушения правил доступа заносится запись о факте несанкционированного доступа. Формат данного сообщения представлен в листинге 2, а формат записи о факте несанкционированного доступа — в листинге 3.

Листинг 2 Формат сообщения, которое содержится в SOAP-ответе

```
<error>
<message>Invalid user access to this Web service</message>
<source>MobileWebService</source>
</error>
```

Листинг 3 Формат записи о факте несанкционированного доступа

```
<unauthorizedAccess>
<date>yyyymmdd</date>
<time>hhmmss</time>
<phoneNumber>string</phoneNumber>
</unauthorizedAccess>
```

К этому следует добавить, что все допустимые обращения к веб-сервису также протоколируются. Предлагаемое решение несложно в реализации, но, тем не менее, защищает систему от нежелательных обращений, так как недооценка возможных угроз, имеющихся при работе в открытом пространстве сети Интернет, может привести к нежелательным последствиям.

СПИСОК ЛИТЕРАТУРЫ:

1. Язык разметки подтверждения безопасности (SAML). URL: http://xml.coverpages.org/saml.html.
2. Безопасность Web-сервисов (WS-Security) рабочей группы OASIS. URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.
3. Подпись XML (XML Signature). URL: http://www.w3.org/TR/xmldsig-core/.
4. Шифрование XML (XML Encryption). URL: http://www.w3.org/TR/xmlenc-core/.
5. *Хейн А. А., Климов В. В.* Задача связи сервис-ориентированного приложения и мобильного устройства // VIII Курчатовская молодежная научная школа. Сборник докладов. М., 2011. Часть 3. С. 166–170.

Г. И. Хоруженко

АНАЛИЗ РЕДУЦИРОВАННОГО АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ PRINT-96 ЛИНЕЙНЫМ МЕТОДОМ И МЕТОДОМ СВЯЗАННЫХ КЛЮЧЕЙ

Алгоритм блочного шифрования PRINT предложен на конференции CHES 2010 в двух вариантах — PRINT-48 и PRINT-96 — в зависимости от размеров блока открытого текста и ключа шифрования [1]. При проектировании авторами алгоритма уделено особое внимание компактности и энергопотреблению его аппаратной реализации. К алгоритму PRINT-48 применены методы линейного и разностного анализа в работах [2–4]. Так, в работе [2] приведены классы слабых ключей алгоритма шифрования PRINT-48, для которых существуют линейные характеристики, позволяющие атаковать 28 раундов. В настоящей работе редуцированный 52-раундовый алгоритм PRINT-96 анализируется линейным методом, аналогичным методу, предложенному в работе [2]. Также предлагается атака на основе метода связанных ключей.

Приведем описание алгоритма шифрования PRINT-96. Пусть ключ шифрования имеет вид $k = \left(k^{(0)}, k^{(1)}\right)$, $k^{(0)} \in V_{96}$, $k^{(1)} \in V_2^{32}$. Пусть также заданы преобразования

$$\hat{s} = \left(\underbrace{s,\ldots,s}_{26}\right), s \in S\left(V_3\right),\ h : V_{96} \to V_{96},\ h\left(\left(\alpha_{95},\ldots,\alpha_0\right)\right) = \left(\alpha_{\sigma(95)},\ldots,\alpha_{\sigma(0)}\right),\ \sigma \in S_{96},$$

$$\hat{\pi}_{k^{(1)}} = \left(\pi_{k_{31}^{(1)}},\ldots,\pi_{k_0^{(1)}}\right),\ \pi_{k_i^{(1)}} \in S\left(V_3\right),\ i \in \{0,\ldots,32\}.$$

Таким образом, раундовая функция для j-го раунда имеет вид

$$g_k^{(j)}(\alpha) = \hat{s}\left(\hat{\pi}_{k^{(1)}}\left(h\left(\alpha \oplus k^{(0)}\right) \oplus c^{(j)}\right)\right),$$

где $c^{(j)} \in V_{96}$ — константа, зависящая от номера раунда.

При построении линейных характеристик используется следующее утверждение.

Утверждение 1. Для любого s-бокса $s \in S\left(V_3\right)$ существует такое преобразование ρ: {0,1,2,}→{0,1,2,}, что

$$\left|\left\{\alpha \in V_3 \mid \alpha_i = s\left(\alpha\right)_{\rho(i)}\right\}\right| \neq 2^2,\ i \in \{0,1,2\}.$$

Далее, при построении характеристик s-бокс будем представлять в виде системы координатных функций $f_i^{(s)} : V_3 \to \{0,1\}$, $i \in \{0,1,2\}$, причем $p\left\{f_i^{(s)}(\alpha) = \alpha_{\rho(i)}\right\} \neq \frac{1}{2}$, $i \in \{0,1,2\}$, α выбирается из множества V_3 случайно и равновероятно.

В работе под слабыми ключами относительно линейного анализа будем понимать ключи шифрования, для которых определенные биты ключа $k^{(1)}$ являются фиксированными. Для получения классов слабых ключей максимальной мощности будем рассматривать характеристики, повторяющиеся при шифровании с определенным периодом $t < 32$.