Моделюючий комплекс допускає можливість виключення або модифікації одного або декількох примітивів, які беруть участь в утворенні гам.
Ключові слова: криптографічні примітиви, поточні шифри, програмно-моделюючий комплекс.

PROGRAM-MODELING COMPLEX BPC ALGORITHM STREAM ENCRYPTION AND NOISELESS CODING VIDEO SIGNALS UAV

Stream BPC (Block Packet Cipher) algorithm is oriented to cryptographic protection and noiseless coding discrete video transmitted from the board of rolling the aircraft to the ground. Encryption is done bitwise addition modulo 2 blocks of the source text, the size of which form the 128, 256, 512 or 1024 bits, with equal length blocks of binary pseudo-random numbers (keys or gammas). Flows of gamma synchronously generated both on board and on the ground, produced a set of cryptographic transformations (primitives) secret base public key is loaded on the stage of pre-service and in ground equipment onboard encryption. Noiseless coding blocks encrypted video by one of the three algorithms: Hamming, BCH or Reed-Solomon. A plurality of blocks of data, the number of which is proportional to the size range of forms packet encrypted information. Forming a transition to the next packet is preceded by conversion of the public encryption key, which in turn controls the parameters of the key block (XOR function). Modeling complex is subject to exclusion or modification of one or more primitives involved in the formation of ciphering schemes.
Keywords: cryptographic primitives, stream ciphers, software-modeling complex.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net
Білецький Анатолій Якович, доктор технічних наук, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, Doctor of Science, Professor of Department Electronics of National Aviation University.

Максименко Артем Владимирович, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: maxisery@gmail.com
Максименко Артем Володимирович, бакалавр, кафедра електроніки Національного авіаційного університету.
Maksymenko Artem, Bachelor, Department of Electronics of National Aviation University.

Навроцкий Денис Александрович, аспирант кафедры электроники Национального авиационного университета.
E-mail: sg6336@yandex.ua
Навроцький Денис Олександрович, аспірант кафедри електроніки Національного авіаційного університету.
Navrotskyi Denys, Postgraduate student of Department Electronics of National Aviation University.

Свердлова Анастасия Дмитриевна, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: miss.bookmark@yandex.ua
Свердлова Анастасія Дмитрівна. Бакалавр, кафедра електроніки Національного авіаційного університету.
Sverdlova Anstasia, Bachelor, Department of Electronics of National Aviation University.

Семенюк Александр Иванович, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: sovist9@mail.ru
Семенюк Олександр Іванович, бакалавр, кафедра електроніки Національного авіаційного університету.
Semenjuk Alexander, Bachelor, Department Electronics of National Aviation University.

УДК 004.056.52

ADFS АУТЕНТИФИКАЦИЯ В ИНФРАСТРУКТУРЕ ОБЛАЧНЫХ СЕРВИСОВ

Владимир Демчинский

В настоящее время применение облачных вычислений приобретает все большее значение. Основная особенность облачных вычислений — предоставление услуг удаленно, в требуемом объеме и в требуемое время, с гибкой системой управления. Однако, использование облачных вычислений порождает новые угрозы информационной безопасности, а также требует переосмысления традиционных угроз для сетевой инфраструктуры. Одна из ключевых задач безопасности – аутентификация - также требует нового подхода. В статье рассмотрены вопросы обеспечения безопасности облачной инфраструктуры и, в частности, использование служб федераций Active Directory для аутентификации.
Ключевые слова: *службы федераций Active Directory, аутентификация, облачные вычисления.*

Вступление. Тема данной статьи – особенности использования и защиты облачных инфраструктур и, в частности, применение ADFS (Active Directory Federation Services – службы федераций Active Directory) для задач аутентификации. Цель работы: презентация результатов исследования и внедрения технологии ADFS. В работе сформулированы атаки, специфичные для данной службы, а также освещены некоторые практические аспекты внедрения ADFS.

Согласно определению NIST [2] «Облачные вычисления – это модель предоставления удобного сетевого доступа в режиме «по требованию» к коллективно используемому набору настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ данных, приложений и/или сервисов), которые пользователь может оперативно задействовать под свои задачи и высвобождать при сведении к минимуму числа взаимодействий с поставщиком услуги или собственных управленческих усилий.” Основные характеристики облачных вычислений: самообслуживание по требованию, широкая доступность через сеть, объединение ресурсов в пул, способность к быстрой адаптации и измеримость услуг. Преимущества использования облачных сервисов – оптимизация издержек, гибкая масштабируемость, избыточность и надежность (отказоустойчивость, восстанавливаемость), доступность, простота доступа, совместная работа и непрерывность бизнес-процессов, упрощенное управление и автоматизированная подготовка.

Модели обслуживания и проблемы безопасности облаков. Основные модели обслуживания, предоставляемые облачными провайдерами [4]: программное обеспечение как услуга (Software as a service, SaaS), платформа как услуга (Platform as a service, PaaS) и инфраструктура как услуга (Infrastructure as a service, IaaS). Применяемая модель обслуживания существенно оказывает влияние на процесс защиты. Например, в контексте модели SaaS можно четко продумать интерфейс взаимодействия клиент – облако и таким образом упростить процесс контроля над взаимодействиями. Или же модели IaaS, обеспечивающей наибольшую свободу реализации, соответственно возрастает сложность механизмов защиты.

Обеспечение безопасности облачных сервисов требует пересмотра средств защиты, применяемых в традиционной IT-инфраструктуре. Например, для облачных сервисов следует переосмыслить такие риски, как смешение данных и вторичное их использование, атаки на гипервизор и атаки в пределах хоста, а также риски, вызванные юридическими отличиями в законодательствах различных стран. В целом, для облачных инфраструктур следует переосмыслить проблему управления ресурсами облака, которая может включать, например, такие факторы, как политика доступа, выделение ресурсов и качество обслуживания, балансировка нагрузки и оптимизация энергопотребления. Поэтому, развитие технологий облачных вычислений сопровождается появлением новых подходов к обеспечению аутентификации, управления доступом, криптографической защиты, контроля сетевого трафика и т.д.

Исследуем одно решение проблемы аутентификации в облачных инфраструктурах и интеграции системы аутентификации в домене Active Directory с авторизацией в облачных сервисах. ADFS – служба безопасной распределенной аутентификации и обмена идентифицирующей информацией между организациями – партнерами [3]. В технических терминах – служба аутентификации между доменами Active Directorty без установления традиционных доверительных отношений между доменами или лесами доменов. Типичный сценарий использования ADFS позволяет проводить автоматическую аутентификацию пользователей приложениями, поддерживающими утверждения (claims). В частности, ADFS может обеспечивать единую Web-аутентификацию (SSO – Single Sign On) для клиентов из других доверенных административных областей. Службы федераций впервые появились в Windows Server 2003 R2 по названием Geneva Server, а в Windows Server 2012 были значительно переработаны и улучшены.

Сценарий применения ADFS. Рассмотрим такой сценарий взаимодействия. Последовательность шагов процедуры аутентификации показана на рисунке.

Субъектам организации A (Account Partner, Домен пользователей) требуется предоставить доступ к Web-приложениям организации B (Resource Partner, Ресурсный домен). При первом запросе клиента к Web-приложению (1) он будет перенаправлен Web-агентом посредством HTTP-Redirect к ADFS сервису ресурсного домена (2), где ему будет предложено указать свою принадлежность к тому или иному учетному домену (данная фаза работы протокола называется Home Realm Discovery). Если публикация списка орга-

низаций – партнеров по той или иной причине не желательна, то идентификатор организации может быть включен в строку URL. ADFS сервер B изначально не имеет данных относительно субъектов различных учетных доменов, но имеет так называемое «доверие федерации» с ADFS серверами соответствующих доменов.

Затем субъект будет перенаправлен к ADFS сервису A (3), где он будет аутентифицирован (явно или неявно) в соответствии с используемой технологией (интегрированная аутентификация Active Directory, Web-форма, сертификат, смарт-карта и т.д.) Сервер федерации маршрутизирует запрос проверки подлинности в соответствующий каталог учетного домена для генерации токена защиты субъекта, запрашивающего доступ. Сервер федерации A запрашивает утверждения во внутреннем хранилище данных аутентификации учетного домена (4). Затем сервер конструирует токен защиты ADFS, содержащий идентификатор субъекта и права доступа в виде набора утверждений (атрибутов), заверенный цифровой подписью ADFS сервера.

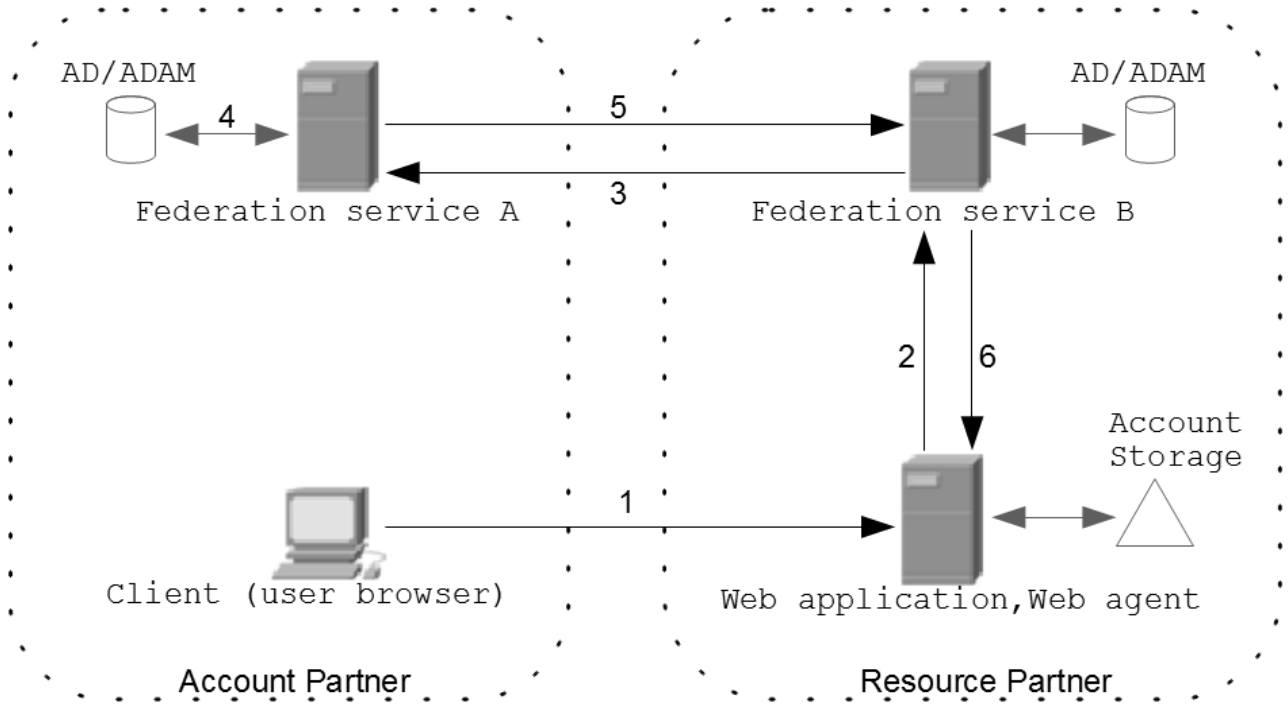

Рис. Процедура аутентификации в службе ADFS

Согласно настроенной в домене A политике доступа, клиент получит от ADFS сервиса A подписанный токен защиты, содержащий набор утверждений, предназначенных для B. Утверждение содержит информацию относительно определенных свойств клиента (например, идентификатор, имя, ключ, группа, свойства, привилегии и т.д.), содержание которых согласовано между сервисами федераций двух сторон. Можно заметить, что ответственность за аутентификацию внутренних субъектов возлагается на свой домен. После этого клиент снова будет перенаправлен к ADFS сервису B (5), который проверит цифровую подпись ADFS сервиса A в токене защиты, содержащем набором утверждений.

Утверждения токена защиты проверяются в соответствии с установленной политикой доверия, фильтруются и отображаются (mapping) в утверждения, имеющие локальное значение (т.е. понятные Web-приложению). В случае использования Active Directory в учетном домене, утверждения соответствуют группам AD. Полученный у B набор утверждений также имеет вид токена защиты, подписанного цифровой подписью ADFS сервиса B. Носителем токена защиты является HTTP-Cookie в браузере клиента. После этого клиент наконец будет перенаправлен (6) к Web-приложению (по URL-адресу исходного запроса), которое (с помощью агента) проверит цифровую подпись локального токена, идентифицирует клиента и примет решение относительно его авторизации. Локальный токен может быть подписан цифровой подписью, соответствующей сертификату ADFS сервиса B или иметь вид сеансового ключа Kerberos.

При последующих попытках доступа произойдет прозрачная авторизация через ADFS-Cookie. Web-агент Web-сервера обращается к браузеру клиента и запрашивает ADFS-cookie, подтверждающие подлинность клиента. Файл ADFS-Cookie содержит цифровую подпись содержащихся в нем утверждений, но не зашифрован. Однако, весь обмен данными защищается протоколом SSL/TLS. После закрытия сеанса файл ADFS cookie уничтожается. По умолчанию срок действия Cookie истекает через 10 часов.

Заметим, что в архитектуре ADFS каждый партнер самостоятельно управляет учетными записями своей организации, а клиенты, с целью получения доступа к внешним приложениям, проходят проверку аутентичности в своей сети. ADFS сервис учетного домена использует локальное хранилище учетных записей для аутентификации пользователей и получения данных с целью формирования заявок. В ADFS хранилищем учетных записей может быть либо Active Directory, либо Active Directory Application Mode (ADAM), либо AD LDS (Active Directory Lightweight Directory Service). Для взаимодействия с хранилищем учетных записей используется протокол LDAP.

В процессе настройки ADFS организации формируют партнерские отношения. Должны быть установлены доверительные отношения (обмен сертификатами) между партнерскими службами федераций. Сервер Web-приложения должен установить начальные доверительные отношения с локальным сервисом федераций (обмен сертификатами). Кроме того, поскольку передача токенов защищена SSL, стороны должны обладать доверенными сертификатами аутентификации SSL соединений. Масштабируемость внедрения ADFS требует использования общего корневого центра сертификатов всеми участниками. Возможны также сценарии с мультифакторной аутентификацией, в которых агент получает токены защиты от нескольких служб ADFS и объединяет утверждения из нескольких источников в один токен для сервера приложений.

Архитектура ADFS. ADFS – это реализация WS-Federation passive requestor profile (WS-F PRP) protocol от Microsoft [3] (спецификация из архитектуры WS-* веб-сервисов, обеспечивающая совместимость продуктов разных вендоров – стандартный протокол получения пассивными клиентами доступа к серверам приложений через службы федераций). Для совместимости с ADFS приложение должно быть federation-aware (соответствовать спецификации WS-F PRP, и, в частности, иметь Web-агент). Web-приложение должно уметь обрабатывать утверждения в токенах защиты (использовать библиотеку аутентификации ADFS). Утверждения (метаданные в виде символьных строк) должны быть понятны каждой из сторон и отображаться в локальную политику доверия. Однако, стороны сохраняют свободу в семантическом содержании утверждений. Утверждения в токенах защиты представляются в формате SAML (Security Assertion Markup Language). SAML это XML стандарт для обмена сведениями об идентификационных данных между системами аутентификации. SAML-токен может содержать несколько утверждений относительно природы клиента. Требование к клиентскому браузеру – поддержка механизмов Java-script и Cookie.

В протоколе WS-Federation определены три вида утверждений (identity, group, custom):

1. Идентификационные атрибуты:

– имя пользователя (UPN – User Principal Name, например user@realm) – обязательный атрибут;

– почтовый адрес (user@email.com);

– обобщенное имя (произвольная строка).

2. Группа или роль (boolean) (пользователь может принадлежать к нескольким группам).

3. Утверждения произвольного вида (атрибуты имя/значение).

Особенности внедрения и атаки на ADFS. Следует отметить особенности внедрения [1] служб федераций. Прежде всего, традиционная модель внедрения ADFS предполагает, что клиент в учетном домене и сервер в ресурсном домене ограждены от внешних сетей фильтрующими сетевыми экранами. Однако архитектура ADFS предусматривает для этого роли Proxy-агента и Web-агента, которые инспектируют трафик, проходящий через периметр сети и устраняют необходимость в дополнительных открытых портах на брандмауэрах. Корректная работа ADFS служб все же требует синхронизации времени в пределах 5 минут (иначе же отметки времени в маркерах станут недействительными). Для этого вполне подходит традиционный протокол NTP.

Один из векторов атаки на ADFS – похищение SAML-токена и его использование. Этому препятствует протокол SSL/TLS, защищающий сеансы связи между клиентским браузером и службами ADFS. Более того, каждый ADFS-

Cookie помечен Secure bit, который есть сигналом браузеру передавать его только посредством HTTPS. Произвольной модификации токена препятствует механизм цифровой подписи. Однако, похищение Cookie все же возможно через приложение, имеющее XSS уязвимость. Еще одним важным свойством ADFS является возможная анонимность перед Resource Partner т.е. взаимодействие может быть настроено таким образом, чтобы вся уникальная, идентифицирующая пользователя информация не выходила за пределы учетного домена.

Выводы. Таким образом, преимущества использования ADFS – в упрощении управления учетными записями (нет необходимости дублировать учетные записи, каждый партнер использует собственные хранилища), возможности установлении доверия и предоставлении полномочий на уровне организаций и отделении аутентификации от авторизации. Однако, каждый партнер должен установить доверительные «отношения федерации» с другими партнерами и установить в своей сети хотя бы один ADFS сервер. В целом же использование ADFS способствует масштабируемости, гибкости и совместимости облачных решений, поддержке доступа с портативных устройств и, в целом, улучшению управляемости облачными службами и безопасности облаков!

ЛИТЕРАТУРА

[1]. Dan Holme, Nelson Ruest, Danielle Ruest, and Jason Kellington.MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server® 2008 Active Directory® (2nd Edition)/ Microsoft Press, 2011.- 1040 p. ISBN-10:0-7356-5193-0, ISBN-13:978-0-7356-5193-7.

[2]. Peter M. Mell, Timothy Grance. «The NIST Definition of Cloud Computing.» Techincal Report SP 800-145. National Institute of Standards & Technology, Gaithersburg, MD, United States 2011

[3]. Active Directory Federation Services (ADFS) / TechNet Library [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/en-us/ library/cc736690(v=ws.10).aspx

[4]. Cloud computing / Wikipedia, the free Encyclopedia [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Cloud_computing.

REFERENCES

[1]. Dan Holme, Nelson Ruest, Danielle Ruest, and Jason Kellington.MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server® 2008 Active Directory® (2nd Edition)/ Microsoft Press, 2011.- 1040 p. ISBN-10:0-7356-5193-0, ISBN-13:978-0-7356-5193-7.

[2]. Peter M. Mell, Timothy Grance. «The NIST Definition of Cloud Computing.» Techincal Report SP 800-145. National Institute of Standards & Technology, Gaithersburg, MD, United States 2011.

[3]. Active Directory Federation Services (ADFS) / TechNet Library [Online]. – Available from: http://technet.microsoft.com/en-us/library/ cc736690(v=ws.10).aspx.

[4]. Cloud computing / Wikipedia, the free Encyclopedia [Online]. - Available from: http://en.wikipedia.org /wiki/Cloud_computing.

ADFS АВТЕНТИФИКАЦІЯ В ІНФРАСТРУКТУРІ ХМАРНИХ СЕРВІСІВ

В наш час застосування хмарних обчислень набуває все більшого значення. Головна особливість хмарних обчислень – надання послуг віддалено, в необхідному обсязі та в необхідний час, з гнучкою системою керування. Однак, використання хмарних обчислень породжує нові загрози інформаційної безпеки, а також вимагає переосмислення традиційних загроз для мережної інфраструктури. Одне з ключових завдань безпеки – автентифікація також вимагає нового підходу. У статті розглянуті питання забезпечення безпеки хмарної інфраструктури і, зокрема, використання служб федерацій Active Directory для автентифікації.

Ключові слова: служби федерацій Active Directory, автентифікація, хмарні обчислення.

ADFS AUTHENTICATION SERVICES FOR CLOUD INFRASTRUCTURE

Currently the use of cloud computing is becoming increasingly important. The main feature of cloud computing - providing services remotely, to the extent needed and in the required time, a flexible control system. However, the use of cloud computing poses new threats to information security, but also requires a rethinking of the traditional threats to network infrastructure. One of the key tasks of security - authentication also requires a new approach. The article discusses the security of cloud infrastructure and, in particular, the use of Active Directory Federation Services for authentication.

Keywords: Active Directory Federation Services, authentication, cloud computing.

Демчинський Володимир Васильович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».

E-mail: vvd@bigmir.net

Демчинский Владимир Васильевич, кандидат технических наук, доцент Физико – технического института НТУУ «КПИ».

Demchinskyy Volodymyr, Ph.D., Associate Professor of Physics and Technology Institute at NTU «KPI».