УДК 621.3

АУТЕНТИФИКАЦИЯ В РАСПРЕДЕЛЕННЫХ ГЕТЕРОГЕННЫХ СИСТЕМАХ С ДИНАМИЧЕСКОЙ АРХИТЕКТУРОЙ

Алексеев Н.А., Мазанка Р.М.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: alexeyev@its.kpi.ua, roman.mazanka@outlook.com

Authentication methods in distributed heterogeneous systems with dynamic architecture

With increasing amounts of data processing large amounts of information is becoming more difficult. The traditional way to solve this problem is to build dedicated high-performance distributed environments. Since the transmitted data must be protected against theft and distortion, the choice of authentication method that could effectively be used must be made. In this paper, the aim is to carry out an analytical review of the existing authentication methods.

С увеличением количества данных и ростом технического прогресса проблема обработки большого количества информации становится все более критичной. Традиционным, достаточно затратным способом решения данной проблемы является построение специализированных высокопроизводительных распределенных сред, таких как грид-системы или вычислительные кластеры. Одним из подходов к снижению материальных затрат при построении таких сред является использование неотчуждаемых некластеризованных распределенных вычислительных ресурсов, значительную долю которых составляют персональные устройства пользователей, подключенные посредством беспроводной сети. Поскольку передаваемые таким образом данные должны быть надежно защищены от кражи и искажения, выбор метода аутентификации, который мог бы эффективно использоваться при построении таких распределенных гетерогенных системах с динамической архитектурой является актуальной задачей. В данной работе ставится цель провести аналитический обзор существующих методов аутентификации с целью дальнейшего использования при построении систем такого рода, грид-систем персональных компьютеров (далее – ГСПК).

Рассмотрим самые распространенные методы аутентификации, которые поддерживаются большинством устройств, используемых в ГСПК: WEB-аутентификация, Media Access Control (MAC) filtering, Wired Equivalent Privacy (WEP), WPA2-PSK и 802.1x.

Wired Equivalent Privacy (WEP) – метод аутентификации, при котором один и тот же ключ (пароль) должен ввести каждый клиент сети. Поскольку сеть, использующая данный метод может быть легко скомпрометирована [http://arstechnica.com/gadgets/2007/04/new-attack-cracks-wep-in-record-time/], метод считается устаревшим и его использование не рекомендуется.

Еще один метод, который используется для защиты сетей – это Media Access Control (MAC) filtering – фильтрация по MAC адресу устройства. Достоинством этого метода является то, что точка доступа подключает лишь клиентов с известными ей

MAC адресами. Данный метод аутентификации может быть эффективен в малых сетях при использовании совместно с WEP. Но такой подход имеет существенный недостаток: MAC адрес может быть изменен пользователем, и тогда злоумышленник может перехватывать пакеты настоящего пользователя, или же совершать противоправные действия от его имени.

При использовании WEB-аутентификации во время подключения к беспроводной точке доступа у клиента запускается браузер и он попадает на страницу входа, где должен ввести свои учетные данные. При попытке перейти на другую страницу без прохождения процедуры аутентификации система автоматически перенаправляет пользователя на страницу входа. Такая система часто используется в публичных местах для уведомления пользователя об условиях предоставления услуг.

Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK) – это режим аутентификации, который предполагает ввод пароля каждым из клиентов, которые желают подключиться к сети. [http://www.juniper.net/techpubs/en_US/network-director1.1/topics/concept/wireless-wpa-psk-authentication.html] Данный метод является хорошим решением для домашней сети, но в корпоративной – его использование нежелательно, так как зная пароль, злоумышленник может перехватить передаваемый пакет и расшифровать данные. Другая сложность применения данного стандарта в корпоративной сети – невозможность централизованного администрирования беспроводного доступа: при необходимости администратор вынужден сменить пароль на каждой точке доступа, после чего каждый пользователь должен будет ввести его на своем устройстве. Необходимость смены пароля возникает довольно часто – при уходе сотрудника из компании, при краже или взломе устройства.

802.1x (также известна как Wi-Fi Protected Access 2 Enterprise (WPA2-Enterprise)) – протокол, который работает на основе портов. При подключении пользователя если авторизация прошла успешно, клиенту открывается виртуальный порт.

Таблица 1. Сравнение методов аутентификации.

Метод аутентификации	*WEP*	*Mac filtering*	*WEB-аутентификация*	*WPA2-PSK*	*802.1x*
Использование разных ключей для каждого пользователя / наличие фильтрации по адресу клиента	-	-	+	-	+
Простота администрирования	-	+	-	-	+
Отсутствие необходимости вмешательства пользователя при повторных подключениях	+	+	-	+	+
Обоснованность использования в корпоративном сегменте	-	-	-	-	+
Доступ к сети только для авторизированных пользователей	+	+	-	+	+
Сумма	2	3	1	2	5

Для анализа рассматриваемых методов приведем сравнительную таблицу 1. Проанализировав данную таблицу можем сделать вывод, что для корпоративной сети необходимо использовать технологию 802.1x. При подключении пользователя к беспроводной точке доступа, последняя отправляет EAP-Request – запрос на аутентификацию, клиентское устройство посылает EAP-Response – ответ, который перенаправляется на RADIUS сервер. RADIUS сервер отправляет пакет-запрос аутентификатору (коим является точка доступа), которая в свою очередь переупаковывает его в EAPOL и отправляет клиенту (в различных схемах количество таких сообщений может изменяться), клиент отвечает на запрос, ответ поступает на аутентификатор и перенаправляется на RADIUS сервер. В случае правильного ответа RADIUS сервер дает команду аутентификатору открыть порт.[http://citforum.ru/nets/articles/authentication/].

Таким образом, можно выделить следующие преимущества использования стандарта 802.1x:

- контроль на уровне сети (запрет доступа неавторизованным пользователям);
- может быть использован для проводных и беспроводных сетей;
- дает возможность разделять пользователей по VLAN-ам;
- динамическая смена ключей;
- невозможность перехвата трафика;
- IEEE 802.1x позволяет использовать несколько методов аутентификации – имя/пароль, сертификаты, tokens и т.д.

Во время тестового внедрении метода 802.1x в информационно-телекоммуникационную инфраструктуру Института телекоммуникационных систем НТУУ «КПИ» он подтвердил свою эффективность для использования в корпоративной среде и планируется для внедрения на постоянной основе.

Проанализировав различные методы аутентификации можно сделать вывод, что для построения гетерогенной системы с динамической архитектурой целесообразнее всего использовать стандарт 802.1x, так как он обеспечивает необходимую безопасность и дает возможность централизованно управлять подключением к распределенной системе.

Литература

1. Ars Technica. New attack cracks WEP in record – [Электронный ресурс] – Режим доступа: http://arstechnica.com/gadgets/2007/04/new-attack-cracks-wep-in-record-time– Электрон. текстовые данные (дата обращения: 26.03.2016).
2. Guniper Networks. Understanding WPA-PSK and WPA2-PSK Authentication – [Электронный ресурс] – Режим доступа: http://www.juniper.net/techpubs/en_US/network-director1.1/topics/concept/wireless-wpa-psk-authentication.html - Электрон. текстовые данные (дата обращения: 26.03.2016).
3. Сетевая аутентификация на практике – [Электронный ресурс] – Режим доступа: http://citforum.ru/nets/articles/authentication/ – Электрон. текстовые данные (дата обращения: 26.03.2016).