УДК 004.056
Р. Леськів, Ю. Сметанка
Тернопільський національний технічний університет імені Івана Пулюя

РОЛЬ АУТЕНТИФІКАЦІЇ У РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

UDC 004.056
R. Leskiv, Yu. Smetanka
(Ternopil Ivan Pului National Technical University, Ukraine)

AUTENTIFICATION ROLE IN DISTRIBUTED COMPUTER SYSTEMS

Питання авторизованого доступу до обчислювальних ресурсів є актуальним як для локальних комп'ютерів, так і для мереж та хмарних сервісів. Дати відповідь на запитання, а чи є наш партнер в поточній сесії зв'язку в розподіленій системі саме тим, за кого він себе видає, ми можемо лише шляхом узгодження з ним спільної політики безпеки.

Щоб рішення на основі довіри працювало, ми повинні бути повністю впевнені, що надіслані дані можуть бути перевірені нашими партнерами як такі, що справді надходять від нас, а також ми повинні бути впевнені, що дані, які приходять до нас, дійсно були створені нашими партнерами. Це задача автентифікації. Зазвичай для аутентифікації використовується пароль та/або приватний ключ.

Паролі, як правило, корисні, якщо існує велика кількість сторін, яким потрібно автентифікувати себе конкретній іншій стороні. Публічні ключі, як правило, корисні, якщо є одна сторона, якій потрібно автентифікувати себе величезній кількості партій.

За допомогою пароля аутентифікація надає докази того, що хтось знає пароль. Якщо потрібно точно знати, хто це (що зазвичай важливо), тільки аутентифікація з залученням третьої сторони може надати таку інформацію. З відкритим ключем багато сторін можуть знати ключ, але тільки одна сторона, яка знає відповідний приватний ключ, може підтвердити автентифікацію самої себе. Тому ми схильні використовувати обидва механізми, але для різних випадків. Коли веб-сайт автентифікує у себе користувачеві, це робиться за допомогою криптографії. Поширюючи один відкритий ключ (для величезної кількості користувачів), веб-сайт може бути автентифікований усіма його користувачами.

Як практично ми використовуємо кожен з цих механізмів аутентифікації в розподіленій системі? Потрібно буде зашифрувати транспортування пароля через мережу. Шифрування пароля вимагатиме від нас мати або спільний симетричний ключ, або відкритий ключ нашого партнера.

Надання паролів з використанням третьої сторони реалізує сервер автентифікації Kerberos. На сьогодні Kerberos є одним з найстаріших протоколів автентифікації, що використовуються на сьогоднішній день [1]. До цього протоколу є багато розширень та доповнень як загального характеру, так і спеціальних. Цей протокол не базується на HTTP на відміну від багатьох інших протоколів автентифікації. Завдяки цьому дані, що передаються мережею, зовсім непридатні для читання людиною без застосування додаткових інструментів. Протокол з моменту створення зазнав немало доповнень та модифікацій, але з середини 80-х років минулого століття змін не зазнавав [2].

Література

1. The Kerberos Network Authentication Service (V5). [Електронний ресурс] . – Режим доступу: https://tools.ietf.org/html/rfc4120
2. Kerberos Protocol Tutorial. [Електронний ресурс] – Режим доступу: http://www.kerberos.org/software/tutorial.html