УДК 681.3:658

Рощенко Ю. В.

ЗАСТОСУВАННЯ ЗАСОБІВ ДЕЦЕНТРАЛІЗОВАНОЇ АВТЕНТИФІКАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОЇ ОСВІТИ

Досліджено сучасні тенденції у системах авторизації та єдиного входу, виділено системи, придатні для створення міжорганізаційних об'єднань електронної освіти. Розглянуто, зокрема, сучасні децентралізовані системи, включаючи Shibboleth, OpenID і Windows CardSpaces, та їх сумісність із популярними веб-базованими системами електронної освіти, такими як ILIAS, Moodle, elgg and BlackBoard.

Кожна система електронної освіти, взята окремо від інших, призначена для надання своїм користувачам певного спектра послуг. Розглянуті в сукупності, ці системи віддалені одна від одної географічно та топологічно в мережі, здатні взаємодіяти якщо не беспосредньо, то через своїх користувачів, які зазвичай користуються послугами не однієї системи. При цьому виникає як здорова конкуренція систем, так і зайве дублювання ресурсів і зусиль.

Пов'язані спільними цілями й організаційними рамками, системи електронної освіти могли б об'єднуватися у спільних проектах або міжорганізаційних ініціативах, що мають на меті надавати створення єдиного інформаційного простору освітніх послуг. Єдиний інформаційний простір потребує узгодження зусиль і, врешті, одночасних прав доступу одному користувачеві одразу до кількох систем. Виникає необхідність надавати певній групі осіб доступ до багатьох систем відразу. Необхідність автентифікації всіх користувачів із такої групи кожною із систем окремо становить серйозне обмеження з точки зору адміністрування, безпеки та організації даних для сучасного світу електронних послуг.

До недавнього часу проблема ідентифікації користувачів відразу в багатьох системах вирішувалась досить великою кількістю специфічних, немасштабованих і порівняно складних у підтримці засобів, заснованих на традиційній моделі безпеки (ISO7498-2 - документ 1989 р.) [1].

За потреби надання одному користувачеві доступу до кількох систем відразу частіше практикують такі підходи [2]:

• Користувач створює однакові ідентифікатори та паролі в усіх системах. Недоліки: складність усунення суперечностей, недостатній захист інформації, незахищеність від зловживань. Адміністратор однієї системи може спробувати використати інформацію, до якої має доступ, для доступу до іншої системи. Також однакові ідентифікатори в різних системах можуть бути створені різними особами. Недоліком є значна надлишковість даних, зокрема ідентифікаторів користувачів та паролів.

. Обмеження доступу користувача за його IP адресою. Недоліки: недостатня гнучкість. Користувач не зможе працювати в системі з іншої адреси.

• Proxy-сервери та доступ за VPN. Недоліки: додаткова незручність для користувачів, зменшена швидкість роботи.

. Використання однієї спільної БД про користувачів. Недоліки: погана безпека та погана масштабованість, несумісність форматів.

• Централізована автентифікація за допомогою серверів Kerberos та LDAP Недоліки: потрібно мати постійно діючий центральний сервер з усією інформацією про користувачів. Системам-учасникам слід мати домовленості про спільний доступ та «прив'язані» до центрального сервісу автентифікації.

Ефективне вирішення завдання ідентифікації користувачів багатьма системами вимагає зміни парадигми в побудові інфраструктури безпеки мережних застосувань, у порівнянні з традиційною. Автори [3] виділяють такі основні вимоги до сучасних засобів автентифікації та авторизації:

• В управлінні доступом системи обмінюються як можна меншою кількістю ідентифікаційної інформації.

• Ідентифікаційна інформація має не стільки ідентифікувати користувача, скільки бути достатньою для прийняття рішення про надання користувачеві доступу до певного ресурсу.

. Коли той, хто надає послуги, має інформацію про те, до якої організації належить користувач,

постачальник може зробити запит до спеціальної служби організації користувача, щоб автентифікувати його.

. Після автентифікації постачальник може визначити, базуючись на інформації про роль користувача, чи має користувач доступ до ресурсу.

Розподілені мережні застосування та веб-сервіси з розподіленими ресурсами вимагають нової архітектури безпеки, в основі якої лежить семантичний ідентифікаційний об'єкт - документ, повідомлення, завдання, пов'язані з суб'єктом або іншим застосуванням, що ініціювало об'єкт. Ідентифікаційний об'єкт при цьому може переміщуватися між багатьма серверами, сервісами та адміністративними доменами. Фактично, це системи децентралізованої ідентифікації.

Важливою рисою нової архітектури безпеки є поділ функцій автентифікації та авторизації шляхом використання інфраструктури керування правами, заснований на політиках, і керування доступом на основі ролей (Policy/Role Based Access Control (RBAC) і Privilege Management Infrastructure (PMI)), відомої також, як PKI, стандартом X.509, а також ISO 10181-3 Access Control Framework [1].

Елементами такої архітектури є:

• сервіс / функція аутентифікації (Auth);

. функція контролю доступу (Access Enforcement Function (AEF) або Policy Enforcement Point (PEP));

. функція ухвалення рішення про доступ (Access Decision Function (ADF) або Policy Decision (PDP));

. політика доступу (Access Control Information (ACI) або Policy).

Розглянемо кілька найпоширеніших архітектур організації спільного доступу до інформаційних ресурсів.

Архітектура AAA. Архітектуру автентифікації, авторизації та обліку (AAA - Authentication, Authorisation, Accounting), описану групою стандартів IETF RFC 2902-2906, в основному орієнтовано на мобільні мережні застосування. Запропонована архітектура визначає базовий протокол AAA і включає:

• розподілені AAA-сервери;

. AAA-менеджери ресурсів (ASM - Application Specific Module);

• модулі політики (RP - Policy and event Repository);

. центри посвідчення (CA - Certification Authority), що утворюють адміністративні домени.

Така архітектура може працювати в багатодоменному середовищі, однак складність її практичного застосування, крім мобільного зв'язку, ускладнюється необхідністю інтегрального AAA-протоколу, у той час як архітектура безпеки веб-сервісів вимагає роздільних функцій автентифікації та авторизації, які відповідно мають належати до суб'єкта та ресурсу (автентифікації користувача і авторизації його прав на ресурс).

PERMIS (Privilege and Role Management Infrastructure Standards validation). PERMIS, побудований виходячи з базової концепції поділу функцій автентифікації та авторизації, використовує архітектуру авторизації на підставі політики та ролей, які визначаються X.509 Attribute Certificate (AC). Основні риси системи:

• може працювати з будь-якими системами автентифікації (наприклад, ім'я / пароль, сертифікат відкритого ключа X.509, Kerberos та ін);

• на підставі ідентифікатора суб'єкта, цільового ресурсу / сервісу і запитуваної дії видає висновок відповідно до прийнятої політики доступу до ресурсу;

. політика доступу визначається відносно ролей, які можуть задаватися атрибутами користувача, обумовленими AC;

. політика описана у форматі XML, близькому до XACML (eXtensible Access Control Markup Language).

SPOCP (Simple Policy Control Protocol). SPOCP приймає рішення про авторизації доступу на підставі запиту від своїх клієнтів, використовуючи таку інформацію:

• надавану користувачем або клієнтом (рівень автентифікації та роль або атрибути);

. запитувану з директорій або інших служб ідентифікації (ідентифікатор користувача і його атрибути або ролі).

SPOCP використовує вирази LISP для опису політики доступу і формування рішення про доступ. SPOCP використовує спрощений у порівнянні з SAML [6] та XACML протокол і формат повідомлень, однак може «говорити» й за допомогою SAML.

WebISO. Система WebISO розроблена з метою дати можливість користувачам зі стандартним браузером здійснювати доступ до розподілених сервісів, включаючи веб-сервери, використовуючи звичайну центральну службу аутентифікації (як правило, за допомогою імені / пароля).

A-Select. A-Select пропонує службу аутентифікації для веб-застосувань, що відносяться до одного адміністративного або довірчого домену. Подальший розвиток системи та використання SAML дозволять здійснювати міждоменну аутентифікацію й надавати послуги аутентифікації іншим системам.

PAPI (Point of Access to Provider of Information) використовує локальну аутентифікацію користувача для формування авторизаційного маркеру (token), що передається користувачеві як cookie. PAPI є досить простою системою, але її подальший розвиток на основі використання SAML дозволить їй успішно інтегруватися з іншими системами.

Shibboleth. Можливо, найамбітнішим із open-source проектів новітніх систем управління доступом є Shibboleth [4]. Це проект комітету Middleware Architecture Committee for Education, під егідою якого створюється Internet 2. Покликання Shibboleth у цій мережі нового покоління – побудова інфраструктури роботи з обліковими записами користувачів мережі.

Shibboleth забезпечує авторизацію, засновану на атрибутах користувача, і використовує SAML [6] як формат декларацій Auth / Auth і протоколу. Особливістю Shibboleth є покращена конфіденційність користувача: дані про користувача зберігаються тільки в його рідній організації, і процедура авторизації запитує тільки мінімальний набір даних, необхідних для прийняття рішення; у такий спосіб Shibboleth має можливість використати зовнішні сервіси автентифікації. Федерована ідентифікація дає змогу обмінюватись інформацією про користувачів у рамках одного адміністративного домену, а також надавати частину інформації іншим організаціям у федерації.

Це уможливлює міждоменний вхід користувачів та видаляє потребу підтримувати окремі логіни та паролі.

Windows CardSpace. Windows CardSpace – порівняно нова децентралізована система єдиного входу від Microsoft. Для здійснення входу до деякої системи CardSpace дозволяє використовувати цифрове посвідчення з набору посвідчень, що збережені попередньо користувачем на локальній робочій станції. Ідентифікація за допомогою Windows CardSpace дає змогу обійтись без централізованої системи, яка створювала би й перевіряла посвідчення.

OpenID. OpenID – децентралізована відкрита система єдиного входу, що дає змогу використовувати один логін та пароль на великій кількості сайтів. На сайтах, що підтримують OpenID, користувачам не доводиться реєструватися й запам'ятовувати дані для кожного сайту. Замість цього їм достатньо бути зареєстрованими на сайті провайдера ідентифікації OpenID. Оскільки технологія OpenID децентралізована, то будь-який сайт може використовувати ПЗ OpenID у якості засобу для входу; OpenID вирішує проблему без використання централізованого сайту для підтвердження особи користувача – натомість будь-який сайт може виступати як ідентифікатор. OpenID прийшла зі світу блогів (таких, як livejournal.com) та підтримується значною кількістю ресурсів (наприклад, Livejournal-URL блог можна використовувати як OpenID-ідентифікатор).

Перевагами OpenID є простота (у порівнянні з Shibboleth) та відкритість (у порівнянні з Windows CardSpaces).

Засоби децентралізованої аутентифікації у системах електронної освіти

Найпоширенішими нині є такі засоби децентралізованої автентифікації: OpenID, Shibboleth та Windows CardSpace.

З власного дослідження відкритих Moodle, ILIAS 3, elgg та комерційної BlackBoard, що є одними з найпопулярніших сьогодні, можна побудувати таку таблицю сумісності.

Таблиця. **Сумісність систем**

	OpenID	**Shibboleth**	**CardSpace**
Moodle	Підтримує як модуль з версії 1.8	Підтримує	–
ILIAS 3	–	Підтримує	–
Elgg	Підтримує	–	–
BlackBoard (комерційна)	–	–	–

Динаміку зміни популярності технологій можна спостерігати за Google Trends – засобом, що дає змогу відстежувати частоти пошуку різних ключових слів у Google та наявність цих слів у новинах (рис.).

Як випливає, Shibboleth виник і користувався попитом у пошуковій системі раніше за всіх, CardSpace – пізніше за всіх, а OpenID користується найбільшою популярністю саме нині.

Висновок. На найближчий час найперспективнішою системою для використання в системах електронної освіти є OpenID – вона комбінує простоту в реалізації, відкритість та достатньо потужні можливості. Вона вже підтримується такими системами як Moodle, elgg та ще багатьма іншими ресурсами. Вона вже відома серед користувачів популярних ресурсів, таких як livejournal.

Саме OpenID можна рекомендувати для створення міжуніверситетських федерацій та спільного доступу до ресурсів як у рамках одного університету, так і між університетськими системами електронного навчання.

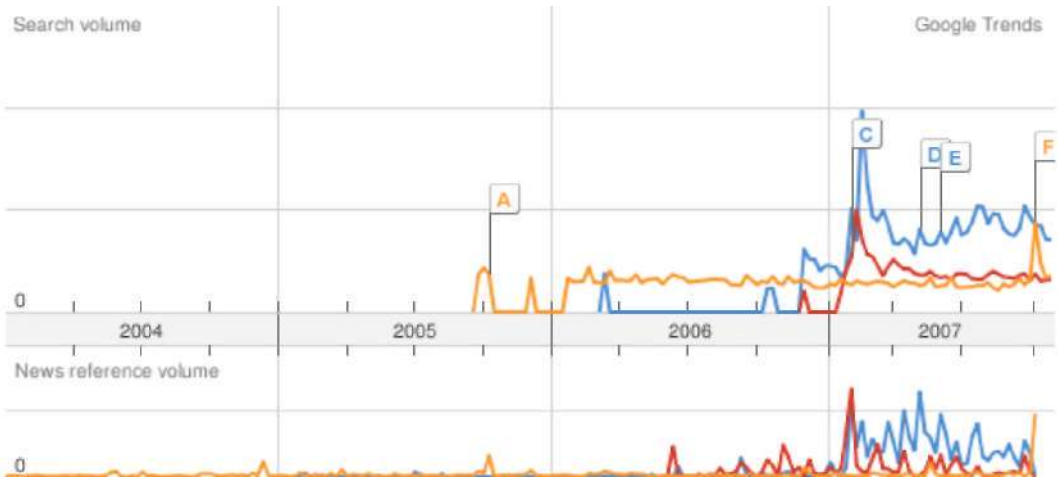

Рис. Частота пошуку ключових слів: A, F – Shibboleth, D, E – OpenID, C – Cardspace

1. *Демченко Ю.* Архитектура сервисов аутентификации и авторизации и сетевая идентификация в Интернет.– http://staff.science.uva.nl/~demch/papers/relarn2003-ydemchenko-aa-identity.html
2. Shibboleth Update.– http://shibboleth.internet2.edu/
3. *Brantley P.* "Shibboleth & Privacy".– Presentation Director of Technology, California Digital Library University of California, Office of the President, September 2005.– http\\seminar.deff.dk/presentations/brantey2.ppt
4. Shibboleth Technical Overview.– http://shibboleth.internet2.edu/shib-tech-intro.html
5. *Маквитти Л.* Говоря на языке SAML.– http://www.ccc.ru/magazine/depot/04_02/read.html?0501.htm.
6. OASIS Standards and Other Approved Works: SAML 1.1 specification.– http://www.oasis-open.org/specs/index.php# samlv1.1
7. http://www.openid.org.
8. OpenID Plugin for Moodle.– http://moodle.org/mod/data/view.php?d=13&rid=928

Y. Roshchenko

DECENTRALIZED AUTHENTICATION METHODS IN E-LEARNING SYSTEMS

The paper describes recent trends in single sign-on frameworks for web-based systems, which are able to serve as a base for multi-homed, federated e-learning efforts. Several decentralized frameworks, including Shibboleth, OpenID and Windows CardSpaces are selected and analyzed against modern web-based e-learning systems, including popular ILIAS, Moodle, elgg and BlackBoard systems.