УДК 004.738.5

А. С. ОГАРКОВ, Е. Г. ВАСЕЦЬКИЙ, Г. Л. МОРОЗОВ, С. В. КУХЛІВСЬКИЙ (ДІІТ)

ПРИМУСОВА АВТОРИЗАЦІЯ В МЕРЕЖІ ІНТЕРНЕТ

У статті висунуто перспективну ідею рішення все більш актуального питання ідентифікації особи в мережі Інтернет. Зростаюча популярність Інтернету несе з собою проблему анонімності людини в мережі. Стаття пропонує упровадити новий спосіб ідентифікації, який при всій своїй строгості уточнення інформації за паспортними і біометричними даними людини, є досить демократичним і надає користувачеві можливість самому вирішувати, як розпоряджатися цією інформацією.

Ключові слова: Інтернет, авторизація, ідентифікація

В статье выдвинута перспективная идея решения все более актуального вопроса идентификации личности в сети Интернет. Растущая популярность Интернета несет с собой проблему анонимности человека в сети. Статья предлагает внедрить новый способ идентификации, который при всей своей строгости уточнения информации по паспортным и биометрическим данным человека, является достаточно демократичным и предоставляет пользователю возможность самому решать, как распоряжаться этой информацией.

Ключевые слова: Интернет, авторизация, идентификация

The article describes a promising idea of solving more and more pressing problem of personality authentication in the Internet. Growing popularity of the Internet carries with itself the problem of man anonymity in a network. The article suggests inculcating a new identification method, which at all strictness of information clarification from passport and biometric data of a man, is democratic enough and gives possibility for user to decide how to dispose this information.

Keywords: Internet, authentification, identification

Вступ

Інтернет за останні декілька років став невід'ємною частиною життя суспільства. Із зростанням його розповсюдження феномен анонімності джерела інформації став представляти серйозну проблему. Адже будь-яка інформація, яку користувач передає в мережу, не контролюється і її достовірність лежить на совісті самого користувача. Тільки окремі ресурси із строго обмеженим колом відвідувачів можуть дозволити собі проводити реальний контроль достовірності.

Як показала практика, найбільш поширені способи контролю доступу виявляються безсилими проти достатньо досвідчених користувачів, які легко знаходять методи обходу подібних систем. Більш того, існують спеціальні послуги, що допомагають користувачам одурювати такі засоби контролю і відвідувати ресурси, закриті для їх доступу.

ІСНУЮЧІ СПОСОБИ

Існуючі способи ідентифікації користувача в основному засновані на реєстрації клієнта з прив'язкою до нього деякого ідентифікатора. Він варіюється від прапорця на призначеній для користувача стороні до значення, складно побудованого за певними ознаками клієнта, на стороні ресурсу (далі сервера).

Всі способи можна умовно розділити на три групи: з прив'язкою до комп'ютера, з прив'язкою до одного облікового запису і з прив'язкою до користувача.

Припустимо, що на сервері знаходиться якась служба, яка проводить опит. Для того, щоб один і той же відвідувач не голосував кілька разів, серверу необхідно якимсь чином його запам'ятати.

Перший спосіб – «Cookies». Він відноситься до категорії прив'язки до комп'ютера і є реєстрацією якоїсь змінної на стороні клієнта. Ідентифікатор цієї змінної прив'язується до сервера, а її значення указує на те, що даний клієнт проголосував в конкретному опиті. Коли ж користувач зробить спробу повторного голосування в тому ж опиті, сервер перевірить значення цієї змінної і, якщо воно указує на цей опит, відбудеться відмова в голосуванні.

Недолік такого способу в тому, що користувач у будь-який момент може видалити всі Cookies за допомогою браузера (програма-клієнт) або здійснити повторне голосування через інший браузер, який не має доступу до зареєстрованих раніше змінних Cookies [1].

Другий спосіб – ідентифікація IP клієнта. Він заснований на визначенні адреси клієнта в

мережі (IP). Він також відноситься до категорії прив'язки до комп'ютера. Під час обробки голосування сервером, визначається IP клієнта. Якщо клієнт ще не голосував в даному опиті, сервер записує його IP в базу даних, як той, що проголосував. При повторній спробі голосування тим же клієнтом, сервер визначає, що з його IP голос був врахований і відмовляє користувачеві.

На жаль, у даного способу є свої серйозні недоліки. По-перше, клієнт може змінити свій IP через анонімні проксі-сервера. Це дає можливість обходити системи, засновані на обмеженні доступу через ідентифікацію IP. По-друге, зараз досить поширені локальні мережі, які об'єднують в собі безліч клієнтів, що мають один зовнішній IP на всіх. При цьому якщо один клієнт вже проголосував в подібному опиті, сервер не дасть іншим клієнтам з цієї мережі пройти голосування, оскільки у них така ж IP-адреса, що і у того, що проголосував.

Третій спосіб – «Супербан». Він заснований на визначенні коду, складеного по унікальних особливостях комп'ютера, через який користувач здійснює доступ. Є найнадійнішим способом, що відноситься до категорії прив'язки до комп'ютера.

Після того, як клієнт вперше проголосував в опиті, який використовує даний метод ідентифікації, сервер за допомогою певних засобів на клієнтові визначає унікальні властивості комп'ютера клієнта (MAC-адреса мережевої карти, параметри монітора і т.д.) і складає якусь послідовність за отриманими даними. Далі, ця послідовність записується в базу даних сервера і вже при спробі повторного голосування з даного комп'ютера користувачеві буде відмовлено.

Ця система вважається найбільш надійною, але навіть її можна обійти шляхом зміни параметрів системи комп'ютера (наприклад, змінити параметри монітора).

Четвертий спосіб – «Open ID» та аналогічні їй системи. Він відноситься до категорії прив'язки до одного облікового запису, заснований на використанні єдиного облікового запису. Розглянемо його принцип дії.

Користувач, що виявив бажання реєструватися на конкретному ресурсі, часто зобов'язаний заповнити цілий ряд полів, таких як логін, пароль, E-mail, деяку особисту інформацію. При цьому для кожного нового ресурсу він зобов'язаний вводити всю цю інформацію наново. Ресурс, який використовує систему Open ID або подібну до неї, пропонує користувачеві ввести тільки свій OPENID, який є ідентифікатором, отриманим користувачем при реєстрації в самій системі Open ID. Поля облікового запису, який був заведений користувачем у момент реєстрації в системі авторизації, пізніше будуть представлені ресурсу, таким чином, користувачеві можна буде не вводити наново всі ці значення.

Після введення OPENID, яке містить в собі ім'я користувача і посилання на провайдера ідентифікації, користувач потрапляє на сторінку провайдера, де повідомляє йому, чи довіряє він даному сайту. Якщо користувач довіряє, то провайдер надасть інформацію про нього ресурсу і перенаправить користувача назад на ресурс. В осоружному ж випадку, перенаправлення все одно відбудеться, але ресурсу буде відмовлено в наданні значень.

Варто відзначити, що необов'язковою опцією є створення деякого секретного ключа, узгодженого між провайдером ідентифікації і сервісом. Якщо з боку користувача відбудеться спроба зламати систему і він спробує обдурити її шляхом відвідування підробної сторінки провайдера, ресурс звірить цей секретний ключ з ключем, заздалегідь узгодженим з провайдером ідентифікації, який повинен був видати користувачеві повноваження використовувати його інформацію. Якщо ключ не відповідає, користувачеві буде відмовлено в доступі [3].

На прикладі з голосуванням, уніфікація користувачів проводитиметься по OPENID ідентифікатору. Але при цьому користувач може завести собі декілька облікових записів.

Перевага цієї системи полягає в тому, що вона дозволяє користувачеві завести один обліковий запис і більше не утрудняти себе в її повторному введенні для кожного ресурсу окремо.

Шостий спосіб – реєстрація з явкою клієнта. Він відноситься до категорії прив'язки до користувача, виконує реєстрацію клієнтів через спеціальні відділи реєстрації, які враховують їх в спеціальній базі даних. Цей спосіб дозволяє уникнути повторної реєстрації при голосуванні на виборах через Інтернет або для привласнення випускникам, що беруть участь в єдиному тестуванні, індивідуального коду. Особливість цієї системи в тому, що цей код видається по документах, підтверджуючих особу людини.

Недоліком цього способу є те, що він недостатньо поширений серед систем реєстрації користувачів в Інтернет і він може не врахувати той факт, що в деяких країнах дозволено подвійне громадянство і одна і та ж людина може мати декілька паспортів і, відповідно, може реєструватися кілька разів.

Висновок. Для способів прив'язки до комп'ютера характерний один недолік: користувач, що має певні навики, легко зможе обійти систему ідентифікації, помінявши комп'ютер, як

точку входу в мережу Інтернет. Але вони можуть стати хорошою основою для інших способів.

У способів прив'язки до одного облікового запису також є свій недолік: будь-який користувач може завести собі необмежене число облікових записів. Але при цьому такі способи дуже зручні для користувача, оскільки дозволяють ввести інформацію про себе тільки один раз, указуючи ресурсам тільки ім'я свого облікового запису, якщо ці ресурси підтримують таку систему ідентифікації.

Способи реєстрації з прив'язкою до користувача найнадійніші, оскільки не дозволяють одній людині завести декілька облікових записів. Але при цьому вони обмежені межами окремих організацій або країн і не адаптовані для масштабної роботи в мережі Інтернет.

ВИМОГИ ДО СИСТЕМИ

У зв'язку із зростанням числа користувачів Інтернету виникла необхідність створення нової системи ідентифікації користувачів Інтернет-ресурсами, яка матиме надійну прив'язку до користувача і вимагатиме від нього введення достовірної інформації про себе. При цьому система повинна бути універсальною, безпечною, зручною і простою для користування і, що важливо для новаторських систем, не повинна вимагати значних змін у вже існуючій інфраструктурі мережі Інтернет.

При створенні нової системи ідентифікації слідує, до всього іншого, врахувати, що не всі користувачі захочуть, щоб інформація, яка може вказати на них, була доступна кому-небудь в Інтернет. Якщо ввести примусову авторизацію для доступу до кожного ресурсу в мережі, неминучі конфлікти і протести з боку користувачів.

Тому система також повинна бути прозорою для користувача, гарантувати йому конфіденційність і можливість повного управління наданою інформацією. На ранніх же стадіях впровадження вона не повинна вимагати своєї участі в процесі ідентифікації користувачів кожним ресурсом мережі Інтернет, таким чином, надаючи їм право вибору, адже існують сайти, що не потребують точної інформації про користувачів.

ОПИС ЗАПРОПОНОВАНОГО СПОСОБУ

Автори пропонують новий варіант ідентифікації користувачів в мережі Інтернет, вільний від недоліків існуючих способів ідентифікації.

Суть його полягає в наступному.

Враховуючи всі правила, пропонується створити спеціальну web-службу, яка об'єднає в собі всі переваги вищеописаних способів і виключить деякі їх недоліки.

Запропонована служба візьме від систем прив'язки до єдиного облікового запису одноразову реєстрацію, яка дозволить користувачеві отримати щось на зразок паспорта в Інтернеті, який міститиме в собі всю необхідну інформацію про користувача для кожного ресурсу.

Від систем прив'язки до користувача служба візьме уніфікацію кожного користувача за його паспортними даними. При цьому, виходячи з того, що паспортні дані можуть в деякій мірі співпадати або ж можуть розрізнятися стандарти складання паспорта в різних державах, пропонується також ввести уніфікацію користувача по його деякій біометричній ознаці.

Пропонована служба складатиметься з авторизованих відділів реєстрації клієнтів, серверів авторизації, а також із служби технічного контролю.

Відділ реєстрації є відведеним приміщенням, доступним для відвідування користувачами, обладнаним одним або більш (залежно від навантаження на відділ) комп'ютером (з доступом в Інтернет і спеціальними пристроями для реєстрації користувачів) і що має штат - навчений персонал, який обслуговуватиме клієнтів.

Сервера авторизації повинні складатися з єдиної бази даних клієнтів, серверної системи обслуговування і реєстрації клієнтів і системи, за допомогою якої здійснюватиметься контроль роботи серверів службою технічного контролю.

З приводу бази даних варто відзначити, що крім різних службових таблиць, вона повинна містити ще чотири таблиці.

Перша таблиця містить обов'язкову інформацію про користувача, яку вводять безпосередньо під час його реєстрації.

Друга таблиця містить необов'язкову інформацію, яку користувач може ввести і змінити у будь-який час через Інтернет або при явці у відділ реєстрації.

Третя таблиця містить інформацію про переваги ресурсів, які були віддані користувачем. Це адреси ресурсів, покажчики на користувачів, які працюють з цими ресурсами, і перелік дозволених значень, які можна видати даним ресурсам.

Четверта таблиця – налаштування. Вони містять в собі особисті налаштування користувача, що допомагають сервісу бути зручнішим в обігу.

Система обслуговування і реєстрації клієнтів виконує найголовнішу функцію. Саме ця система є центром серверів авторизації, яка стане найбільш важливою частиною проекту, оскільки вона буде схильна до найбільшого наван-

таження і швидше за все найбільшої кількості атак хакерів.

Система реєстрації клієнтів повинна мати серверну і клієнтську частину.

В ролі серверної частини виступає безпосередньо сам сервер, який здійснює роботу по обробці отриманих даних і їх занесенні в базу даних.

В ролі клієнтської частини виступає комп'ютер, що знаходиться в точці реєстрації.

Як же відбувається сам процес реєстрації?

Користувач, охочий реєструватися в системі, приходить в точку реєстрації з дійсним посвідченням особи. Таким посвідченням може служити паспорт або посвідчення водія.

Він укладає з підприємством, яке надає даний сервіс, договір, що зобов'язує це підприємство у жодному випадку не розголошувати інформацію про користувача без його угоди.

Пред'явивши посвідчення операторові системи реєстрації, користувач повідомляє, які дані він хоче занести через заповнення спеціальної анкети. Окрім обов'язкових даних, таких як прізвище, ім'я, по батькові, дата народження, місто мешкання, пароль і логін до облікового запису, користувач може вказати і необов'язкові, такі як точна адреса, фотографія, номер електронного гаманця, електронна поштова адреса і так далі. При цьому необов'язкову інформацію можна занести не тільки під час реєстрації. Можлива також додаткова явка користувача в будь-який відділ реєстрації для зміни або доповнення інформації. Також деяку інформацію можна доповнювати і через Інтернет.

Але навіть після введення оператором всієї обов'язкової інформації про користувача залишається одна проблема. Необхідна ідентифікація користувача за приватною ознакою, яка могла б його відрізнити від будь-якої іншої людини.

Припустимо, що такою ознакою може стати відбиток пальця користувача [2].

Склавши код за унікальною ознакою, можна вирішити ряд проблем.

По-перше, клієнт може дістати доступ до свого облікового запису, не маючи при собі ніяких посвідчень і не маючи пароля, якщо його обліковий запис, скажімо, зламали.

По-друге, система матиме унікальну інформацію про користувача, яка не мінятиметься при спробі повторної реєстрації в іншому відділі.

Зібрана інформація відправляється на сервер реєстрації через спеціальне безпечне з'єднання. Там в першу чергу перевіряється унікальний код користувача. Якщо такий вже існує, в реєстрації буде відмовлено. Тому складання і перевірку унікального коду варто проводити на самому початку реєстрації. Якщо ж код не присутній в базі даних, сервер створює новий обліковий запис з своїм порядковим номером, записує туди всі введені значення і повідомляє оператора про вдалу реєстрацію користувача.

Подібні відділи реєстрації, на пізніх етапах впровадження системи, повинні знаходитися в досяжності користувачів по всьому світу (де є доступ до мережі Інтернет).

Система обслуговування клієнтів грає ключову роль в запропонованому методі. Вона буде найчастіше використовуватися і, найімовірніше, буде сильно схильна до спроб злому. Тому саме цій системі варто приділити більше всього уваги.

Основна ідея була узята у Open Id [4] (див. рис. 1).

Розглянемо на прикладі голосування. В мить, коли клієнт спробує проголосувати на деякому ресурсі, йому потрібно буде реєструватися на ньому за допомогою сервера авторизації. Клієнт автоматично переадресовується на сервер, де він вводить свої логін і пароль або пред'являє відбиток пальця. Після цього йому надається перелік необхідних для реєстрації на ресурсі даних. Затвердивши цей перелік повністю або частково, клієнт переадресовується назад на ресурс, де вже залежно від затверджених даних йому дозволяють або відмовляють реєструватися.

При цьому ресурс проводить запит на сервер авторизації для з'ясування переліку доступних йому даних.

У такого методу є недолік: якщо ресурс створювався недобросовісно, то клієнта можна переадресувати на підроблену сторінку сервера авторизації (див. рис. 2). При цьому довірливий клієнт введе свої логін і пароль або образ відбитку пальця в базу даних творця цього підробленого сервера для подальшого корисливого використання третіми особами. Щоб уникнути цього, клієнтові пропонується ввести секретне питання і відповідь, які відомі лише йому і серверу авторизації. Кожного разу, коли клієнта туди переадресовують, він вводить секретне питання, після чого сервер повинен відповісти на нього, використовуючи введену раніше клієнтом відповідь. Якщо відповідь саме така, яку очікує клієнт, то він може бути упевнений в тому, що він знаходиться на справжньому сайті сервера авторизації [5].

Слабкою стороною вищеописаного методу є те, що користувачі відноситимуться до подібного роду системам з недовір'ям і це серйозно ускладнить її впровадження. При правильній рекламі та сертифікації цього можна уникнути. Також з'являється людський чинник при реєстрації користувача – правильність роботи точок

реєстрації повністю лежить на сумлінності обслуговуючого їх персоналу.

Отже, для успішного впровадження запропонованого принципу необхідно буде в подальшому вирішити ряд питань: організаційне, технічне та соціально-психологічне.

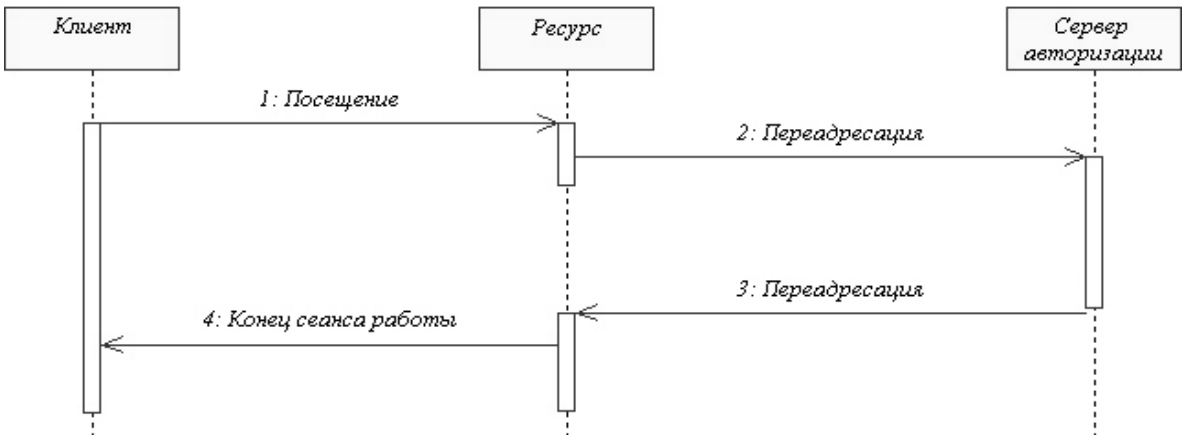

Рис. 1

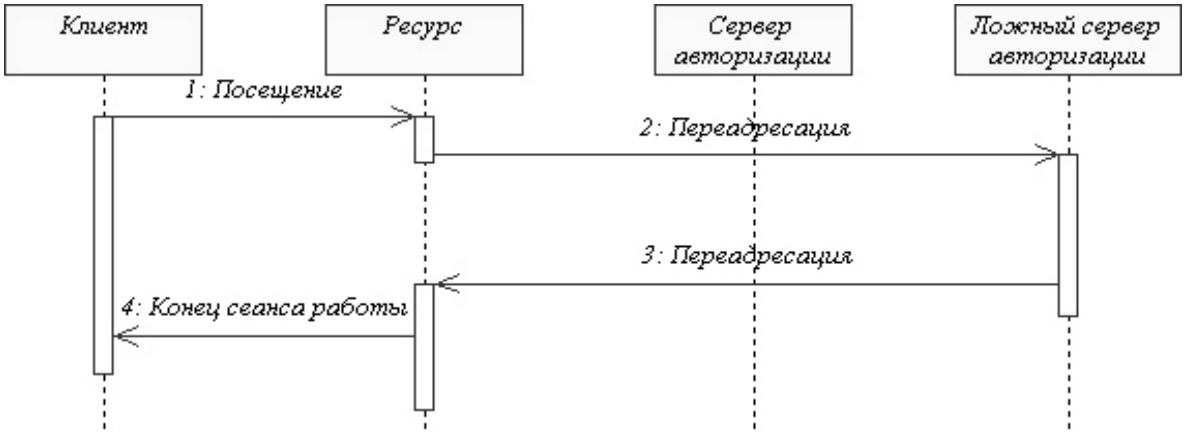

Рис. 2

Організаційне питання полягає у розгортанні доступної мережі пунктів реєстрації, якою могла би скористатися кожна людина.

Технічне питання полягає у оснащенні клієнтських терміналів дешевими засобами вводу біометричних даних.

Найважче питання, соціально-психологічне, потребує переконання користувача у корисності та безпечності такого способу ідентифікації.

У результаті запропонована система при правильному впровадженні забезпечить як з фізичної, так і з юридичної точки зору повну конфіденційність інформації, наданої користувачем. При цьому її достовірність гарантується точками реєстрації.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Кришнамурти, Б. Web-протоколы. Теория и практика [Текст] / Б. Кришнамурти, Дж. Рексфорд. – М.: БИНОМ, 2002. – С. 58-61.
2. Benantar, M. Access Control Systems: Security, Identity Management and Trust Models [Text] / Messaoud Benantar.
3. Recordon, D. OpenID: The Definitive Guide: Identity for the Social Web [Text] / D. Recordon, L. Rae, Ch. Messina.
4. Bell, G. Building Social Web Applications: Establishing Community at the Heart of Your Site [Text] / Gavin Bell.
5. Andrews, M. How to Break Web Software: Functional and Security Testing of Web Applications and Web Services [Text] / M. Andrews, J. A. Whittaker.

Надійшла до редколегії 17.08.2010.
Прийнята до друку 25.08.2010.