УДК 004.056

І. В. Миронець, *к.т.н., доцент,*
e-mail: irenmir@ukr.net
Н. Є. Радзієвський, *аспірант,*
e-mail: delumcor@rambler.ru
Черкаський державний технологічний університет,
б-р Шевченка, 460, м. Черкаси, 18006, Україна

АНАЛІЗ МЕТОДІВ ТА ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Стаття присвячена аналізу основних методів та протоколів аутентифікації користувача. В процесі дослідження проаналізовано принцип роботи методів і протоколів аутентифікації та їх ключові особливості, сфера застосування і ступінь захищеності інформації при використанні того чи іншого методу та протоколу. В комп'ютерних системах для передачі інформації на етапі ідентифікації користувач надає свої особисті електронні дані для перевірки, на етапі аутентифікації особисті електронні дані користувача перевіряються за допомогою тих чи інших протоколів і на кінцевому етапі, в результаті успішної перевірки електронних даних користувача на правдивість, користувач отримує права доступу до того чи іншого ресурсу. Електронні системи передачі інформації мають і складніші методи аутентифікації та авторизації, побудовані на роботі різних протоколів. Дослідивши переваги та недоліки розглянутих протоколів аутентифікації користувача в комп'ютерних мережах, було визначено подальші напрямки дослідження та шляхи вирішення проблем, які виникли в рамках проведеного аналізу.

Ключові слова: *ідентифікація, аутентифікація, авторизація, комп'ютерні системи, конфіденційні дані, захист інформації.*

Постановка проблеми. Поняття безпеки є досить широким у сфері захисту інформації та містить в собі такі фактори як: надійність роботи комп'ютера користувача, забезпечення цілісності даних, тобто захист інформації від несанкціонованого внесення до неї змін, не допущеними до цього особами, захист таємниці електронного листування чи передачі даних при використанні електронного зв'язку. На сторожі особистої безпеки громадян завжди стоїть закон, але у сфері інформаційної безпеки практика на даний момент розвинена не на такому високому рівні, а процес створення законів не завжди встигає за темпами розвитку комп'ютерних систем та засобів передачі даних, в чому опирається на заходи особистого захисту.

Постійно постає проблема вибору між забезпеченням необхідного рівня захисту інформації та ефективністю роботи систем електронної передачі даних. Деякі заходи для забезпечення інформаційної безпеки іноді користувачі можуть розцінювати як заходи, що обмежують доступ до електронних систем передачі даних чи знижують ефективність їх роботи. Такий засіб, як криптографія надає змогу значно підвищити рівень захисту інформації та не обмежувати користувачів у доступі до неї.

Захист даних під час швидкої та ефективної передачі через мережу є вкрай важливою проблемою.

Аналіз останніх досліджень та публікацій. Аналіз наукової літератури [1-8] доводить актуальність досліджень методів та протоколів аутентифікації в комп'ютерних мережах. Публікації останніх років показують, що засоби заволодіння інформацією, яка передається в комп'ютерних мережах, удосконалюються не менш інтенсивно, ніж заходи захисту від них. Захист інформації - це не разовий захід і навіть не сукупність - це безперервний цілеспрямований процес, що вимагає вживання відповідних заходів на всіх етапах обробки, передачі та зберігання даних. Розробка нових методів та протоколів повинна вестися паралельно з розробкою комп'ютерних мереж, які захищаються, тому дослідження в даній області проводяться постійно.

Зокрема, Домаревим В. В. розроблено ефективні методологічні засоби моделювання загроз передачі даних і побудовані методи захисту інформації [1].

Смітом Р. Е. детально розглянуто сучасні протоколи аутентифікації, а також їх основні вразливості [2].

Малюком А. А. детально розписано принципи роботи протоколів аутентифікації, а також їх взаємодія з веб-серверами та веб-додатками [3].

За результатами проведеного аналізу публікацій було визначено основні вразливі місця в комп'ютерних мережах [6]. Зазвичай це - апаратура, інформаційний сервер, паролі і середовище передачі даних. Якщо інформаційний сервер може бути захищений організаційними заходами, то комп'ютерну мережу в такий спосіб захистити не можливо.

Метою даної роботи є дослідити методи та протоколи аутентифікації користувача в комп'ютерних мережах, проаналізувати їх переваги та недоліки.

Виклад основного матеріалу. В наш час усюди застосовуються різноманітні методи та протоколи аутентифікації користувача, які застосовуються у роботі з веб-додатками у мережі. Розглянемо основні методи та протоколи, що використовуються у веб-додатках для аутентифікації користувача в мережі.

Основними термінами цього напрямку є:

1. Ідентифікація — процедура підтвердження особистості користувача, його особистих даних, такими даними можуть бути: ім'я, адреса електронної поштової скриньки, тощо.
2. Аутентифікація — процедура перевірки раніше наданих особистих даних про особистість користувача.
3. Авторизація – процедура, що в результаті перевірки особистих даних надає користувачеві права доступу.

Отже, спочатку користувач надає особисті дані для перевірки (ідентифікується), потім ці дані підтверджуються (аутентифікуються) і в результаті перевірки користувач отримує дозвіл для роботи (авторизуються).

В комп'ютерних системах для передачі інформації також застосовуються вищеназвані терміни, на етапі ідентифікації користувач надає свої особисті електронні дані (адреса поштової скриньки та пароль) для перевірки, на етапі аутентифікації особисті електронні дані користувача перевіряються за допомогою тих чи інших протоколів і на кінцевому етапі, в результаті успішної перевірки електронних даних користувача на правдивість – користувач отримує права доступу до того чи іншого ресурсу [1].

Електронні системи передачі інформації мають і складніші методи аутентифікації та авторизації, побудовані на роботі різних протоколів.

Одним із таких методів є аутентифікація за допомогою пароля, який полягає в тому, що користувач надає свої електронні дані для перевірки для ідентифікації та аутентифікації, в результаті чого отримуючи доступ до потрібного ресурсу. Як правило, такі електронні дані являють собою особисте електронне ім'я користувача (username) та пароль доступу до системи (password), як особисте електронне ім'я користувача у системі зазвичай використовують адресу поштової скриньки. Ці особисті електронні дані задаються користувачем при реєстрації та зберігаються в базі даних.

Розглянемо основні стандартні протоколи аутентифікації користувача.

Протокол HTTP аутентифікації описаний в стандартах HTTP 1.0/1.1.

Даний протокол, описаний в стандартах HTTP 1.0/1.1, він існує та застосовується в комп'ютерних мережах вже давно і на сьогоднішній день є актуальним.

В комп'ютерних мережах цей протокол працює наступним чином (рис. 1.):

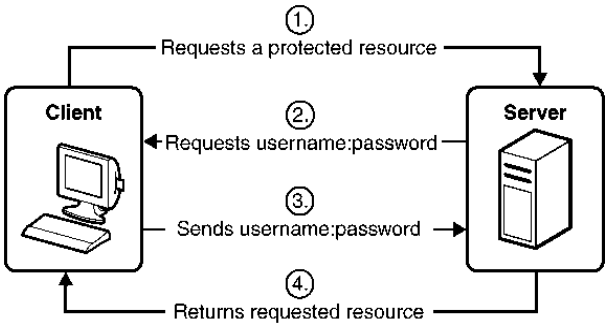

Рис. 1. Приклад роботи HTTP протоколу аутентифікації користувача

1. При зверненні неавторизованого користувача до захищеного веб-ресурсу сервер відсилає користувачеві HTTP повідомлення «401 unauthorized», а також додає до нього заголовок «www-authenticate» в якому вказані схема і параметри аутентифікації.
2. Коли користувач отримує таке повідомлення – браузер автоматично виводить користувачеві інтерфейс для вводу особистої електронної інформації користувача.
3. В подальшому до всіх запитів користувача до цього веб-ресурсу браузер додава-

тиме HTTP заголовок «authorization», де будуть передаватися дані для аутентифікації сервера.

4. Сервер отримавши таке HTTP повідомлення від користувача аутентифікує його. На основі особистих даних користувача рішення про надання користувачеві доступу проводиться окремо.

Робота цього протоколу є стандартизованою і добре підтримується виконується всіма браузерами та веб-серверами.

Багаторічна практика знайшла у цього протоколу ряд своїх переваг та недоліків, декілька слів про них:

HTTP протокол аутентифікації користувача має такі переваги:

1. Простота – даний протокол дозволяє з легкістю створювати потрібні клієнтські програми.

2. Розширюваність – стандартні можливості даного протоколу дозволяють додавати особисті заголовки, за допомогою таких заголовків є можливість підвищення функціональності.

3. Розповсюдженість – даний протокол добре підтримується в якості клієнта багатьма програмами та завдяки цьому він широко використовується для рішення різних задач.

Недоліками даного протоколу є наступні:

1. Відсутність «навігації» – у протоколу HTTP аутентифікації у явному вигляді відсутні засоби навігації між веб-ресурсами сервера. Тобто клієнт напряму не може запросити перелік доступних файлів. Ця проблема вирішується за допомогою розширюючого протоколу WebDAV, при використанні допомогою додаткового методу PROFIND.

2. Відсутність підтримки розподіленості – Початково HTTP протокол був розроблений для рішення побутових типових задач, де час обробки даних не мав займати багато часу, або взагалі не мав відігравати значної ролі. Але з плином часу стало зрозуміло, що при використанні його у промислових цілях з використанням зазначених розрахунків та при високій навантаженості на сервер протокол є не ефективним, в зв'язку з цим у 1998 році був запропонований альтернативний протокол HTTP-NG(HTTP Next Generation), який досі знаходиться у розробці [2].

З вище описаних особливостей можна зробити висновок, що HTTP протокол аутентифікації користувача є простим, універсальним, легко модифікованим, і, якщо можна так сказати, він став стандартом, але він має і свої недоліки, оскільки він був розроблений для багатьох цілей, а не виключно для аутентифікації, він потребує більше часу для роботи, додаткові підтримку та налаштування для якісної роботи.

В даний час поширені є такі схеми аутентифікації, які за рівнем безпеки відрізняються:

1. Basic – дана схема являється однією з доступних та простих, передає особисті електронні дані користувача в заголовку «authorization» (рис. 2.) у незашифрованому вигляді (base64-encoded).

Рис. 2. Приклад HTTP аутентифікації з використанням Basic схеми

2. Digest – це схема, яка працює за принципом запит-відповідь, коли сервер надсилає унікальний запит, а у відповідь браузер надсилає унікальну відповідь, котра містить хеш дані про пароль користувача, обчислену за допомогою зазначеного унікального значення, надісланого сервером. Тобто ця схема є більш надійною альтернативою Basic схеми при використанні незахищених з'єднань, але вразлива до так званих «Людина в центрі» атак, коли йде перехват і заміна повідомлення, якими обмінюються клієнт і сервер. Використання даної схеми обмежує використання сучасних хеш-функцій для зберігання на сервері паролів користувачів.

3. NTLM (Windows authentication) – ця схема також побудована на запит-відповідь методі роботи у якому пароль у чистому вигляді не передається. Ця схема підтримується більшістю серверів і браузерів, але вона не є стандартом HTTP та використовується переважно для роботи у веб додатках Windows Active Directory.

4. Negotiate – ця схема є зразком так званого сімейства Windows authentification, що надає можливість клієнтові обирати між NTLM та Kerberos схемою аутентифікації. Система аутентифікації Kerberos є більш безпечним протоколом, що працює по технології

єдиного входу, але він може працювати лише тоді, коли сервер та клієнт знаходяться в зоні Internet і являються частиною домену Windows.

Іншим широко використовуваним протоколом аутентифікації є протокол Formsauthentification. Певного стандарту для цього протоколу не існує, тому всі види його реалізації унікальні визначених систем, або як їх ще називають – модулів аутентифікації фреймворків розробки.

Робота протоколу Formsauthentification побудована наступним чином: до веб-додатку додається HTML-форма для введення персональних електронних даних користувача, до якої потрібно внести особисті електронні дані користувача та відправити їх до сервера для аутентифікації. Якщо аутентифікація завершена успішно, тоді веб додаток створює спеціальну мітку (токен, sessiontoken), яка поміщається зазвичай в тимчасові файли браузера. Надалі токен буде автоматично додаватися у наступні запити користувача до сервера і дозволятиме тим самим отримувати додатково відомості про активного користувача для авторизації запиту (рис. 3.).

Створення додатком токена може відбуватися двома способами:

Рис. 3. Приклад роботи протоколу Formsauthentication

1. Створення токена, який буде використовуватись в якості ідентифікатора аутентифікованого за допомогою сесії активного в даний час користувача та зберігатиметься в базі даних чи в пам'яті сервера.

2. Створення токена як підписаного чи зашифрованого об'єкта, котрий в собі містить дані про користувача. Такий спосіб дає змогу застосувати багаторівневу (stateless server) архітектуру сервера, але потребує забезпечення постійного оновлення даних про сесійний сертифікат після завершення терміну його дії.

Варто зазначити, що такий рівень доступу, як і при введенні електронних даних може надати перехоплення токена. Для запобігання перехоплення токена спілкування між клієнтом і сервером, при використанні протоколу Formsauthentification, має проходити тільки по захищеному з'єднанню HTTPS [3].

Потрібно відмітити, що при використанні HTTP протоколу аутентифікації користувача неможливо завершити роботу браузера стандартним шляхом, окрім як закрити всі вікна бразера, чи взагалі завершити його роботу шляхом переривання роботи на системному рівні Windows.

Протокол Formsauthentification має деякі переваги, а саме:

1. Універсальність – даний протокол одразу готовий до роботи, для постійного підтримання функції входу в систему і не потребує для цього додаткових налаштувань чи додаткових протоколів.

Недоліками цього протоколу є такі фактори:

1. Роздробленість – функція входу в систему є залежною від машинного ключа, що робить необхідною перевірку машинних ключів на всіх серверах системи.
2. Не раціональне збереження тимчасових даних – тимчасові файли, які знаходяться у браузері містять зашифровані дані для аутентифікації, які там можна і не зберігати.

Таким чином можна зазначити, що протокол Formsauthentification є універсальним і заздалегідь підготовленим рішенням багатьох задач для систем аутентифікації, але він виконує деяку зайву роботу і має деякі вагомі вразливості з точки зору захисту інформації.

У цілому аутентифікація за допомогою пароля вважається не дуже надійним методом, адже пароль може бути підібраний, а користувачі мають властивість часто використовувати дуже прості чи однакові паролі для декількох веб-ресурсів, або взагалі записувати їх на папері [4]. Користувач часто не дізнається, що його пароль був підібраний. Окрім цього, помилки можуть і самі допускати ряд помилок, які дають зловмисникам нагоду зламу облікових записів.

Існують такі найбільш поширені вразливості при використанні аутентифікації за паролем [5]:

1. Веб-додаток дає дозвіл користувачам на використання простих паролів.

2. Веб-додаток не оснащений захистом від механізмів підбору паролів.

3. Веб-додаток виконує передачу паролів через незахищене HTTP з'єднання.

4. Веб-додаток не користується захищеними хеш-функціями для захищеного зберігання паролів користувачів.

5. Веб-додаток може використовувати не захищену функцію для відновлення пароля користувача, до якої можливо отримати доступ для неавторизованого використання інших облікових записів.

6. Веб-додаток може не запитувати у користувача дані для повторної аутентифікації при виконанні важливих дій, таких як зміна пароля.

7. Веб-додаток може надавати користувачам токени, яки вже передбачені для інших користувачів, таким чином токени можуть бути підібрані.

8. Веб додаток може не завершувати сесію користувача після не тривалого періоду неактивності.

Дослідивши вказані переваги та недоліки методів та протоколів аутентифікації користувача в комп'ютерних мережах, було визначено подальші напрямки дослідження та шляхи вирішення проблем, які виникли в рамках проведеного аналізу.

Висновки. В процесі даного дослідження розглянуті основні методи та протоколи для аутентифікації користувача в комп'ютерних мережах та системах.

Проведено дослідження роботи HTTP протоколу аутентифікації користувача та протоколу Formsauthentification.

Виконаний аналіз ключових моментів в роботі цих протоколів і відмічені переваги та недоліки, які вимагають захисту та доопрацювання в подальшому дослідженні.

Список літератури

1. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ООО «ТИД «ДС». 2001. 688 с.
2. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. Москва: Горячая линия-Телеком, 2001. 148 с.
3. Смит Р. Е. Аутентификация: от паролей до открытых ключей = Authentication: from passwords to public keys. First Edition. Москва: Вильямс, 2002. С. 432.
4. Острейковский В. А. Информатика: учеб. пособие. Москва: Высшая школа, 2001. 319 с.
5. Молдовян А. А., Молдовян Н. А., Рад Б. Я. Криптография. С.Пб.: Изд-во «Лань», 2001. 224 с.
6. Норткатт С., Новак Д., Маклахлен Д. Обнаружение вторжений в сеть. Изд-во «ЛОРИ», 2001. 384 с.
7. Мухин В. Е., Дарвиш Л. Средства для анализа и повышения эффективности протоколов аутентификации в компьютерных сетях. *Вісник НТУУ "КПІ". Серія "Інформатика, управління та обчислювальна техніка"*. 2004. № 42. С. 71–83.
8. Столингс В. Основы защиты сетей. Приложения и стандарты. Москва: Вильямс, 2002. 324 с.

References

1. Domarev, V. V. (2001) The security of information technologies. Methodology for creating protection systems. Kiev: LLC "TID" DS ", 688 p. [in Russian].
2. Malyuk, A. A, Pazizin, S. V., Pogozhin, N. S. (2001) Introduction to information protection in automated systems. Moscow: Goryachaya liniya-Telekom, 148 p. [in Russian].
3. Smit, R. E. (2002) Authentication: from passwords to public keys. First Edition. Moscow: Williams, p. 432 [in Russian].
4. Ostrejkovskiy, V. A. (2001) Informatics. Moscow: Vysshchaya shkola, 319 p. [in Russian].
5. Moldovyan, A. A., Moldovyan, N. A., Rad, B. Ya. (2001) Cryptography. St. Petersburg: Izd-vo "Lan", 224 p. [in Russian].
6. Norcutt, S., Novak, D., McLachlan, D. (2001) Detection of intrusions into the network. Izd-vo "LORI", 384 p. [in Russian].
7. Mukhin, V. Ye., Darvish, L. (2004) Means for analyzing and increasing the efficiency of authentication protocols in computer networks. *Visnyk NTUU "KPI". Seriya "Informatyka, upravlinnya ta obchyslyuvalna tehnika"*, No. 42, pp. 71–83 [in Russian].
8. Stolings, V. (2002) The fundamentals of network protection. Applications and standards. Moscow: Williams, 324 p. [in Russian].

I. V. Myronets, *Ph.D., associate professor,*
e-mail: irenmir@ukr.net,
N. E. Radzyevskyj, *postgraduate*
e-mail: delumcor@rambler.ru
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

THE ANALYSIS OF METHODS AND AUTHENTICATION PROTOCOLS IN COMPUTER NETWORKS

This article is devoted to the analysis of the main methods and protocols of user authentication. During the research, the principle of operation of authentication methods and protocols and their key features, scope and degree of information security when using one or another method and protocol are analyzed. In computer systems for information transferring, at the identification stage, user provides his personal electronic data for verification. At the stage of authentication, personal user's electronic data are verified with certain protocols. Ultimately, as a result of successful verification of user's electronic data the user gets access rights to a particular resource. Electronic systems of information transmission also have more sophisticated methods of authentication and authorization built on various protocols. After the investigation of advantages and disadvantages of the considered user authentication protocols in computer networks, the further directions of research and ways of solving the problems that arose during the analysis are determined.

Keywords: *identification, authentication, authorization, computer systems, confidential data, protection of information.*

Рецензенти: Рудницький В. М., д.т.н., професор,
Голуб С. В., д.т.н., професор