УДК 004.056 **В.М. Ахрамович**

# ІДЕНТИФІКАЦІЯ Й АУТЕНТИФІКАЦІЯ, КЕРУВАННЯ ДОСТУПОМ

Досліджена проблема надійності ідентифікації/аутентифікації в тому числі, в традиційних кабельних мережах та бездротових з урахуванням протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача й системного адміністратора з іншого. Вказано на недоліки аутентифікації в бездротових мережах коли логін та пароль передається за мережею в незашифрованому вигляді, або з використанням ненадійних методів шифрування, в тому числі в операційній системі Windows з урахуванням доступу до процесів. Вказано на ненадійність методу аутентифікації за допомогою Mac-Адрес. Аутентифікація PEAP на бездротових маршрутизаторах LinksysWRT54GuGS буде ще одним додатковим рівнем безпеки.

***Ключові слова:*** комп'ютерна система захисту, сучасні засоби ідентифікації/ аутентифікації, атака, потоки, розмежування прав користувачів, системний адміністратор, Mac-Адреса, криптозахист, сертифікати, маркери, паролі.

**Вступ**

Ідентифікація – встановлення тотожності невідомого об'єкта відомому на основі співпадання ознак; впізнання.

Ідентифікація в інформаційних системах – присвоєння суб'єктам и об'єктам ідентифікатора і / або порівняння ідентифікатора с переліком присвоєних ідентифікаторів.

Аутентифіка́ція (англ. *authentication*; від грец. αὐθεντικός [authentikos] – реальний, справжній; від αὐθέντης [authentes] – автор) – процедура перевірки дійсності, наприклад:

- перевірка дійсності користувача шляхом порівняння введеного їм пароля з паролем, збереженим у базі даних користувачів;
- підтвердження справжності електронного листа шляхом перевірки цифрового підпису листа за відкритим ключем відправника
- перевірка контрольної суми файлу на відповідність сумі, заявленої автором цього файлу.

**Основна частина**

Комп'ютерна система захисту (КСЗ) повинна забезпечувати ідентифікацію користувачів при запитах на доступ, повинна перевіряти дійсність ідентифікатора суб'єкта - здійснювати аутентифікацію. КСЗ повинна мати у своєму розпорядженні необхідні дані для ідентифікації й аутентифікації й перешкоджати входу у систему не ідентифікованого користувача або користувача, чия дійсність при аутентифікації не підтвердилася.

Ідентифікація дозволяє суб'єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе ( повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає [1]. У якості синоніма слова " аутентифікація " іноді використовують словосполучення "перевірка дійсності".

Суб'єкт може підтвердити свою дійсність, пред'явивши принаймні одну з наступних сутностей:

- щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і т.п.);
- щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);
- щось, що є частина його самого (голос, відбитки пальців і т.п., тобто свої біометричні характеристики).

У відкритому мережевому середовищі між сторонами ідентифікації/аутентифікації не існує довіреного маршруту [1]; це значить, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими й використаними для перевірки дійсності. Необхідно забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни або відтворення даних. Передача паролів у відкритому вигляді, мабуть,

незадовільна; не рятує положення й шифрування паролів, тому що воно не захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація ускладнюється не тільки через мережеві погрози, але й із цілого ряду причин. По-перше, майже про всі аутентифікаційні сутності можна довідатися, їх можна украсти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача й системного адміністратора з іншогої. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно ввести аутентифікаційну інформацію (адже на його місце могла сісти інша людина), а це не тільки клопітно, але й підвищує ймовірність того, що хтось може підглядати за введенням даних. По-третє, чим надійніше засіб захисту, тем він дорожчий.

Сучасні засоби ідентифікації/ аутентифікації повинні підтримувати концепцію єдиного входу в мережу [2,3]. Єдиний вхід у мережу - це, у першу чергу, вимога зручності для користувачів. На жаль, поки не можна сказати, що єдиний вхід у мережу став нормою.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ідентифікації й аутентифікації.

Цікаво відзначити, що сервіс ідентифікації / аутентифікації може стати об'єктом атак на доступність. Якщо система сконфігурована так, що після певного числа невдалих спроб пристрій уведення ідентифікаційної інформації (наприклад, термінал) блокується, то зловмисник може припинити роботу легального користувача буквально декількома натисканнями клавіш.

Враховуючи ступінь довіри й політикові безпеки систем, проведена перевірка дійсності може бути однобічною або взаємною. Звичайно вона проводиться за допомогою криптографічних способів.

Якщо процедура аутентифікації пройшла успішно, наступним кроком є ідентифікація. Завдання ідентифікації - одержати ідентифікатор користувача в системі. Це може бути його id, унікальний логін, пошта і т.д. І, нарешті, після всього цього відбувається авторизація. Суть авторизації в наділенні користувача деякими правами. Наприклад, права адміністратора, користувача, анонiма (неавторизированного користувача).

Найчастіше, в php скриптах немає чіткого поділу між першим і другим етапом, або навіть трьома. У найпростішому випадку ці дії можна зробити однієї вибіркою із БД.

Розглянемо ідентифікацію користувача на прикладі операційної системи Windows. Перший крок ідентифікації, підтримуваний режимом аутентифікації, реалізується при вході користувача в систему. Тут слід виділити два режими – це штатний вхід і вхід у безпечному режимі (Safe Mode). Принциповою відмінністю цих режимів є те, що при запуску системи в безпечному режимі не завантажуються сторонні стосовно системи драйвери й додатки. У даному режимі передбачається вільний вхід для будь-якого користувача, після його ідентифікації й аутентифікації (наприклад, в Unix-Системах подібний вхід у систему дозволений тільки користувачеві root), то даний режим входу в систему несе в собі погрозу зняття додаткової системи захисту інформації несанкціонованого доступу(ЗДСЗІ НСД) (якщо вона використовується).

Другий крок полягає в запуску користувачем процесів, які вже, у свою чергу, породжують потоки (саме потоки здійснюють звертання до ресурсів). Тут також існує дві можливості. Розглянемо їх. Усі працюючі в системі процеси й потоки виконуються в контексті захисту того користувача, від імені якого вони так чи інакше були запущені. Для ідентифікації контексту захисту процесу або потоку використовується об'єкт, який називається маркером доступу (access token). У контекст захисту входить інформація, що описує привілеї, облікові записи й групи, зіставлені із процесом і потоком. При реєстрації користувача у системі створюється початковий маркер, що представляє користувача, який входить у систему, і зіставляє його із процесом оболонки, застосовуваної для реєстрації користувача. Усі програми, що запускаються користувачем, успадковують копію цього маркера. Механізми захисту в Windows використовують маркер, визначаючи набір дій, дозволених потоку або процесу.

Однак у загальному випадку користувач має можливість запуску процесу, як із власними правами, так і під обліковим записом іншого користувача. Запуск користувачем процесу під чужим обліковим записом можливий тільки після виконання процедури авторизації – користувач повинен увести ідентифікатор і пароль облікового запису. Зокрема, подібну можливість в ОС Windows надає утиліта: runas.exe. Подібна можливість, насправді, досить критична в частині забезпечення комп'ютерної безпеки. Справа в тому, що на практиці розмежовується не тільки доступ до інформації, але й режими її обробки. Наприклад, для обробки конфіденційних даних можуть бути встановлені режими: збереження на зовнішньому носієві тільки в зашифрованому вигляді, заборона передачі за мережею і т.д. Для обробки ж відкритої інформації дані обмеження не потрібні. Тоді не тільки доступ до інформації, але й режими її обробки визначаються ідентифікатором користувача. Тепер припустимо, що один з паролів скомпрометований. У цьому випадку критичним стає не тільки знання користувачем, допущеним до обробки відкритої інформації, пароля користувача, конфіденційної інформації. Справа в тому, що в цьому випадку користувач, допущений до конфіденційної інформації може запускати процеси з більш широкими правами, ніж визначені йому. Як наслідок, виникає погроза розкрадання конфіденційної інформації. Тут не зайвим буде відзначити, що більшу ймовірність компрометації має пароль саме користувача, допущеного до обробки відкритих даних ( з очевидних міркувань вимоги до нього й до його зберігання нижчі, тому що інформація-те відкрита, загальнодоступна).

І, нарешті, третій крок полягає в породженні процесом потоків, які й звертаються до ресурсів. Вертаючись до маркера безпеки, відзначимо, що маркер може бути основним (ідентифікує контекст захисту процесу) або, що персоніфікує (застосовується для тимчасового запозичення потоком іншого контексту захисту – зазвичай іншого користувача). Уособлення (impersonation) надає можливість окремому потоку виконуватися в контексті захисту, відмінного від контексту захисту процесу, тобто діяти від імені іншого користувача. Уособлення, наприклад, застосовується в моделі програмування " клієнт-сервер". При запозиченні прав сервер тимчасово ухвалює профіль захисту клієнта, " від імені" якого звертається до ресурсу. Тоді сервер може працювати з ресурсом від імені клієнта, а система захисту проводити перевірку його прав доступу. Звичайно серверу доступне більш широке коло ресурсів, ніж клієнтові, і при уособленні потік втрачає частину вихідних прав доступу, що запустив його процес. І, навпаки, при уособленні відповідний потік може одержати додаткові права. Подібна можливість, практично ніяк не контрольована ОС Windows, привела до появи цілої групи уразливостей, пов'язаних з некоректністю використання сервісів уособлення, надаваних ОС, розроблювачами додатків (помилки програмування). Атаки на ці уразливості, як правило, мають своєю метою розширення привілеїв, зокрема, несанкціоноване одержання прав користувачів System і Administrator.

Пропоновані підходи до реалізації механізмів ідентифікації й аутентифікації додатковими засобами.

В ряді додатків механізми ідентифікації й аутентифікації вбудовані в ОС Windows реалізуються не коректно (наприклад, відсутній контроль уособлення). Як наслідок, необхідні додаткові засоби. Застосування ж додаткових засобів приводить до некоректності реалізації інших механізмів, зокрема механізму ідентифікації й аутентифікації користувача при вході в систему в захищеному режимі.

Коректна (однозначна) ідентифікація суб'єкта доступу до ресурсів можлива лише по сукупності двох параметрів – ідентифікатор користувача й ефективний ідентифікатор користувача, під яким розуміються ідентифікаційні параметри потоку, що здійснює доступ до ресурсів.

Доводиться твердження від зворотного. Якщо при контролі доступу до ресурсів розглядається тільки ідентифікатор користувача, то в загальному випадку не представляється можливим надійно зв'язати отриману ідентифікацію користувача з усіма діями даного користувача, тому, що потік перед звертанням до ресурсу може уособити себе із правами іншого користувача, ідентифікація якого при цьому системою не здійснюється.

Якщо ми говоримо про те, що однозначно суб'єкт доступу ідентифікується лише парою параметрів – ідентифікатор і ефективний ідентифікатор користувача, то дотримуючись основ теорії захисту інформації, можливі два підходи до захисту в цьому випадку – розмежування прав користувачів (або процесів) на одержання ефективного ідентифікатора (уводяться списки дозволених, або, навпаки, заборонених пар: ідентифікатор і ефективний ідентифікатор, і засобами СЗІ НСД контролюється їхнє створення), відповідно, контроль ідентифікуючих ознак (дозволених, або, навпаки, заборонених пара: ідентифікатор і ефективний ідентифікатор) при доступі до ресурсів.

Не краще ситуація виглядає в бездротових мережах, в тому числі, з питань ідентифікації/ аутентифікації. Розлянемо це на декількох прикладах.

Підслуховування. Найпоширеніша проблема в таких відкритих і некерованих середовищах, як бездротові мережі, - можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, що передаються. Підслуховування дозволяє зібрати інформацію в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника - зрозуміти, хто використовує мережу, які дані в ній доступні, які можливості мережевого встаткування, у які моменти його експлуатують найбільше й найменш інтенсивно і яка територія розгортання мережі. Усе це пригодиться для того, щоб організувати атаку на мережу. Загальнодоступні мережеві протоколи передають таку важливу інформацію, як ім'я користувача пароль, відкритим текстом. Це дозволяє провести зловмиснику ідентифікацію/ аутентифікацію в короткі терміни з мінімальними затратами.

Погрози криптозахисту**.** У бездротових мережах застосовуються криптографічні засоби для забезпечення цілісності й конфіденційності інформації. Однак помилки приводять до порушення комунікацій і використання інформації зловмисниками. WEP - це криптографічний механізм [4], створений для забезпечення безпеки мереж стандартом 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується всіма користувачами. Доступ до ключів, часта їхня зміна й виявлення порушень практично неможливі. Дослідження Wep-шифрування виявило вразливі місця, через які атакуючий може повністю відновити ключ після захоплення мінімального мережевого трафіка. В Internet є засоби, які дозволяють зловмисникові відновити ключ протягом декількох годин. Тому на WEP не можна покладатися як на засіб аутентифікації й конфіденційності в бездротовій мережі. ШифруванняWEP (Wired Equivalent Privacy) було дискредитоване за рахунок уразливостей в алгоритмі розподілу ключів RC4. Це трохи пригальмувало розвиток Wi-Fi ринку й викликало створення інститутом IEEE робочої групи 802.11i для розробки нового стандарту, що враховує уразливості WEP, та забезпечує 128-бітне AES шифрування й аутентифікацію для захисту даних. Wi-Fi Alliancев 2003 представив свій власний проміжний варіант цього стандарту — WPA (WPAFi Protected Access). WPA використовує протокол цілісності тимчасових ключів TKIP (TKIPoral Key Integrity Protocol). Також у ньому використовується метод контрольної суми MIC (MICsage Integrity Code), яка дозволяє перевіряти цілісність пакетів .В 2004 Wi-Fi Alliance випустили стандарт WPA2, який являє собою поліпшений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування: TKIP і AES. WPA2 забезпечує більш високий рівень захисту мережі, тому що TKIP дозволяє створювати ключі довжиною до 128 біт, а AES –до 256 біт. Шифрування даних в WPA займається протокол TKIP, що використовує динамічні ключі. Також у ньому застосовуються більш довгий вектор ініціалізації й криптографічна контрольна сума (MIC) для підтвердження цілісності пакетів.

Недоступність MAC-адрес. Прийнято вважати, що розмежування доступу, засноване на поділі апаратних Mac-Адрес бездротових мережевих адаптерів на "своїх" і "чужих", є ефективним засобом протидії атакам. Це дійсно так, але лише при забезпеченні додаткових заходів безпеки. До речі, аутентифікація бездротового клієнта за Mac-адресою - винятково ініціатива конкретного виробника, специфікації бездротових стандартів 802.11b/g такого заходу безпеки не передбачають. Тобто подібний метод аутентифікації може бути присутнім,

або ні, - залежно від бажання й маркетингової політики виробника. Навіть якщо існує можливість "відсівання" чужих бездротових клієнтів, повністю покладатися на цей захід не варто - її злом займає лічені хвилини й доступний навіть починаючому хакерові з незакінченою середньою освітою. Суть злому така: за допомогою спеціальної утиліти прослуховується радіообмін крапки доступу на каналі, по якому відбувається обмін інформацією із клієнтами, і в отриманому трафіку виділяється список "своїх" клієнтів. Потім залишається лише програмно підмінити апаратну адреса свого бездротового адаптера на один зі списку добутих адрес (у переважній більшості випадків це можна зробити навіть стандартними засобами драйвера) - і "чужий" адаптер став "своїм".

Аутентифікація. Для захисту від цієї погрози слід впроваджувати аутентифікацію. Аутентифікація додає ще один рівень безпеки, вимагаючи, щоб комп'ютер клієнта зареєструвався в мережі. Традиційно це виконується за допомогою сертифікатів, маркерів або паролів (також відомих як Preshared-key), які перевіряються на сервері аутентифікації.

Стандарт802.1X дозволяє працювати з WEP, WPA і WPA2 і підтримує кілька типів аутентифікації EAP(Extensible Authentication Protocol). Налаштування аутентифікації може виявитися скрутним й дорогим завданням навіть для професіоналів, не говорячи про звичайних користувачів. На щастя, ситуація постійно поліпшується, уже не потрібно купувати повноцінний сервер RADIUS, оскільки з'явилася безліч простих в установці альтернативних розв'язків. Подібний продукт від Wireless Security Corporation (недавно придбаної Mcafee) зветься WSC Guard. Ціна передплати на нього починається від $4,95 на місяць за кожного користувача, при оплаті декількох місць діють знижки. Наступний розв'язок більше підходить для досвідчених "адміністраторів мереж" –TinyPEAP являється прошиванням із сервером RADПJS, який підтримує аутентифікацію PEAP на бездротових маршрутизаторах LinksysWRT54GиGS.

**Висновки**

Ідентифікацію й аутентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й аутентифікація - це перша лінія оборони, "прохідна" інформаційного простору організації.

Необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ідентифікації й аутентифікації.

Коректна (однозначна) ідентифікація суб'єкта доступу до ресурсів можлива лише за сукупністю двох параметрів – ідентифікатор користувача й ефективний ідентифікатор користувача, під яким розуміються ідентифікаційні параметри потоку, що здійснює доступ до ресурсів.

В бездротових мережах рекомендується використовувати WPA2. Основна відмінність між WPA і WPA2 полягає в технології шифрування: TKIP і AES. WPA2 забезпечує більш високий рівень захисту мережі, тому що TKIP дозволяє створювати ключі довжиною до 128 біт, а AES –до 256 біт. Також у ньому застосовуються більш довгий вектор ініціалізації й криптографічна контрольна сума (MIC) для підтвердження цілісності пакетів.

Збільшення надійності захисту інформації можливе за рахунок використання комплексного підходу до вказаної проблеми.

**Література**

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009. – 276с.

2. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. — М.: Вильямс, 2002. – С. 432. – ISBN 0-201-61599-1.

3. Груздева С.Л., Нахаева Ю.С. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам./ Под. редакцией А.А. Шелупанова, = Authentication. Theory and practice of ensuring access to information resources.. – М.: Горячая линия – Телеком, 2009. – С. 552.

4. Шнайер Б.Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

Надійшла 30.11.2016 р. Рецензент: д.т.н., доц. Казакова Н.Ф.