УДК 3.007.3

Класифікація механізмів аутентифікації користувачів і їх огляд

Клопотовський Д.О., д.т.н., проф. Писаренко Л.Д.

Під час роботи над дипломним проектом, постало завдання класифікації існуючих механізмів аутентифікації, щоб можна було чітко відрізняти аналізовані системи авторизації.

Після аналізу існуючої інформації в Інтернеті, а також серед публікацій, виявилося, що загальної та, водночас, зручної класифікації не існує. Також було виявлено, що ніякої загальноприйнятої класифікації немає, і у кожного автора вона своя, якщо вона взагалі є. Тому була створена дана класифікація.

Провівши аналіз існуючих механізмів аутентифікації користувачів було виділено 3 основних характеристики, якими володіє кожен з них (Рис. 1.).

Ступінь автоматизації

Ступінь автоматизації – автоматизація може бути повною, або неповною. Мається на увазі автоматизація аутентифікації з боку системи, а не користувача. Наприклад, система аутентифікації більшості сайтів повністю автоматизована, а система аутентифікації за допомогою домофона, в повному обсязі, тому що для аутентифікації гостя необхідне втручання господаря.

Рис. 1 Основні характеристики

Пріоритет використання

Пріоритет використання - це те, в якому порядку користувач користується даними способом аутентифікації.

Основний метод аутентифікації:

Як видно з назви, цей метод використовується для штатного входу в систему. Найпоширеніший з них - вхід за паролем, який використовується в переважній більшості комп'ютерних систем. Менш поширеним способом є використання апаратних ідентифікаторів, на які записуються ключі доступу або призначені для користувача паролі.

Також в корпоративному секторі популярна двухфакторная аутентифікація. Як правило, під цим розуміється зв'язка з е-токена і пін-коду, що вводиться користувачем, але зустрічаються і більш екзотичні поєднання, що складаються з біометричного сканера і апаратного ідентифікатора або паролю [1].

Резервний метод аутентифікації:

У разі втрати пароля або е-токена, або взлому облікового запису в силу вступають резервні методи аутентифікації. Найбільш поширені два методи: відповідь на «секретне питання» і відправка пароля на довірену поштову скриньку, вказану при реєстрації.

Є багато цікавих модифікацій даного способу аутентифікації. Наприклад, одним з перших була пропозиція використовувати власні «секретні питання» [1]. Що було, практично негайно реалізовано у провідних провайдерів [2].

Як було сказано на початку, другим способом є відсилання пароля на довірену поштову скриньку. Слід додати, що так як поштова скринька є не основною, то використовується вона рідше, а тому ймовірність забути пароль або відповідь на «секретне питання» стає набагато вище. У багатьох провайдерів з'явилася можливість відправляти нові паролі за допомогою sms повідомлень. Вперше ця система була використана банками для додаткової аутентифікації транзакцій [4, 5], після чого довівши свою ефективність, була перейнята іншими інтернет сервісами. Але і у такий системи є свої недоліки, властиві всім апаратним ідентифікаторам. Телефони дуже часто губляться, крадуться або ламаються. Наприклад, в статті 2008 року, повідомляється про те, що тільки в нью-йоркських таксі щорічно забувається більше 60 000 мобільних апаратів [6].

last-resort механізм («останньої інстанції»):

Незважаючи на всі мінуси і слабкості таких механізмів резервного відновлення доступу до облікових записів, провідні інтернет компанії змушені ними користуватися, Це механізм, до якого вдаються в самих крайніх випадках, коли всі інші способи виявилися безсилі. В даний момент це означає звернення до адміністраторів інформаційних систем, або в спеціальні відділи підтримки клієнтів. Але навіть такі відділи практично беззахисні перед соціальною інженерією, про що писав ще легендарний хакер Кевін Митник в 2002 році у своїй книзі [7]. Він справедливо вказує, що людина буде найслабшою ланкою навіть у найскладнішій системі захисту.

Використовуємий фактор аутентифікації

Використовуємий фактор аутентифікації - аутентифікація являє собою процес порівняння інформації, що надається користувачем, з еталонною. Залежно від типу інформації її можна віднести до одного з чотирьох основних факторів, або до їх комбінації.

Фактор знання (Парольна аутентифікація) - «те, що ти знаєш».

Перший і найпоширеніший на даний момент механізм аутентифікації, введення чогось, що відомо тільки користувачеві, наприклад, пароля або відповіді на секретне питання.

По-перше користувачі, як правило, задають слабкі паролі, що пов'язано з самою фізіологією людини, точніше її мозку. Наше мислення асоціативно і безпосередньо пов'язане з мовою, ми мислимо образами, кожен з яких має назву, тому в якості пароля ми вибираємо назву одного з них. Таким чином більшість паролів, що задаються користувачами ми можемо знайти в звичайному словнику, а тому вони легко підбираються методом перебору по словнику.

До того ж, з ростом складності пароля він все важче для запам'ятовування. Дослідження SafeNet від 2004 року виявило, що 47% респондентів забували свої паролі протягом року [8]. А з ростом кількості облікових записів від різних комп'ютерних систем, яких з кожним роком стає все більше, ситуація ще більш ускладнюється. Здатність запам’ятовувати паролі була вивчена в лабораторії By в 2007 році. Після першого тижня 12.5% учасників забули їх шести символьні буквено-цифрові паролі. З учасників, які повинні були пам'ятати паролі про п'ять облікових записів, 25% забули принаймні один [9].

Крім того, зі збільшенням складності паролів збільшується і кількість помилок при його введенні.

Дослідження, проведене Джоном Лейдоном в 2003 році, виявило страшну схильність офісних працівників повідомляти свої паролі незнайомцям за символічну плату. У дослідженні взяло участь 152 людини. Їм була задана серія питань, один з яких просив вказати пароль користувача, і 75% опитаних негайно його назвали. Вони розкрили свій пароль в обмін на дрібничку вартістю менше одного фунта стерлінгів [10].

Наступний за поширеністю механізм аутентифікації зазвичай використовують якщо пароль все-таки втрачено. Тоді користувача просять відповісти на так зване «секретний питання», відповідь на яке він вказав при реєстрації облікового запису.

Однак, криптостійкість подібних «питання і відповідь», які обирають користувачі, ще менше, ніж у обираних ними паролів. У 2009 році на конференції IEEE Security and Privacy була опублікована доповідь про дослідження, в якому взяло участь 130 осіб. Результати показали, що трохи менше третини випробуваних - 28 відсотків - змогли «вгадати» відповідь на секретний пароль, в разі якщо близько знали свого опонента. Якщо ж опонент був повністю незнайомий, то відповідь на питання вгадали 17 відсотків випробовуваних. Втім, кінцевий результат багато в чому залежить від складності поставленого питання. Навіть на питання особистого характеру - місце

народження, або кличка домашнього вихованця - крадій дає правильну відповідь в 45 і 40 відсотків випадків відповідно. Аналогічні роботи проходили і раніше в 1996-му [11] і в 1990-му [12] роках. Вони теж досліджували здатність запам'ятовувати і вгадувати відповіді на «секретні питання». І показали схожі результати, а саме: подружжя та близькі друзі могли вгадати 33% -39% відповідей, а 20% -22% забули свої відповіді протягом 3-х місяців.

Цікава роботи була опублікована не так давно. Її метою було з'ясувати криптостійкість відповідей на «секретні питання» самі по собі. З цією метою автори зібрали величезну базу даних (порядку 269 млн.) Імен, прізвищ, прізвиськ домашніх тварин, дат і місць народження користувачів. При аналізі цих даних з'ясувалося, що вони підкоряються розподілу Ціпфа, окремим випадком якого є «закон Парето», тобто на 20% імен і дат доводилося 80% користувачів. В результаті, виявилося, що криптостійкість відповідей на дані «секретні питання» відповідає криптостійкості ключа шифрування довжиною від 8 до 23 біт, в залежності від поширеності конкретного імені або прізвища [13].

У 2005 році В. Гріффін і М. Якобсон провели дослідження виявило, що відповіді на найпопулярніші «секретні питання» можна знайти у відкритих джерелах.

Матеріальний фактор (Апаратна аутентифікація) - «те, чим ти володієш». В першу чергу під цим розуміються апаратно-програмні системи ідентифікації і аутентифікації (СІА) або пристрої введення ідентифікаційних ознак [14]. До складу СІА входять апаратні ідентифікатори, пристрої введення-виведення (зчитувачі, контактні пристрої, адаптери, роз'єми системної плати та ін.) І відповідне ПО. Ідентифікатори призначені для зберігання унікальних ідентифікаційних ознак. Крім цього, вони можуть зберігати і обробляти конфіденційні дані. Пристрої введення-виведення і ПО здійснюють обмін даними між ідентифікатором і захищаємою системою.

В електронних СІА ідентифікаційні ознаки представляються у вигляді цифрового коду, що зберігається в пам'яті ідентифікатора. За способом обміну даними між ідентифікатором і пристроєм введення-виведення електронні СІА поділяються на:

1. контактні:

- iButton - information button - інформаційна «таблетка»;
- смарт-карти - інтелектуальні карти;
- USB-ключі або USB-токени (token - розпізнавальний ознака, маркер);

2. безконтактні:

- RFID-ідентифікатори - radio-frequency identification - радіочастотні ідентифікатори;
- смарткарти.

Контактне зчитування має на увазі безпосереднє зіткнення ідентифікатора з пристроєм вводу-

виводу. Безконтактний (дистанційний) спосіб обміну не вимагає чіткого позиціонування ідентифікатора і пристроя введення-виведення. Читання або запис даних відбувається при піднесенні ідентифікатора на певну відстань до пристрою введення-виведення.

СІА на базі смарт-карт і радіочастотних ідентифікаторів можна віднести за часом їх створення до старшого, iButton - до середнього, а USB-ключів - до молодшого покоління.

Під час обговорення надійності СІА зазвичай розглядають найважливішу і в той же час найслабшу ланку системи - ідентифікатор. У свою чергу, надійність ідентифікаторів пов'язують зі ступенем їх захищеності від механічних впливів, впливу температури, зовнішніх електромагнітних полів, агресивних середовищ, пилу, вологи, а також від атак, спрямованих на розкриття чіпів, що зберігають секретні дані.

До недоліків СІА на базі iButton слід віднести відсутність вбудованих в ідентифікатори криптографічних засобів, що реалізують шифрування даних при їх зберіганні і передачі в комп'ютер. Тому iButton зазвичай використовується спільно з іншими системами, на які покладаються функції шифрування.

Звичайно, за ступенем механічної надійності радіочастотні ідентифікатори, смарт-карти і USB-ключі поступаються iButton. Проведені в ході реалізації французького проекту GIE Carte Bancaire десятирічні дослідження над 22 мільйонами карт показали, що ймовірність їх відмови по ряду причин (куди також входять механічні пошкодження) становить 0,022.

«Вузьким» місцем USB-ключів є ресурс їх USB-роз'ємів. Розробники даних ідентифікаторів навіть включають цей показник в технічні специфікації виробів. Наприклад, для ідентифікаторів сімейства eToken гарантоване число підключень становить не менше 5000 разів.

Перевага радіочастотних ідентифікаторів, смарт-карт і USB-ключів полягає в тому, що в їх склад входить захищена незалежна пам'ять і криптографічний процесор, що дозволяють підвищити рівень захисту пристроїв. Однак, опубліковано безліч робіт, в яких описуються різноманітні атаки на чіпи ідентифікаторів. Ці дослідження носять як теоретичний, так і практичний характер. До теоретичних методів розкриття відносять, зокрема, атаки Bellcore, диференційний аналіз спотворень DFA (Differential Fault Analysis) і живлення DPA (Differential Power Analysis). До практичних методів можна віднести глітчінг (glitching) і фізичні атаки, спрямовані на розпакування чіпа і вилучення необхідної інформації.

Розробники криптографічних процесорів прагнуть у міру можливості адекватно реагувати на атаки за допомогою різноманітних механізмів зовнішнього та внутрішнього захисту. До механізмів

зовнішнього захисту відносять установку датчиків (ємнісний або оптичний сенсор), покриття чіпа металевим шаром, спеціальними клеями і т. д., До внутрішніх - шифрування шини, випадкове тактування, проведення повторних обчислень, генерування шуму.

Загалом, через вартість апаратних ідентифікаторів, вони застосовуються в основному в бізнесі, там де потрібні зручність, надійність і висока криптостійкість. Основних мінусів всього два: їх можна відняти або втратити і вони можуть зламатися.

Біофактор (Біометрична аутентифікація) - «те, що є частиною тебе». Біометричні дані, для зняття яких, як правило, необхідні спеціальні програмно-апаратні засоби - так звані, біометричні сканери, які розрізняються за характером зчитувальних даних.

Біометричні сканери, засновані на статичних методах:

- Розпізнавання за відбитками пальців. Це - найпоширеніший статичний метод біометричної ідентифікації, в основі якого лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетвориться в цифровий код (згортку) і порівнюється з раніше введеним шаблоном (еталоном) або набором шаблонів;
- Розпізнавання за райдужною оболонкою ока. Цей метод розпізнавання заснований на унікальності малюнка райдужної оболонки ока. Для реалізації методу необхідна камера, що дозволяє отримати зображення ока людини з достатньою роздільною здатністю, і спеціалізоване програмне забезпечення, що дозволяє виділити з отриманого зображення малюнок райдужної оболонки ока, за яким будується цифровий код для ідентифікації людини.

Біометричні сканери, засновані на динамічних методах:

- Розпізнавання по рукописному почерку. Як правило, для цього динамічного методу ідентифікації людини використовується його підпис (іноді написання кодового слова). Цифровий код ідентифікації формується за динамічними характеристиками написання, тобто для ідентифікації будується згортка, в яку входить інформація по графічним параметрам підпису, тимчасовим характеристикам нанесення підпису і динаміка натиску на поверхню в залежності від можливостей обладнання (графічний планшет, екран кишенькового комп'ютера і т. д .);
- Розпізнавання по клавіатурному почерку. Метод в цілому аналогічний вищеописаному, однак замість підпису в ньому використовується якесь кодове слово, а з обладнання потрібно тільки стандартна клавіатура. Основна характеристика, за якою будується згортка для

ідентифікації, - динаміка набору кодового слова;

- Розпізнавання по голосу. В даний час розвиток цієї однієї з найстаріших технологій прискориіся, так як передбачається її широке використання при спорудженні інтелектуальних будівель. Існує досить багато способів побудови коду ідентифікації по голосу: як правило, це різні поєднання частотних і статистичних характеристик останнього.

Висновки

Був проведений загальний аналіз існуючих систем авторизації та аутентифікації. Отримано загальну класифікацію методів, їх переваги та недоліки у порівнянні з іншими. Дана інформація може бути корисною при розробці систем авторизації в цифрових комплексах, за для класифікації обраних методів, чи за для вибору найоптимальніших методів захисту у своїх системах. При написанні цієї статті було виділено декілька дуже важливих факторів. Одним з яких є те, що в будь якій системі авторизації найслабкішою ланкою є людина.

Література

1. M. Just. Designing authentication systems with challenge questions. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Use, , Sebastopol, CA, 2005. O'Reilly Media, Inc. - C 143–155

2. B. Sullivan. 'forgot your password?' may be weakest link. MSNBC Red Tape Chronicles, Aug. 26, 2008. URL: redtape.msnbc.com/2008/08/almost-everyone.html

3. M. Jakobsson, E. Stolterman, S. Wetzel, and L. Yang. Love and authentication. In CHI '08: Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2008. ACM. -C 197–200

4. T. Pullar-Strecker. NZ bank adds security online. Sidney Morning Herald, 8 November 2004. Referenced 2006 at www.smh.com.au.

5. CommonwealthBank. NetBank NetCode SMS, 2008. URL: www.commbank.com.au/netbank/netcodesms.

6. CREDANT Technologies. Mountains of mobiles left in the back of New York cabs, 16, 2008. URL: www.credant.com/mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html.

7. K. D. Mitnick and W. L. Simon. The Art of Deception: Controlling the Human Element of Security. Wiley, 2002

8. SafeNet, Inc. 2004 annual password survey results, 2005. URL: www.safenet-

inc.com/news/view.asp?newsID=239.

9. K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, J. Cook, and E. E. Schultz. Improving password security and memorability to protect persona and organizational information. Int. J. Hum.-Comput. Stud., 65(8): 2007. -C 744–757

10. S. Brostoff and A. M. Sasse. Ten strikes and you're out: Increasing the number of login attempts can improve password usability. In Proceedings of CHI 2003 Workshop on HCI and Security Systems, 2003.

11. J. Leyden. Office workers give away passwords for a cheap pen. The Register, 18 April 2003. Referenced 2006 at www.theregister.co.uk.

12. J. Podd, J. Bunnell, and R. Henderson. Cost-effective computer security: Cognitive and associative passwords. In OZCHI '96: Proceedings of the 6th Australian Conference on Computer-Human Interaction (OZCHI '96), сторінка 304, Washington, DC, USA, 1996. IEEE Computer Society.

13. M. Zviran and W. J. Haga. User authentication by cognitive passwords: an empirical assessment. In JCIT: Proceedings of the Fifth Jerusalem Conference on Information technology, Los Alamitos, CA, USA, 1990. IEEE Computer Society Press.

14. Joseph Bonneau, University of Cambridge, Mike Just, Greg Matthews, What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions. In Financial Cryptography and Data Security '10, -C 137–144