SEKCJA 18. TECHNIKA.(ТЕХНИЧЕСКИЕ НАУКИ)
ПОД- СЕКЦИЯ 3. Информатика, вычислительная техника и автоматизация.

Онищенко Ю.М.
кандидат наук з державного управління
Харківський національний університет
внутрішніх справ
Кобзев І.В.
доцент, кандидат технічних наук
Харківський регіональний інститут
Національної академії державного управління
при Президентові України
Мордвинцев М.В.
доцент, кандидат технічних наук
Харківський національний університет
внутрішніх справ

МЕХАНІЗМИ БЕЗПЕКИ ЕЛЕКТРОНИХ СЕРВІСІВ

Ключові слова: електронний сервіс, електронний підпис, безпека, аутентифікація, кіберзлочин, авторизація

Keywords: electronic services, electronic signature, security, authentication, cybercrime, authorization

З ростом привабливості електронних сервісів для користувачів стала рости і їх привабливість для кіберзлочинців, що мають хорошу підготовку в області інформаційних технологій і шукають наживу в мережі Інтернет.

Додатковий інтерес кіберзлочинців до електронних сервісів підігрів Закон України від 22.05.2003 № 852 — IV «Про електронний цифровий підпис» (потокова редакція — Редакція від 28.06.2015) [1], порядок застосування електронного підпису (далі — ЕП), що визначив, для надання юридичної значущості електронним документам. Закон, з одного боку, надав розробникам електронних сервісів можливість робити ширший спектр послуг, дозволяючи користувачам електронних сервісів видалено підписувати договори, угоди, доручення, заявки, ставши свого роду драйвером для розвитку і впровадження технологій ЕП в різні електронні сервіси. З іншого боку, Закон притягнув увагу кіберзлочинців, оскільки підробка підписів під електронними документами є для них потенційним способом здійснення шахрайських дій з метою крадіжки грошових коштів. Зокрема, підробка платіжного доручення в системах дистанційного банківського обслуговування може дозволити кіберзлочинцям вкрасти грошові кошти з рахунків клієнтів банків, а підробка підпису під електронним договором дарування майна може дозволити шахраям незаконно оволодіти майном і так далі.

У дослідженні «Фінансові наслідки кіберзлочинів» за 2015 рік, проведеному Ponemon Institute за підтримки HP Enterprise Security, представлено дані про щорічні витрати на усунення наслідків кібератак для компаній в США, Великобританії, Японії, Німеччині, Австралії, Бразилії і Росії. Згідно з цими відомостями, в американських компаніях збиток від кіберзлочинів склав 15 млн. доларів США [2].

Очевидно, що розвиток електронних сервісів триватиме, причому активно і динамічно. І електронний підпис завдяки своїм очевидним перевагам, незважаючи на загрози кіберзлочинців, впроваджуватиметься у все більшу кількість сервісів і систем електронного документообігу. У зв'язку з цим питання забезпечення безпеки таких сервісів і систем стає вже не додатковим, а пріоритетним при розробці Web–застосувань і хмарних сервісів.

Серед основних завдань безпеки, які необхідно вирішити для Web-сервісів, можна виділити наступні:

- забезпечити безпечний вхід користувача в особистий кабінет на видаленому сервері. При цьому треба перевірити достовірність як користувача, так і сервера;
- реалізувати можливість безпечного формування і перевірки електронного підпису для забезпечення юридичної значущості електронної взаємодії;
- забезпечити конфіденційність даних, що передаються по каналу зв'язку.
- При використання криптопровайдера для вирішення цих завдань виникають проблеми наступного характеру:
- від користувачів потрібні навички установки і налаштування спеціального програмного забезпечення (ПЗ) для роботи з додатками;
- необхідна прив'язка користувачів до конкретного ПК, на якому встановлений криптопровайдер і наявність прав локального адміністратора операційної системи;
- при перевстановленні операційної системи вимагається наново проводити установку і налаштування ПЗ.

На сьогоднішній день користувачі стали вимогливішими, мобільнішими і звикли працювати з додатками як сервісами, до яких можна отримати доступ з будь-якого пристрою, на якому є браузер і доступ в Інтернет, без накладення додаткових обмежень і необхідності установки спеціального криптографічного ПЗ.

Наприклад для підвищення безпеки різних електронних сервісів альянс FIDO пропонує перехід на двофакторну систему аутентифікації користувачів.

Учасники альянсу, до числа яких входять такі компанії, як Infineon, PayPal і Lenovo, відмічають, що сьогодні кіберзлочинці використовують паролі як одне з найбільш вразливих місць електронних систем [3].

При використанні одноразових паролів слід враховувати, що: використання SMS–повідомлень для доставки одноразових паролів не є абсолютно безпечним, оскільки SMS можуть бути перехоплені; картки одноразових паролів можуть бути вкрадені і скомпрометовані; генератори одноразових паролів також не завжди є безпечними.

Більше того, використання одноразових паролів не забезпечує можливість підписання електронних документів для надання їм юридичної значущості, а також не вирішує задачу забезпечення цілісності і конфіденційності даних, переданих по каналу зв'язку.

Для забезпечення цілісності і конфіденційності даних ряд Web-сервісів на додаток до одноразових паролів використовує вбудований у браузери протокол HTTPS з вбудованими криптоалгоритмами.

Проте такий підхід не завжди застосовний зважаючи на законодавчі обмеження по обробці персональних даних, банківської таємниці, захисту даних в дер-

жавних інформаційних системах і в інших випадках, коли потрібний захист конфіденційності даних відповідно до законодавства.

Більше того, нещодавно стало публічно відомо, що деякі спецслужби вже давно уміють читати дані, захищені західними криптоалгоритмами в HTTPS-протоколі стандартних браузерів. А значить не виключено, що це під силу і кіберзлочинцям. У зв'язку з цим використання надійних алгоритмів для шифрування є надійнішим при захисті конфіденційних даних.

Надійна аутентифікація є одним з ключових елементів системи інформаційної безпеки. Не знаючи, хто саме має доступ до конфіденційних даних, і чи являється цей «хтось» тим, за кого себе видає, неможливо побудувати ефективну, прозору і керовану систему захисту інформаційних ресурсів.

Вимоги до надійності, типу, технології і засобів аутентифікації залежать від важливості оброблюваної інформації, прав і повноважень адміністраторів і користувачів системи, вірогідності інциденту і визначаються на основі аналізу ризиків можливого збитку (фінансового, репутаційного, організаційного).

На вибір типу аутентифікації сильно впливають права і повноваження користувача в системі (керівник, Топ-менеджер, адміністратор), а також сценарії роботи (видалений користувач, мобільний користувач, робота з домашнього комп'ютера та ін.).

Добре зарекомендувала себе двофакторна аутентифікація, в процесі якої використовуються аутентифікаційні чинники двох типів. Наприклад, користувач повинен надати смарт-карту і ввести пароль. В цьому випадку зловмисник не зможе отримати доступ до даних, оскільки йому доведеться не лише підглянути пароль, але і пред'явити фізичний пристрій, крадіжка якого, на відміну від крадіжки пароля, практично завжди швидко виявляється.

Проте найбільш надійним і безпечним способом упевнитися в тому, що «хтось» є саме тим, за кого себе видає, виступає технологія строгої аутентифікації. При строгій аутентифікації користувач повинен довести, що має заздалегідь отриманим безпечним способом секрет (закритим криптографічним ключем). В процесі доказу сторони в захищеному режимі обмінюються послідовно підписаною інформацією. Строга аутентифікація не допускає підробки або клонування персонального секрету, яким є закритий криптографічний ключ.

Для строгої аутентифікації необхідно використовувати криптографію і інфраструктуру відкритих ключів (Public Key Infrastructure – PKI). Інші методи і технології здатні забезпечити лише просту або посилену аутентифікацію.

У PKI-інфраструктурі тільки апаратні рішення – смарт-карти, USB- і MicroSD-токени на основі спеціалізованого захищеного мікроконтроллера, які апаратно реалізують криптографічні алгоритми, – в змозі надійно захистити закритий криптографічний ключ користувача навіть при роботі в небезпечних середовищах.

При строгій аутентифікації використовуються, як мінімум, два чинники аутентифікації різних типів: перший чинник – володіння USB-токеном або смарт-картою; другий чинник – знання PIN-коду для виконання криптографічних операцій усередині токена.

При доступі до критично важливої інформації рекомендується використовувати додатковий третій чинник аутентифікації – біометричну ідентифікацію власника токена, що робить неможливим використання пристрою без його власника.

При впровадженні в Україні електронних сервісів оптимальним варіантом для ідентифікації клієнтів може являтися банківська ідентифікація.

У Україні запустили пілотний проект універсальної електронної ідентифікації громадян через банківські дані [4]. Проект вирішуватиме питання верифікації користувача через Інтернет для надання довідок, дозвільних та інших документів в електронному вигляді.

Суть технології проста: банки країни об'єднуються в деяку систему, яка дозволяє проводити видалену ідентифікацію, умовно кажучи, Інтернет-банкінг. Наприклад, щоб отримати довідку на державному порталі, Вам досить ввести пароль Інтернет-банкінгу вашого банку і, скажімо, SMS-пароль (щось схоже, до речі, дозволяє робити Facebook). При обранні громадянином верифікації особини через BankID достатньо ввести логін та пароль свого Інтернет -банку, пройти через другий етап авторизації шляхом введення SMS-паролю — і отримати доступ до переліку електронних послуг.

Література

1. Про електронний цифровий підпис Верховна Рада України; Закон України від 22.05.2003 № 852-IV / [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/852-15
2. Cost of Cyber Crime Study: United States / Ponemon Institute // [Електронний ресурс]. – Режим доступу до ресурсу: http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states
3. Новая система безопасности сделает кражу паролей бесполезной / [Електронний ресурс]. – Режим доступу до ресурсу: http://news.tts.lt/?r=oldie%2Farticle&section_id=5&article_id=18355
4. В Україні запускають універсальну електронну ідентифікацію громадян BankID / [Електронний ресурс]. – Режим доступу до ресурсу: http://www.imena.ua/blog/bank-id/