УДК 681

КОМБІНОВАНА ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ

М.Ф. БОНДАРЕНКО, П.О. КРАВЧЕНКО

Пропонується комбінована інфраструктура, що володіє перевагами як над традиційною ІВК, так і ІВК на ідентифікаторах.

The papers proposes a combined public key infrastructure that has advantages over both traditional and identity-based public key infrastructures.

ВСТУП

На сьогоднішній день для забезпечення захищеного документообігу використовуються інфраструктури відкритих ключів. Існуюча ІВК використовується у багатьох країнах і вже зарекомендувала себе як надійне рішення. Традиційна інфраструктура відкритих ключів є перевіреною часом та ґрунтується на надійному математичному апараті, витримала багато перевірок широкого кола експертів. Криптопримітиви та протоколи, що використовуються у ній, є стандартизованими, процес впровадження та експлуатації – добре налагоджений та прогнозований. Але подальший розвиток інфраструктур відкритих ключів призводить до необхідності підвищення кількісних та якісних показників, насамперед вартості та складності впровадження і використання. На сьогоднішній день вартість одного сертифікату відносно висока, а процес взаємодії користувачів один з одним та з центрами сертифікації не досить прозорий та вимагає від них хоча б базових знань. Це призводить до багатьох помилок з боку користувачів та значної вартості впровадження електронного документообігу на підприємстві. Вирішення питання зниження вартості та складності багато хто бачить у якісній зміні існуючої архітектури, тому що підвищення ефективності неможливе лише за рахунок деяких оптимізацій.

Однією з найважливіших проблем, вирішенням якої займається багато дослідників, є отримання поточного статуса сертифіката відправником зашифрованого повідомлення. Ця проблема відома як “certificate revocation problem”. Для вирішення її необхідна інфраструктура. На сьогодні існує два підходи - CRL (список відкликаних сертифікатів) та OCSP (онлайн протокол перевірки статусу сертифіката). Підхід з використанням CRL дуже громізкий для центрів сертифікації з великою кількістю користувачів. Це пов’язано з необхідністю надання цього списку кожному, хто хоче перевірити статус сертифіката. До того ж, процедура обміну цими списками між різними центрами сертифікації та перевірка користувачем листів відкликаних сертифікатів інших центрів сертифікації є складною. Використання OCSP передбачає підписану відповідь центра сертифікації на кожний запит щодо статусу конкретного сертифіката, що призводить до підвищення навантаження на криптографічні модулі. Також у цьому разі центр сертифікації стає вразливим до DoS атак.

Один зі шляхів вирішення проблем з необхідністю отримання статусу сертифіката запропонував Gentry [1]. Взагалі, його ідея полягає в розділенні таємного ключа користувача на дві частки - одна зберігається у користувача, інша обчислюється цетром сертифікації для кожної процедури розшифрування. Центр сертифікації надає цей частковий таємний ключ користувачу на вимогу. Таким чином, відправник повідомлення не повинен перевіряти статус сертифіката одержувача. Взагалі ця модель отримала назву CBE (certificate-based encryption). Було розроблено багато різновидів цієї схеми [].

Одним зі шляхів вирішення проблеми з оновленням статусу сертифіката є використання іншої інфраструктури. Але інфраструктура відкритих ключів на базі ідентифікаторів, яку вважають заміною традиційної ІВК, також має деякі особливості. Її впровадження тільки починається, активно розробляє та впроваджує цю інфраструктуру тільки компанія Voltage Security [2]. До її переваг відносять відсутність необхідності у використанні сертифікатів відкритих ключів, зручність для користувачів, низьку вартість впровадження. Так, наприклад, компанія Ferris Research підрахувала, що вартість впровадження та використання інфраструктури відкритих ключів на базі ідентифікаторів у середньому у три рази нижче, ніж для традиційної ІВК. Звісно, це дуже привабливо для компаній, що планують впровадження електронного документообігу. Однак, ІВК на ідентифікаторах володіють суттєвими недоліками, що уповільнюють її впровадження та звужують сферу застосування. Найголовніші з них – необхідність високого рівня довіри кожного користувача до уповноваженого на генерацію ключів та потрібність у захищеному каналі для передачі таємних ключів від уповноваженого до користувача. Очевидно, що інфраструктура, що володіє такими недоліками, не може використовуватися у глобальних мережах. Також важливими особливостями є використання малодослідженого математичного апарату, відсутність міжнародних стандартів (першими розробками у цій галузі є RFC 5408 та IEEE P1363.3) та низький рівень впровадження.

Аналіз переваг традиційної ІВК та ІВК на ідентифікаторах показує, що кожну з них доціль-

но використовувати у різних сферах [3,4,5]. Традиційну інфраструктуру відкритих ключів доцільно застосовувати на глобальному рівні (де вона й успішно використовується), ІВК на ідентифікаторах можна використовувати на рівні компаній та підприємств. До такого підходу вдалася й вищезгадана Voltage Security, яка впроваджує цю інфраструктуру у конкретних компаніях (Integro Insurance Brokers, ING Canada, Kodac та ін.). Вже були запропоновані рішення, які дозволяють поєднати переваги цих інфраструктур та поєднати глобальний рівень та рівень компанії у єдину інфраструктуру.

СВЕ схеми, ідея яких була описана вище, поєднують у собі обидва підходи – користувач володіє парою таємний/відкритий ключ та сертифікатом, але центр сертифікації використовує схему на ідентифікаторах (ІВЕ) для його формування. Також користувач отримує від центра сертифікації частковий сертифікат, необхідний для кожної процедури розшифрування. Очевидно, що це призводить до певних проблем – сервер повинен кожен раз обчислювати та надавати користувачу частковий таємний ключ (користувач не може розшифрувати повідомлення без запиту на сервер).

1. КОМБІНОВАНА ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ

Сутність комбінованої ІВК полягає в об'єднанні процедури сертифікації відкритого ключа користувача та механізмів шифрування на ідентифікаторах. Загальна схема зображена на рис. 1.

1. Користувач отримує ПО у центрі сертифікації.

2. Користувач генерує таємний ключ s та свій відкритий ключ sP.

3. Користувач відправляє у центр сертифікації ідентифікатор ID, відкритий ключ sP та час *t*, що визначає період дії відкритого ідентифікатору.

4. Центр сертифікації видає користувачу сертифікат, у якому зазначаються його ідентифікатор ID, відкритий ключ sP та період *t*.

Тепер користувач володіє як парою таємний – відкритий ключ, що може бути використана у традиційній ІВК, так і ключем для інфраструктури відкритих ключів на ідентифікаторах.

2. СХЕМА ВЗАЄМОДІЇ КОРИСТУВАЧІВ

Розглянемо детально схему взаємодії користувачів на прикладі направленого шифрування (рис. 2).

Схема направленого шифрування складається з наступних п'яти ритмів:

Setup. Алгоритм отримує на вхід параметр безпеки $k \in Z^+$.

Алгоритм генерує просте q, дві групи G_1, G_2 порядку q та білінійне відображення $\hat{e}: G_1 \times G_1 \to G_2$. Вибирається генератор групи $P \in G_1$.

Вибирається криптографічна геш-функція $H_1 : \{0,1\}^* \to G_1^*$. Вибирається криптографічна геш-функція $H_2 : G_2 \to \{0,1\}^n$ для деякого n.

Вибирається випадкове $s_{CA} \in Z_q^*$ як таємний ключ та обчислюється $P_{PUB} = s_{CA} P$ - відкритий ключ.

Системними параметрами будуть

$$< q, G_1, G_2, \hat{e}, n, P, P_{PUB}, H_1, H_2 > .$$

SetKeyPair. Вибирається випадкове $s_1 \in Z_q^*$ як таємний ключ користувача та обчислюється РК = $= s_1 P$ – відкритий ключ.

Certify. Вхідні дані $< s_1 P, t, ID_{s1} >$ підписуються на таємному ключі s_{CA} та формується сертифікат Cert.

Encrypt. Для за шифрування повідомлення M на відкритому ключі ID_{s1}, (1) обчислюється $Q_{ID} = H_1(ID) \in G_1^*$ та (2) вибирається випадкове $r \in Z_q^*$ та (3) обчислюється криптограма за допомогою наступної формули $< rP,\ M \oplus H_2(\hat{e}(s_1 P,\ H_1(ID_{s1}))^r) >$, де $s_1 P, ID_{s1}$ –

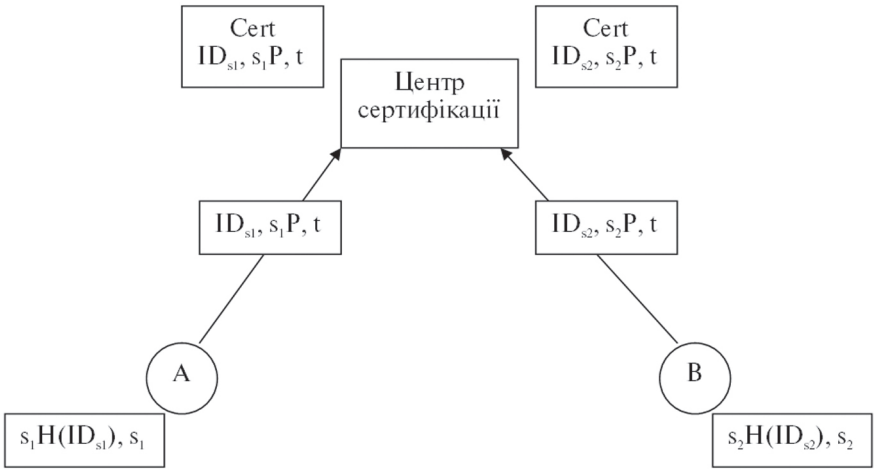

Рис. 1. Схема генерації ключів. Центр сертифікації генерує та розповсюджує загальні параметри (еліптична крива, базова точка та її порядок, кофактор та ін.)

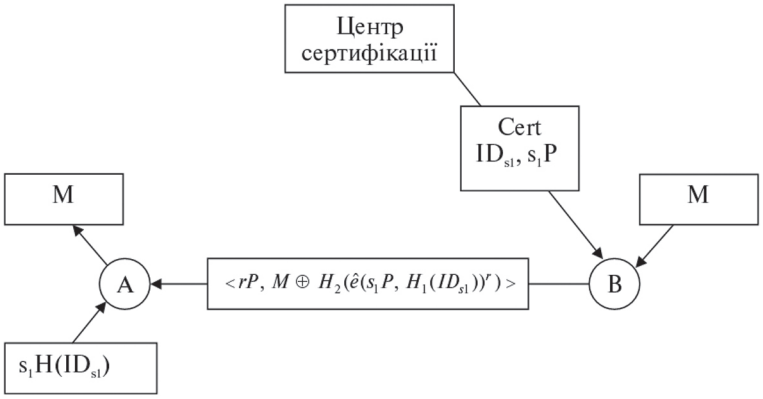

Рис. 2. Схема направленого шифрування

відкритий ключ та відкритий ідентифікатор одержувача відповідно.

Decrypt. Для вхідного зашифрованого повідомлення $C = <U, V>$, яке було зашифроване на відкритому ідентифікаторі ID_{s1}, повідомлення отримується за наступною формулою: $M = V \oplus H_2(\hat{e}(U, s_1 H(ID_{s1})))$, де $U = rP$.

Коректність схеми легко перевірити:

$$(\hat{e}(s_1 P, H_1(ID_{s1}))^r = (\hat{e}(rs_1 P, H_1(ID_{s1}))) =$$
$$= (\hat{e}(rP, s_1 H(ID_{s1}))).$$

До переваг нашої схеми можна віднести:

1. Інфраструктура практично повністю сумісна з існуючою ІВК та ІВК на ідентифікаторах.
2. Користувач сам генерує собі таємний ключ (інфраструктури на ідентифікаторах).
3. Відкритий ідентифікатор засвідчується у сертифікаті, відповідний таємний ключ може змінюватися багато разів за час існування сертифікату.
4. Застосування відомих сертифікованих протоколів.

ВИСНОВКИ

Запропонована комбінована інфраструктура, на наш погляд, володіє перевагами як традиційної ІВК, так і ІВК на ідентифікаторах і може бути застосована при побудові реальних систем. Користувач може змінювати свій таємний ключ багато разів за час дії сертифікату, що суттєво знижує імовірність його компрометації. Таємний мастер-ключ користувача s буде використовуватися лише для обчислення таємних ключів ІВК на ідентифікаторах. Таким чином, реально в системі будуть використовуватися механізми шифрування і підпису на ідентифікаторах. Але в цьому випадку відсутня проблема довіри до центру сертифікації та проблема таємного каналу між користувачем та центром сертифікації, тому що користувач сам генерує собі ключі. До того ж, його відкритий ідентифікатор та час його зміни знаходиться у сертифікаті, що вирішує проблеми відповідності ідентифікатора конкретному користувачу.

Література.

[1] *C. Gentry*. Certificate-based encryption and the certificate revocation problem. DoCoMo USA Labs, 2003.

[2] *Voltage Security*. Identity-Based Encryption and PKI Making Security Work. 2005.

[3] *Jon Callas*. Identity-Based Encryption with Conventional Public-Key Infrastructure. PGP Corporation, USA, 2005.

[4] *Горбенко І.Д., Кравченко П.О.* Комбінована інфраструктура відкритих ключів та її застосування. Радіоелектронні і комп'ютерні системи, 2009, №5.

[5] *Горбенко І.Д., Кравченко П.О.* Аналіз існуючих досліджень в галузі побудови комбінованої ІВК. Прикладная радиоэлектроника, Том 7, №3, 2008. – С. 267-270.

Надійшла до редколегії 16.09.2009

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного університета радіоелектроніки.

Кравченко Павло Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: інфраструктури відкритих ключів.