УДК 681.3.06

АНАЛІЗ ІСНУЮЧИХ ДОСЛІДЖЕНЬ В ГАЛУЗІ ПОБУДОВИ КОМБІНОВАНОЇ ІВК

І.Д. ГОРБЕНКО, П.О. КРАВЧЕНКО

Проводиться аналіз сучасних розробок в галузі побудови інфраструктур відкритих ключів, що поєднують у собі переваги традиційної архітектури та архітектури на ідентифікаторах.

The paper presents analysis of modern developments in the field of constructing public key infrastructures which combine advantages of traditional architecture and idendifier-based architecture.

ВСТУП

Розвиток інфраструктур відкритих ключів призводить до необхідності активних досліджень, особливо в галузі зниження вартості та складності впровадження та використання цих інфраструктур [1, 2]. Вирішення цих проблемних питань неможливо без якісної зміни існуючої архітектури, тому що підвищення ефективності існуючої ІВК неможливе тільки за рахунок деякої оптимізації. Тому існує два можливих шляхи вирішення – зміна архітектури ІВК або застосування комбінованої архітектури. Альтернативна інфраструктура на базі ідентифікаторів, якій зараз приділяють багато уваги, не може прийти на заміну традиційної ІВК, тому що її основні недоліки дуже сильно проявляються у глобальних системах. В основному це стосується проблеми довіри до уповноваженого на генерацію ключів та проблеми надання кожному користувачу унікального загальновідомого ідентифікатора. Тому постійно ведуться дослідження, метою яких є побудова комбінації традиційної ІВК та ІВК на ідентифікаторах. У цій статті ми проаналізували результати, які були отримані розробниками різноманітних комбінованих архітектур.

Традиційна ІВК є широко розповсюдженою, а отже перевіреною часом та грунтується на надійному математичному апараті. Третя довірена сторона не має доступу до таємного ключа користувача. ІВК на ідентифікаторах, навпаки, має невисоку складність та вартість (за рахунок відсутності сертифікатів), але потребує довіри до уповноваженої сторони та має складну політику безпеки.

За результатами аналізу виходить, що традиційна ІВК ефективна для використання на рівні держави та організацій, а ІВК на ідентифікаторах – на рівні локальних мереж організацій. Взагалі можна зробити висновок, що ІВК на ідентифікаторах краще всього підходить для невеликих інформаційних середовищ, та коли є довіра до уповноваженого на генерацію ключів користувачів (у цьому середовищі). Тому ІВК на ідентифікаторах можна поєднати з традиційною ІВК, яка вже є налагоджена. В такому випадку ІВК на ідентифікаторах буде працювати поверх традиційної ІВК, на кінцевому рівні. Така комбінація вбере у себе більшість переваг обох систем.

1. ВИМОГИ ДО КОМБІНОВАНОЇ ІНФРАСТРУКТУРИ

Для того, щоб мати можливість оцінювати запропоновані рішення, необхідно висунути вимоги до інфраструктур відкритих ключів, що будуть поєднувати у собі елементи традиційної ІВК та ІВК на ідентифікаторах або будуть комбінацією цих двох архітектур. Можна висунути безумовні критерії до таких систем, за якими оцінюється можливість застосування таких систем у реальному середовищі та умовні критерії, що показують ступінь переваги однієї архітектури над іншою.

До безумовних критеріїв віднесемо:

1) Програмно-апаратний рівень гарантій, що надаються ІВК;
2) Безпечність протоколів;
3) Уніфікація;
4) Криптоживучість.

Сформулюємо умовні критерії до комбінованої інфраструктури відкритих ключів:

1) Користувачі традиційної ІВК не повинні довіряти уповноваженому на генерацію ключів (УГК);
2) Використання безпечних протоколів;
3) Користувачі ІВК на ідентифікаторах не повинні мати сертифікати;
4) Повинні існувати механізми взаємодії користувачів традиційної ІВК та ІВК на ідентифікаторах;
5) Низьке навантаження на сервери УГК
6) Стан впровадження.

2. АНАЛІЗ РІШЕННЯ КОМПАНІЇ VOLTAGE

Компанія Voltage є провідним постачальником криптосистем на базі ідентифікаторів та володіє багатьма патентами. Вона запропонувала комбінацію IBE та PKI, яка має поєднати користувачів ІВК на ідентифікаторах та звичайних користувачів ІВК. Розглянемо архітектуру цієї схеми та її особливості:

1) Користувач володіє сертифікатом та ключами ІВК на ідентифікаторах (або чимось одним).
2) Сертифікати використовуються для автентифікації користувача та накладання цифрового підпису.
3) Ключі ІВК на ідентифікаторах використовуються для шифрування.

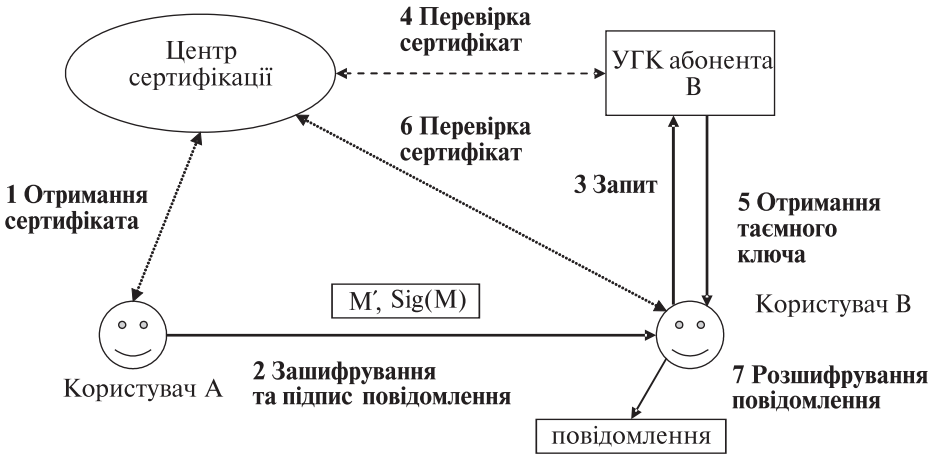

Рис. 1. Схема взаємодії користувачів системи Voltage

Відповідно, змінюються етапи при зашифруванні повідомлення:

1) Користувач А отримує сертифікат відкритого ключа;

2) Маючи в якості вхідних даних загальносистемні параметри та ідентифікатор одержувача В, А направлено шифрує повідомлення та підписує його на своєму таємному ключі ІВК на ідентифікаторах;

3) В надсилає запит до УГК на генерацію таємного ключа;

4) УГК перевіряє автентичність В, перевіряючи його сертифікат;

5) УГК генерує та надсилає В його таємний ключ;

6) В перевіряє цифровий підпис А, перевіряючи сертифікат А;

7) В розшифровує повідомлення.

Сильними сторонами такої системи, на думку компанії Voltage, буде:

1) Відмова від перевіряння відправником сертифікату одержувача (шифрування йде на ідентифікаторах);

2) Можливість взаємодії користувачів з сертифікатами та без них;

3) Можливість підключення додаткових сервісів;

4) Спрощення процедури анулювання сертифікату.

Проведемо аналіз цієї архітектури, зважаючи на вимоги, що були висунуті вище. Спочатку виділимо особливості, якими вона володіє:

1) Ця система може використовуватися, як надбудова над традиційною ІВК;

2) Для повноцінної взаємодії користувачі повинні мати сертифікати;

3) Якщо користувачі обслуговуються різними УГК, вони повинні отримувати цілісні загальні параметри цих УГК;

4) Одержувач повідомлення повинен перевірити сертифікат відправника для верифікації його підпису;

5) Користувач, який не має сертифікату, може приймати повідомлення від інших користувачів, але він не має можливості підписувати повідомлення та повинен деяким чином проходити автентифікацію на УГК. Крім того, він повинен власноруч отримувати відкриті параметри УГК одержувача;

6) УГК повинні довіряти усі користувачі, тому що він має доступ до таємних ключів.

На відміну від традиційної ІВК, відправнику не потрібно перевіряти сертифікат одержувача, тому що шифрування проходить на ідентифікаторах з використанням білінійного відображення. Можна також налагодити взаємодію між користувачами з сертифікатами та без. Але все рівно УГК кожного користувача може розшифровувати повідомлення і усі користувачі повинні бути зареєстровані в УГК (або пройти автентифікацію, кожен раз, коли отримають ключі).

Тобто виходить, що навіть ті користувачі, які мають сертифікат, повинні довіряти УГК. Це дорівнює тому, що виключивши один з недоліків традиційної ІВК (не самий суттєвий, тому що CRL все одно необхідні), ми добавили до існуючої інфраструктури головний недолік ІВК на ідентифікаторах – необхідність довіри до уповноваженого. Крім того, за рахунок використання усіма користувачами елементів обох інфраструктур складність кінцевої системи значно підвищується.

3. РІШЕННЯ, ЗАПРОПОНОВАНЕ ДЖ. КАЛЛАСОМ

Існують і інші погляди на проблемні питання криптографії на ідентифікаторах. Наприклад, Дж. Каллас зазначає, що, по-перше, проблема анулювання сертифікатів (якщо дивитися під кутом швидкодії та необхідності в постійному доступі до Internet) у сучасному світі вже не стоїть гостро, і в подальшому, можливо, зовсім зникне. Це пов'язано з тим, що сьогодні можливості комп'ютерів зросли, а необмежений доступ до глобальної мережі вже не виняток, а реальність. Це зауваження в деякій мірі ставить під сумнів один з найважливіших переваг ІВК на ідентифікаторах – відсутність сертифікатів (і відповідно off-line роботу). По-друге, використання унікальних та простих для запам'ятовування ідентифікаторів (які повинні встановлюватися таким чином, щоб

було зрозуміло їх належність деякому користувачу) теж породжує деякі проблеми. Це, з одного боку, дає можливість зловмиснику (чи соціальному інженеру) досліджувати структуру організації, де використовують таку ІВК, і отримувати інформацію про її службовців. Друга проблема полягає в тому, що отримати ідентифікатор користувача системи набагато легше (тому що він загальновідомий) і, відповідно, обчислити відкритий ключ теж дуже легко. А це вже дозволить спамерам направлено шифрувати повідомлення, будучи впевненими, що воно дійде до адресату.

Дж. Каллас запропонував рішення, яке, на його погляд, вирішувало зазначені ним недоліки та було найбільш ефективним. Він відмовився від використання сертифікату, замінивши його відповіддю (скоріш за все підписаною) сервера.

Наведемо його схему:

1) УГК обирає таємний ключ;

2) УГК обирає IDF (односпрямована безключова функція). Це може бути звичайна геш-функція, або інша псевдо-випадкова односпрямована функція. Також це може бути асиметрична криптографічна функція – наприклад, перетворення RSA. За допомогою цієї функції УГК генерує IDT (цифровий відбиток ідентифікатора), обчислюючи його як $IDT = IDF(K_{PKG}, ID)$, використовуючи свій таємний ключ в якості простого секрету;

3) УГК обирає детермінований псевдо-випадковий генератор, який ініціалізується за допомогою IDT. Цей генератор повинен видавати ключову пару (відкритий ключ, таємний ключ). Він також може бути будь-яким асиметричним криптографічним перетворенням.

Схема дійсно ставить у відповідність будь-якому ідентифікатору відповідну ключову пару та може використовувати відомі та перевірені криптопримітиви. На рис. 2 показана модель взаємодії користувачів запропонованої системи.

Процедура видачі ключів, згідно цієї схеми, буде наступна:

1) УГК виробляє IDT, як $IDT = IDF(K_{PKG}, ID)$ для кожного ID;

2) УГК ініціалізує RNG (псевдовипадковий генератор) початковим значенням, рівним IDT;

3) УГК генерує ключову пару за допомогою RNG – IKP_{ID};

4) Якщо УГК отримує неавтентифікований запит для будь-якого ID, він повертає $IKP_{ID\ public}$. Це трапляється, коли Боб хоче дізнатися відкритий ключ Аліси;

5) Якщо УГК отримує автентифікований запит для будь-якого ID, він повертає $IKP_{ID\ private}$. Це трапляється, коли Аліса хоче отримати свій таємний ключ.

Механізми автентифікації та захисту каналу зв'язку не уточнюються. По суті, від стандартної ІВК на ідентифікаторах відрізняється лише тим, що:

1) Користувачі виробляють відкриті ключі не самостійно, а роблять запит до уповноваженої сторони.

2) Можливо використовувати будь-які відомі криптопримітиви.

Проведемо аналіз цієї схеми. На думку розробника, тепер зловмисник не має можливості самостійно генерувати або визначати відкриті ключі користувачів, йому прийдеться відправляти запит на сервер. Але в той же час, він має доступ до відкритих ідентифікаторів, і, хоча вони не є відкритими ключами, є можливість провести аналіз структури інформаційної системи. Крім того, для такої схеми можна використовувати відомі криптопримітиви, які вже пройшли перевірку часом. Це є суттєвою перевагою даної схеми.

Серед недоліків можна відзначити:

1) Необхідність чітко визначати та застосовувати механізми перевірки цілісності та справжності переданої інформації. Це пов'язано з тим, що відповідь УГК навіть на запит зовнішнього користувача повинна бути підписана (для забезпечення цілісності переданого відкритого ключа). Такі підписані відповіді будуть повним аналогом процедури сертифікації.

2) Так і не вирішена проблема відповідності єдиного відкритого ключа різним ідентифікаторам, тому що, згідно запропонованої схеми, різним ідентифікаторам відповідають різні IDT, а тому і різні відкриті ключі.

3) Значно більше навантаження на УГК (порівняно зі звичайною ІВК на ідентифікаторах), якщо він буде генерувати ключі та підписувати відповідь навіть на неавтентифікований запит.

4) Крім того, зловмисники все рівно зможуть отримувати доступ до відкритих ключів користува-

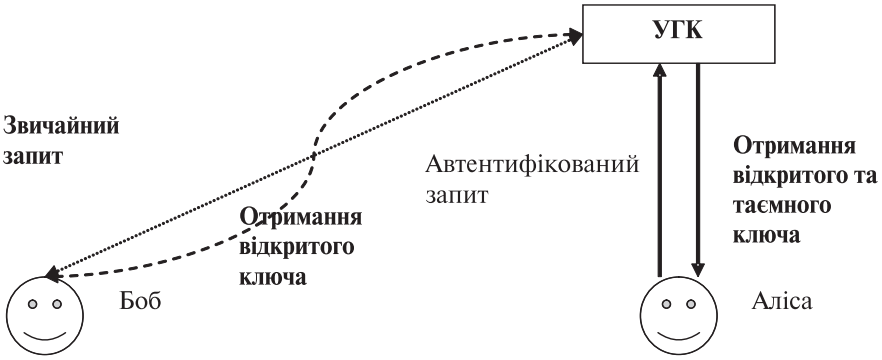

Рис. 2. Схема взаємодії користувачів у схемі Дж. Калласа

чів, тому що вони в змозі зробити неавтентифікований запит на сервер (якщо це дозволяють правила мережевого екрану).

Ця схема нагадує скоріше не ІВК на ідентифікаторах, а традиційну ІВК, де користувачі здійснюють пошук сертифіката по ключовому полю (яким, по суті, є ідентифікатор).

4. ПОРІВНЯННЯ КОМБІНОВАНИХ ІВК

Проведемо порівняння описаних архітектурних рішень за критеріями, що були визначені вище. Порівняння будемо проводити за умовними критеріями, тому що безумовним критеріям відповідають усі рішення (якщо вважати, що розробники відповідних систем використовують надійні протоколи) (див. табл. 1).

Таблиця 1

Порівняння архітектурних рішень ІВК за умовними критеріями

Критерій\ Інфраструктура	Система Voltage	Схема Джо Калласа	ІВК на ідентифікаторах
Необхідність повної довіри до УГК	+	+	+
Використання стандартизованих протоколів	тільки підпис	+	–
Наявність сертифікатів	+	- (але необхідно підписувати відкриті ключі)	–
Можливість взаємодії користувачів різних інфраструктур	+	–	–
Навантаження на УГК (вразливість до DDOS атак)	незначне	значне	незначне
Стан впровадження	+	-	–

Усі з порівняних систем володіють спільним недоліком — необхідністю довіри до уповноваженого на генерацію ключів. Цікаво, що це стосується навіть системи Voltage, користувачі якої повинні довіряти УГК, хоча володіють сертифікатами. Рішення, запропоноване Джоном Калласом, нагадує традиційну ІВК, але замість сертифікатів застосовуються підписані відповіді сервера. До того ж, користувачі повинні довіряти УГК. Тому можна зробити висновок, що ці дві архітектури нічим не краще, ніж звичайна ІВК на ідентифікаторах. На сьогоднішній час реально впроваджена тільки система Voltage, але доречність її застосування покаже час.

ВИСНОВКИ

На сьогоднішній день існує багато розробок у галузі застосування перетворень на ідентифікаторах, але робіт, що досліджують комбінацію традиційної ІВК та ІВК на ідентифікаторах, дуже мало. Аналіз пропозицій, що розглянуті у цій статті, показує, що проблема взаємодії різних інфраструктур (або якісного вдосконалення існуючої ІВК) потребує серйозної уваги, бо зараз не існує такої схеми, яка б відповідала вимогам і була б краще для застосування у великих ІТС, ніж традиційна ІВК.

Література.

[1] *І.Д. Горбенко, Т.О. Гріненко.* Захист інформації в інформаційно-телекомунікаційних системах. Харків, 2004.

[2] *Горбенко И.Д. Мелецкий А.П., Погребняк К.А., Шевченко Д.В.* Билинейное спаривание эллиптических кривых и его теоретические основы. Прикладная Радиоэлектроника. Том 5. – №1, 2006. – С. 3-12.

[3] *Бондаренко М.Ф., Горбенко І.Д., Мелецький О.П., Кравченко П.О.* Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів.// Прикладная радиоэлектроника, Том 6, №3, 2007. – С. 356-362.

[4] *Горбенко І.Д., Мелецький О.П.* Удосконалений протокол вироблення ключів з асиметричними криптографічними перетвореннями зі спарюванням точок еліптичних кривих на базі ідентифікаторів.// Радіотехніка, №147, 2006. – С. – 99-106.

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

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

[7] *A.Shamir.* Identity –based cryptosystems and signature schemes. In Advances in Cryptology-Crypto'86, 1986.

[8] Menezes An Introdution to Pairing-based Cryptography. 2004.

Надійшла до редколегії 22.09.2008

Горбенко Іван Дмитрович, професор, зав. кафедрою БІТ ХНУРЕ, головний конструктор ЗАТ «ІІТ». Область наукових інтересів: проектування та розробка засобів КЗІ.

Кравченко Павло Олександрович, інженер-програміст ЗАТ «ІІТ». Область наукових інтересів: інфраструктури відкритих ключів.