Інформаційні технології

УДК 004.056.55

Колесник Дмитро Олександрович

студент

Харківського національного університету імені В.Н. Каразіна

МОДЕЛЬ ПОРУШНИКА, ЗАГРОЗ, БЕЗПЕКИ ДЛЯ ПОСТКВАНТОВОГО ЦИФРОВОГО ПІДПИСУ

Анотація. *Проведено аналіз моделі порушника, загроз та безпеки для цифрових підписів постквантового періоду на основі конкурсу NIST.*

Ключові слова: *постквантова криптографія, модель порушника, модель загроз, модель безпеки.*

NIST планує стандартизувати кілька механізмів ЕП, які забезпечать стійку ЕП від адаптованих атак повідомлень. У науковій літературі ця безпека називається безпекою EUF-CMA. Таким чином, NIST розглядатиме атаку адаптивного повідомлення як основну атаку. Кандидати ES, які будуть розглядатися в ході цієї дипломної роботи, будуть класифікуватися на основі того, як вони можуть надати таке майно. Скаржники не можуть надати докази безпеки для цього нападу, але такі докази будуть розглянуті за наявності.

Як незаперечні дані пропонується, щоб криптоаналітик мав доступ не більше до 2^{64} вибраних повідомлень. Однак також будуть розглянуті атаки з великою кількістю повідомлень. Швидше за все, NIST спочатку розгляне класичні атаки, а не квантові запити до оракула ЕП.

1.1 Модель порушника та його можливості

Побудова моделі зловмисника необхідна для розробки комплексу заходів, що забезпечують безпеку алгоритму. Така модель може бути побудована за різноманітними критеріями.

Розробка моделі порушника відбувається щоб отримати відповіді на наступні запитання:

1) від кого потрібно захищати інформацію?
2) яка мета у порушника?
3) що знає порушник?
4) які повноваження в системі має можливий порушник?
5) які методи і засоби може використовувати порушник?

Модель порушника - це опис можливих дій зловмисника, що формується на основі аналізу типу зловмисника, рівня його авторитету, знань, практичних та теоретичних можливостей.

Особа, яка може отримати доступ до роботи за допомогою засобів, включених до КС, вважається порушником. Порушників можна класифікувати за рівнем можливостей, що надаються їм стандартними засобами КС. Є 4 рівні можливостей. Класифікація є ієрархічною, кожен наступний рівень включає попередній:

- 1-й рівень визначає самий нижній рівень можливостей для проведення діалогу з КС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації.
- 2-й рівень визначається можливістю створювати та запускати власні програми з новими функціями обробки інформації;
- 3-й рівень визначається здатністю контролювати функціонування КС, тобто впливом на базове ПЗ системи, на склад та конфігурацію її обладнання;
- 4-й рівень визначається всією сферою можливостей осіб, які розробляють, впроваджують та ремонтують апаратні компоненти КС, аж до включення власних засобів з новими функціями обробки інформації в КС [21].

Передбачається, що на його рівні злочинець - це висококваліфікований фахівець, який має повну інформацію про КС та КЗЗ.

Така класифікація досить корисна для використання протягом періоду оцінки ризику, аналізу вразливості системи та ефективності заходів захисту [22].

Для того, щоб скласти модель порушника, усіх порушників, які можуть бути лише там, потрібно класифікувати за різними показниками.

Можливі типи класифікації порушників:

1) За метою порушення - визначити мотиви порушника. Дії зловмисника, залежно від цілі, можуть бути спрямовані на сервери, ключі, алгоритми тощо.

2) За рівнем знань про алгоритм - усі порушники поділяються за рівнем класифікації та обізнаності щодо алгоритму та його вразливостей. Класифікація враховує знання злочинця та його практичні навички роботи з КС та ІТ.

3) За місцем дії - визначити місцезнаходження злочинця щодо організації при спробі отримати несанкціонований доступ до інформаційних ресурсів організації.

4) Відповідно до методів та способів, які вони використовують - зловмисник може отримати конфіденційну інформацію та ISOD, використовуючи різні засоби та/або методи. Порушення може бути скоєне з використанням або без використання засобів отримання інформації. Методи можуть бути як суперечливими закону, так і суперечливими. Методи соціальної інженерії можна вважати дозволеним способом отримання інформації.

5) За рівнем можливостей, що надаються їм за допомогою автоматизованої системи та комп'ютерних технологій, внутрішніх

порушників можна класифікувати за рівнем доступу до наданої системи. Чим вищий рівень доступу, тим більше можливостей отримати ISOD. [22].

6) З мотиву порушень - вони можуть порушувати цілісність алгоритму з різних причин. Порушення можна розділити на дві групи: навмисні і ненавмисні.

Виходячи з написаного, ми можемо побудувати модель порушника.

Таким чином, модель зловмисника така:

1) Необхідно захистити інформацію від зловмисника який володіє квантовим комп'ютером принаймні 100 кубітів потужності або від добре обладнаної хакерської групи, необхідно забезпечити захист навіть від нападів великих професійних груп.

2) Порушник прагне отримати інформацію будь-яким способом за допомогою квантового комп'ютера.

3) У кращому випадку зловмисник не знає системи та алгоритму. Найчастіше зловмисник може знати лише загальнодоступні дані, або може перехопити частину інформації, або бути інсайдером. У нашому випадку це однаково ймовірні варіанти.

4) У кращому випадку злочинець не має повноважень у системі. Якщо це інсайдер або особа, яка отримала адміністративний доступ, вона може замінити процеси в системі та відновити її для себе за умови, що адміністратор має відповідні права. У нашому випадку це знову ж однаково ймовірні варіанти.

5) Ми вважаємо, що він використовує всі доступні ресурси - найпотужніші комп'ютери та необмежений час.

6) У гіршому випадку зловмисник знає все про об'єкт і про все встановлене на ньому охоронне обладнання. У кращому випадку він нічого не знає. Знову ж таки, це однаково ймовірні варіанти.

Таким чином, була розроблена модель вторгнення для постквантових механізмів ЕП.

1.2 Модель безпеки

На даний момент пропонується використовувати модель EUF-CMA як модель безпеки для асиметричних постквантових криптографічних перетворень електронних підписів. EUF-CMA визначає екзистенційну недосконаліть від атак на основі вибраних повідомлень. Зокрема, ця модель не дозволяє криптографічному аналітику виробляти ЕП для повідомлень, які залежать від ключів, наприклад, при використанні закритого ключа sk. Виходячи з цього, застосовуючи безпечну модель ES, згідно з EUF-CMA, EUF-CMA також безпечно атакувати, коли не застосовуються запити на повідомлення, але якщо є хоча б один запит на повідомлення в залежності від ключів, безпека механізму ЕП порушена.

Існує два загальних визначення для безпеки схеми ЦП. Кожне з визначень представлено як "гра" або експеримент, який проводиться між нападником та чесним претендентом.

Добре експеримент EUF-CMA працює наступним чином:

1) Претендент створює робочу пару ключів (pk, sk) і надає pk атакуючому.

2) У атакуючого є змога і повторно запросити підписи на самостійно обраних повідомленнях $(M_1, \dots, M_q)$ та отримати дійсні підписи $(\sigma_1, \dots, \sigma_q)$ у відповідь.

3) Як тільки експеримент закінчується зловмисник має вивести повідомлення та підпис M^*, σ^* таким чином, що (1) повідомлення не було одним із повідомлень, що вимагає попереднього кроку, і (2) повідомлення / підпис перевіряється правильно за допомогою відкритого ключа.

Схема безпечна, якщо жоден зловмисник не має ні найменшої переваги у виконанні зазначених умов. Зазвичай кількість повідомлень q обмежується лише часом виконання зловмисником. Однак для особливого

випадку одноразових підписів криптоаналітик обмежується запитом лише одного підпису на етапі (2).

Це визначення є досить сильним, але все ще слабшим, ніж SUF-CMA.

Неофіційно SUF-CMA (Вибране атакування повідомлень, що сильно уникає існування) працює так:

1) Те ж саме, що й у попередньому експерименті.

2) Те ж саме, що й в попередньому експерименті.

3) Після завершення експерименту Зловмисник повинен відобразити повідомлення та підпис M^*, σ^* так, щоб (1) пара (M^*, σ^*) не була одним із запитуваних повідомлень, а підпис повертався на попередньому кроці (2) повідомлення / підпис перевірено правильно за допомогою відкритого ключа. Зловмисник виграє, якщо вона виконає вищезазначені умови.

Головна відмінність в тому, що це визначення гарантує, що зловмисник не може забрати підпис. Наприклад, схема, в якій зловмисник може повторно випадково підібрати дійсний підпис, щоб залишатися дійсним, але виглядати не так, як початкове значення, не задовольняє SUF-CMA [1].

Показано, що механізм ЕП із компонентами генерації ключів KeyGen, підпису Sign та перевірки Verify справжнім при атаках, заснованих на адаптивно вибраному повідомленні, якщо для всіх компонентів алгоритмів $\boldsymbol{A}$ з доступом до оракула підпису $\text{Sign}(\cdot, sk)$, є функція $\in (\cdot)$ така, що:

$$Pr\left[\begin{matrix}(sk, pk) \overset{R}{\leftarrow} KeyGen(1^k) \\ (M^*, \sigma^*) \overset{R}{\leftarrow} A^{Sign*(\cdot,sk)}(pk)\end{matrix} : M^* \notin Q \wedge Verify(M^*, \sigma^*, pk) = 1\right] \leq \in (\kappa)$$

Де Q – це сукупність запитів, які $\boldsymbol{A}$ видав оракулу ЕП.

Визначимо гру між криптографічним аналітиком і схемою підпису:

EUF–CMA–GAME(*Gen, Sign, Ver, A, n*)

1) $Gen(1^n) \rightarrow (sk, vk)$
2) $\boldsymbol{A}$ отримує vk
3) $\boldsymbol{A}$ створює повідомлення vk
4) $\boldsymbol{A}$ отримує $s \leftarrow Sign(sk, m)$
5) $\boldsymbol{A}$ повторює кроки 3 та 4 за необхідністю
6) $\boldsymbol{A}$ виводить m^*, s^*
7) $\boldsymbol{A}$ перемагає, якщо $Ver(vk, m^*, s^*) = accept$ та m^* не був підписаний раніше $Sign$

Визначення: Схема підпису EUF-CMA є безпечним, якщо для будь-якого криптографічного аналітика $\boldsymbol{A}$, який працює у поліноміальний час, ймовірність перемоги EUF-CMA-GAME є незначною.

1.3 Модель загроз

Загрозою для інформаційної безпеки АС є можливість здійснення впливу на інформацію, що призводить до створення, знищення, копіювання, блокування доступу до інформації, а також можливість впливу на компоненти АС, що призводить до втрати знищення або порушення функціонування носія інформації, засобів взаємодії з носієм або засобів його управління.

Необхідність класифікації загроз інформаційної безпеки зумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна, структурна та функціональна побудова інформаційно-обчислювальних систем (мереж), технології та умови обробки такі, що інформація потрапляє під вплив надмірно велика кількість факторів, відповідно до яких і необхідно формалізувати завдання опису загроз та ефективного протидії їм. Перелік загроз інформаційній безпеці [22; 23] буде розглянуто відповідно до цільового критерію класифікації та опису компонентів інформаційних потоків, критичних для модифікації. Аналіз

цих загроз слід проводити на основі їх кваліфікації за низкою критеріїв. Кожен із знаків відображає одну із узагальнених вимог до системи безпеки (конфіденційність, цілісність, надійність): несанкційоване копіювання з носіїв інформації; необережні дії, які призводять до розголошення конфіденційної інформації або оприлюднення її; не слідування організаційним обмеженням (встановленим правилам) при визначенні рангу системи.

Для системи потрібно визначити список класів загроз (якості моделі): за ступенем навмисності; за станом джерела загроз; за природою виникнення; за безпосереднім джерелом загроз; за впливом на АС; за ступенем залежності від активності АС; за етапами доступу користувача або програми до ресурсів АС; за варіантами доступу до даних АС; за місцем розміщення інформації, яка зберігається та оброблюється в АС.

Під час розгляду питання захисту АС, добре використовувати градацію на чотири рівні доступу до інформації, яка обробляється, зберігається та залишається в АС: рівень засобів роботи з носіями; рівень вмісту інформації; рівень місця, де зберігається інформація; рівень подачі інформації.

Крім того, необхідно сформулювати додаткові вимоги до аналізу інформаційних загроз:

- список загроз повинен бути якомога повнішим та детальнішим. Для кожної із загроз необхідно визначити порушення, на які властивості інформації або АС вона спрямована (конфіденційність, цілісність, доступність, а також відмова служб АС);
- вірогідні методи [23] реалізації загроз.

Беручи до уваги технологію обробки інформації та побудову моделі інформаційних загроз, я розробив модель порушника, яка повинна бути адекватною реальному порушнику для конкретного оратора.

Література

1. EUF-CMA and SUF-CMA. URL: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/ (дата звернення: 16.04.2019).
2. Backes M., Pfitzmann, B. Scedrov A.: Key-dependent message security under active attacks–BRSIM/UC-soundness of symbolic encryption with key cycles, in: CSF '07, Proc. of the 20th IEEE Computer Security Foundations Symposium, IEEE Computer Society, Washington, DC, USA, 2007, pp. 112–124, URL: http://dx.doi.org/10.1109/CSF.2007.23 (дата звернення: 16.04.2019).
3. Black J., Rogaway P., Shrimpton T.: Encryption-scheme security in the presence of key-dependent messages, in: SAC '02 – Selected Areas in Cryptography (K. Nyberg et al., eds.), 9th Annual International Workshop, St. John's, Newfoundland, Canada, 2002, Lecture Notes in Comput. Sci., Vol. 2595, Springer, Berlin, 2003, pp. 62–75.
4. Halevi S., Krawczyk H. Security under key-dependent inputs, in: Proc. of the 14th ACM Conference on Computer and Communications Security – CCS '07 (P. Ning et al., eds.), Alexandria, Virginia, USA, 2007, ACM, New York, NY, USA, 2007, pp. 466–475, URL: http://doi.acm.org/10.1145/1315245.1315303 (дата звернення: 16.04.2019).
5. Boneh D., Halevi S., Hamburg M., Ostrovsky R. Circularsecure encryption from decision Diffie-Hellman, in: Advances in Cryptology–CRYPTO '08 (D. Wagner, ed.), 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2008, Lecture Notes in Comput. Sci., Vol. 5157, Springer, Berlin, 2008, pp. 108–125.
6. Haitner I., Holensteiny T. On the (im)possibility of key dependent encryption, in: TCC '09 – Theory of Cryptography (O. Reingold, ed.), 6th Theory of Cryptography Conference, San Francisco, CA, USA, 2009,

Lecture Notes in Comput. Sci., Vol. 5444, Springer, Berlin, 2009, pp. 202–219.

7. Hofheinz D., Unruh D.: Towards key-dependent message security in the standard model, in: EUROCRYPT '08 – Advances in Cryptology (N. Smart, ed.), 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 2008, Lecture Notes in Comput. Sci., Vol. 4965, Springer, Berlin, 2008, pp. 108–126.
8. Applebaum B., Cash D., Peikert C., Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems, in: Advances in Cryptology – CRYPTO '09 (S. Halevi, ed.), 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2009. Lecture Notes in Comput. Sci., Vol. 5677, Springer, Berlin, 2009, pp. 595–618.
9. Gonzalez M. Cryptography in the Presence of Key-Dependent Messages. Ph.D. Thesis, Florida Atlantic University, December 2009, URL: http://brain.math.fau.edu/Gonzalez/dissertation.pdf (дата звернення: 17.04.2019).
10. BELLARE, M. – MINER, S. K.: A forward-secure digital signature scheme, http://cseweb.ucsd.edu/~mihir/papers/fsig.html, July, 1999.
11. Faust S., Kiltz E., Pietrzak K., Rothblum G. Leakage-resilient signatures, Cryptology ePrint Archive: Report 2009/282, June, 2009, URL: http://eprint.iacr.org/2009/282 (дата звернення: 16.04.2019).
12. Bellare, M., Kilian, J., Rogaway, P.: The Security of Cipher Block Chaining. In: M. Franklin (ed.) Advances in Cryptology – CRYPTO 1994: Proceedings of the 14th Annual International Cryptology Conference, vol. 839, pp. 341-358. Springer (1994).
13. Bellare, M., Yee, B.: Forward-Security in Private-Key Cryptography. In: M. Joye (ed.) Topics in Cryptology – CT-RSA 2003, Lecture Notes in Computer Science, vol. 2612, pp. 1-18. Springer (2003).

14. Gonzalez Muniz, M., Steinwandt, R.: Security of Signature Schemes in the Presence of Key-Dependent Messages. Tatra Mountains Mathematical Publications 47, 15-29 (2010).
15. Jaulmes, E., Joux, A., Valette, F.: On the Security of Randomized CBC-MAC Beyond the Birthday Paradox Limit: A New Construction. In: J. Daemen, V. Rijmen (eds.) FSE 2002: Revised Papers from the 9th International Workshop on Fast Software Encryption, vol. 2365, pp. 237-251. Springer (2002).
16. Kim, J., Biryukov, A., Preneel, B., Hong, S.: On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). In: R.D. Prisco, M. Yung (eds.) Security and Cryptography for Networks, 5th International Conference, SCN 2006, Lecture Notes in Computer Science, vol. 4116, pp. 242-256. Springer (2006).
17. Menezes, A., Vanstone, S., Oorschot, P.V.: Handbook of Applied Cryptography. CRC Press (1996).
18. Preneel, B., van Oorschot, P.: On the Security of Iterated Message Authentication Codes. IEEE Transactions on Information Theory 45(1), 188-199 (1999).
19. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І. Д. Горбенко, Ю. І. Горбенко. Х. : «Форт», 2012. 870 с.
20. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем: монографія. / Ю. І. Горбенко. Х. : Форт, 2015. 959 с.
21. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків: Форт, 2010. 593с
22. Мокренко П.В. Елементи і пристрої фізичної та електронної охорони об'єктів. Львів, 2000.
23. Петраков А. В., Дорошенко П. С., Савлуков Н. В. Охрана и защита современного предприятия. М., 1999.