TECHNICAL SCIENCES AND TECHNOLOGIES

DOI: 10.25140/2411-5363-2024-4(38)-208-213
УДК 004.4:056.57

Олександр Миколайович Полевод

аспірант кафедри інформаційних та комп'ютерних систем
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: oleksandr.polevod23@gmail.com. **ORCID** https://orcid.org/0009-0007-0885-8625

КЛЕПТОГРАФІЯ В КОНТЕКСТІ ЗАХИСТУ ІНФОРМАЦІЇ. КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ АТАК

Стаття досліджує клептографію як наукову дисципліну, що виходить за межі криптографії та охоплює ширший спектр загроз інформаційної безпеки. Автор аналізує сучасні клептографічні атаки, які використовують приховані канали для витоку даних, зокрема через апаратні та програмні вразливості, а також побічні канали, такі як енергоспоживання і таймінги. Пропонується класифікація цих атак і підкреслюється необхідність комплексного підходу до їх виявлення та нейтралізації, що включає криптоаналіз, інженерію та фізичний аналіз систем.

Ключові слова: *клептографія; криптографія; побічний канал; класифікація; реверс-інжиніринг; захист інформації.*

Бібл.: 8.

Актуальність теми дослідження. Із середини 90-х років клептографія та її предметне поле були зведені переважно до дослідження прихованих та побічних комунікацій і асиметричних бекдорів у криптоалгоритмах (таких як генерація та обмін ключами, цифровий підпис, шифрування тощо). З розвитком інформаційних технологій невпинно зростає і інформаційна злочинність, представники якої шукають все більш вишукані та приховані способи для реалізації своїх намірів щодо даних користувачів. До того ж спецслужби держав також мають свої інтереси у сфері контролю інформаційної діяльності населення, використовуючи різноманітні засоби програмно-апаратної природи.

Останнім часом з'являється дедалі більша кількість повідомлень про виявлення сторонніх модулів, не заявлених офіційною специфікацією у пристроях для широкого використання (смартфони, комп'ютери та інші засоби зв'язку). Автори таких заяв стверджують, що виявлені елементи та модулі потенційно мають шпигунське призначення і здатні непомітно для кінцевого користувача передавати певні дані за допомогою прихованих каналів. На фоні таких інцидентів представники, зацікавлених у збереженні контролю над державною безпекою скорочують використання технічних засобів, виробленої у «недружніх країнах» через загрозу компрометації даних, що становлять службову або державну таємницю.

Водночас представники спецслужб засобами державної політики «примушують» виробників інформаційних пристроїв впроваджувати модифікації, які дозволяють отримувати дані про роботу цих пристроїв без відома користувачів. У більшості випадків така «необхідна жертва» для безпеки залишається непоміченою і використовується виключно в законних цілях, хоча моральний бік цього явища залишається спірним і, ймовірно, філософським питанням. Однак із невпинним поширенням інформаційних пристроїв ці «лазівки» дедалі частіше виявляються і представниками злочинності. У таких випадках навмисне імплементований таємний канал використовується для крадіжки особистих даних, що несе пряму шкоду для звичайних користувачів.

Постановка проблеми.

У сучасних умовах стрімкого розвитку інформаційних технологій та їх використання не лише для легальних цілей, але й у протиправній діяльності, проблема захисту інформації набуває нового значення. Клептографія, яка вивчає приховані канали витоку даних і методи імплементації уразливостей у системах безпеки, досі переважно розглядається у вузькому контексті криптографії. Однак її потенціал для аналізу загроз інформаційної безпеки є значно ширшим. Зловмисники та державні спецслужби

використовують лазівки у програмному забезпеченні, апаратних компонентах і криптографічних системах для прихованого доступу до конфіденційних даних. У таких умовах постає питання, як забезпечити надійний захист інформаційних систем, мінімізуючи ризики зловживань прихованими каналами. Це вимагає ширшого підходу до клептографії, включаючи комплексне дослідження всіх рівнів системи, від апаратного до програмного, та розробку методів протидії таким атакам.

Аналіз останніх досліджень і публікацій. Проблематика клептографічних атак активно досліджується, хоча значна частина робіт зосереджена на конкретних аспектах або прикладах їх реалізації. У фундаментальних дослідженнях Young і Yung [1; 2] було представлено концепцію клептографії як способу використання криптографії для створення прихованих бекдорів у системах безпеки. Робота Janovsky, Krhovjak і Matyas [3] аналізує практичне впровадження клептографічних методів у криптографічних протоколах, зокрема TLS, пропонуючи підхід до їх виявлення та протидії. Kovalenko і Kudin [4] досліджують способи усунення пасток у криптографічних протоколах, акцентуючи увагу на створенні захищених систем без прихованих каналів. Праця Ткач та співавторів [5] висвітлює історію розвитку клептографії та визначає її місце в контексті сучасної інформаційної безпеки, акцентуючи на необхідності ширшого підходу до вивчення цієї дисципліни. Історичний кейс операції "Рубікон" [6] демонструє приклад державного рівня атак, спрямованих на використання прихованих каналів у шифрувальних пристроях.

Існуючі підходи до класифікації клептографічних атак здебільшого зосереджені на окремих аспектах, таких як криптографічні бекдори або приховані канали в шифрувальних алгоритмах. Наприклад, роботи Young і Yung акцентують увагу на криптографічних бекдорах, не охоплюючи апаратні чи програмні вразливості. Інші дослідження, такі як аналіз атак у протоколах TLS, пропонують класифікацію, але лише в межах одного рівня системи. Такий вузький підхід не враховує багаторівневий характер клептографічних загроз та їхню еволюцію в сучасних умовах. Крім цього, відсутність єдиного системного підходу ускладнює порівняння різних типів атак, їх ідентифікацію та розробку комплексних заходів захисту. Запропонована у статті класифікація клептографічних атак усуває ці недоліки завдяки багаторівневому та системному підходу. Вона охоплює атаки за цілями, методами, рівнями реалізації, складністю та виконавцями. Такий підхід дозволяє:

- Структуризувати знання: запропонована класифікація охоплює всі аспекти клептографічних атак, від системного рівня до специфічних методів, таких як атаки через побічні канали чи приховані модифікації.

- Полегшити ідентифікацію: чіткий поділ на категорії спрощує виявлення атак на різних етапах життєвого циклу системи – від розробки до експлуатації.

- Підвищити ефективність протидії: врахування всіх типів атак дозволяє розробляти комплексні заходи захисту, які враховують апаратні, програмні та фізичні аспекти.

- Забезпечити адаптивність: класифікація передбачає включення нових типів атак, що з’являються із розвитком технологій.

Таким чином, запропонована у статті класифікація є важливим кроком до створення цілісного підходу до вивчення клептографічних атак та забезпечення їхньої ефективної нейтралізації. Вона сприяє як фундаментальному розумінню цього явища, так і практичному впровадженню рішень для підвищення інформаційної безпеки.

Сучасні дослідження здебільшого аналізують методи впровадження прихованих каналів і їхній вплив на криптографічні системи, однак систематична класифікація клептографічних атак залишається недостатньо розвиненою. Це вказує на потребу в комплексних дослідженнях, спрямованих на побудову більш широких класифікацій атак з урахуванням їх цілей, методів реалізації та рівнів впровадження.

Метою статті є пропозиція змінити підхід і погляд на клептографію, як набагато ширшу дисципліну, та класифікувати шляхи та методи імплементації прихованих каналів витоку конфіденційної інформації

Виклад основного матеріалу. Клептографічні атаки – це способи прихованого доступу до даних, часто впроваджені через лазівки або спеціально створені вразливості в системах безпеки. Вони можуть використовуватися як державними органами для боротьби зі злочинністю, так і зловмисниками для шпигунства чи саботажу. Як було зазначено вище, клептографія переважно розглядалась і продовжує розглядатись як підгалузь криптографії, на що вказують класичні та новітні дослідження. На нашу думку, варто почати з класифікації клептографічних атак для забезпечення повної картини перед подальшими дослідження. Далі наведено варіант класифікації за різними принципами.

1. За метою атаки:

- *Спостереження і розвідка* - атаки, які спрямовані на збір інформації. Наприклад, держава може використати спеціальні лазівки, щоб відстежувати підозрілих осіб. Відомим прикладом є операція "Рубікон" [6], коли спецслужби використовували шифрувальні пристрої з лазівками, щоб читати секретні повідомлення інших країн.

- *Економічне шпигунство* - такі атаки спрямовані на викрадення комерційних таємниць або інтелектуальної власності. Зловмисники можуть впроваджувати лазівки в програмне забезпечення, щоб отримати важливі дані, наприклад, про нові технології.

- *Саботаж* - мета такої атаки в пошкоджені або зруйнуванні системи. Наприклад, атака може бути націлена на IoT-пристрої, щоб дистанційно керувати технікою або зламати її.

2. За способом атаки:

- *Атаки через лазівки* - це коли в систему безпеки навмисно впроваджують прихований доступ, який можна використовувати для дешифрування повідомлень. Наприклад, Clipper Chip [7] був спеціально розроблений для того, щоб правоохоронці могли легко отримати доступ до зашифрованих розмов.

- *Атаки через побічні канали* - це коли зловмисники використовують слабкі місця в апаратному забезпеченні, наприклад, стежать за витратами енергії або часом виконання задач для отримання даних.

- *Приховані (стеганографічні) канали*: - такі атаки використовують «сигнали», заховані в зашифрованих повідомленнях або підписах, щоб непомітно передати інформацію.

3. За рівнем системи:

- *Системні атаки* націлені на основну систему, наприклад, операційну систему чи криптографічні алгоритми. Деякі компанії, такі як Microsoft, працювали зі спецслужбами для впровадження таких лазівок.

- *Атаки на рівні додатків* на прикладному рівні лазівки вбудовуються в конкретні програми, як-от банківські додатки або веббраузери, через які проходить зашифрований трафік.

- *Атаки на рівні апаратного забезпечення* зловмисники впроваджують лазівки безпосередньо у чіпи чи інші елементи пристроїв, що робить атаку більш складною для виявлення.

4. За складністю:

- *Прості атаки* - їх легко впровадити й важко виявити. Наприклад, приховані канали, які дозволяють непомітно передавати невелику кількість інформації.

- *Складні атаки* - вимагають використання більш складних методів шифрування. Наприклад, коли зловмисники змінюють алгоритми шифрування так, що це важко помітити, але вони можуть використовувати лазівки.

5. За виконавцем атаки:

- Інсайдерські атаки - це коли самі розробники навмисно впроваджують лазівки. Наприклад, як це було [8] з Crypto AG, коли компанія, під впливом ЦРУ, розробляла шифрувальні пристрої з прихованими лазівками.

- Атаки ззовні - у цьому випадку зловмисники використовують лазівки, які були випадково або ненавмисно створені в системі.

6. За етапом впровадження:

- *Атаки під час розробки* - лазівки впроваджуються ще на етапі розробки криптосистем або апаратних компонентів.

- *Атаки після розгортання* - лазівки впроваджується після того, як система вже працює. Це можуть бути атаки через оновлення або вразливості, які не були виявлені раніше.

7. За можливістю виявлення:

- *Непомітні атаки* - такі атаки спроєктовані так, щоб бути повністю невидимими для користувачів і систем безпеки.

- *Виявляються, але важко довести* - деякі атаки можна помітити, але довести їх наявність або знайти лазівку дуже складно.

Важливим поняттям при вивченні клептографії є побічні канали витоку інформації — це неочевидні шляхи, через які зловмисники можуть отримати доступ до конфіденційних даних системи, не атакуючи безпосередньо саму криптографію або захищені алгоритми. Замість цього вони використовують властивості фізичної реалізації системи, такі як споживання енергії, час обробки операцій, випромінювання електромагнітних хвиль або звукові коливання, для вилучення чутливої інформації. Одним із класичних прикладів є атаки на основі вимірювання часу виконання криптографічних операцій: різний час обробки може вказувати на структуру ключа або інших важливих параметрів.

Пошук побічних каналів є складним завданням, оскільки вони не свідомо закладені в систему, а є результатом її фізичних характеристик. Аналіз таких каналів зазвичай вимагає спеціального обладнання та методик. Для їх виявлення використовують техніки тестування безпеки, такі як вимірювання енергоспоживання, аналіз часових затримок або моделювання електромагнітного випромінювання пристрою. Виявлення побічних каналів — це важливий крок, оскільки вони можуть бути використані для витоку даних навіть у найбільш надійних на перший погляд системах.

Заходи з нейтралізації побічних каналів включають як зміни в архітектурі системи, так і застосування контрзаходів на фізичному рівні. Наприклад, можна додавати шум до сигналу енергоспоживання або часу виконання операцій, щоб зробити їх менш інформативними для зловмисника. Інші методи включають рівномірний розподіл обчислювальних операцій, використання фізичних екранів для блокування електромагнітного випромінювання та покращення алгоритмів так, щоб вони не демонстрували очевидних закономірностей у фізичній поведінці. Ці заходи роблять побічні канали менш доступними для атак і підвищують загальний рівень безпеки системи.

Висновки. Клептографія еволюціонувала від досліджень, спрямованих на криптографічні бекдори, до більш широкого аналізу загроз інформаційної безпеки, охоплюючи апаратні, програмні та фізичні аспекти. Основна ідея клептографічних атак полягає у використанні прихованих каналів для витоку даних через вразливості на різних етапах створення та експлуатації систем. Проведена класифікація атак дозволяє виявити їх за рівнем системи, складністю, способом впровадження та метою, що сприяє кращому розумінню природи таких загроз і необхідних заходів протидії.

Результати дослідження демонструють, що клептографічні атаки виходять далеко за межі традиційної криптографії, впливаючи на весь спектр інформаційних технологій. Це підкреслює важливість комплексного підходу до захисту систем, який охоплює як розробку захищених алгоритмів, так і запобігання використанню побічних каналів витоку інформації.

Подальші дослідження мають бути спрямовані на створення ефективних методів виявлення прихованих каналів і нейтралізації атак, а також розробку систем захисту, здатних адаптуватися до нових типів загроз. Особливу увагу слід приділити інтеграції криптоаналізу, інженерії апаратного забезпечення та аналізу фізичних процесів у загальну стратегію забезпечення інформаційної безпеки. Це дозволить створити цілісну концепцію боротьби з клептографічними атаками та підвищити рівень захисту сучасних інформаційних систем.

Список використаних джерел

1. Kleptography: Using Cryptography Against Cryptography [Electronic resource] / A. Young, M. Yung. – Accessed mode: https://link.springer.com/content/pdf/10.1007/3-540-69053-0_6.pdf.

2. The Dark Side of Black-Box Cryptography, or: Should we trust Capstone? [Electronic resource] / A. Young, M. Yung. – Accessed mode: https://link.springer.com/chapter/10.1007/3-540-68697-5_8.

3. Bringing Kleptography to Real-World TLS [Electronic resource] / A. Janovsky, J. Krhovjak, V. Matyas. – 2019. – Accessed mode: https://hal.science/hal-02294600/document.

4. Kleptography trapdoor free cryptographic protocols [Electronic resource] / B. Kovalenko, A. Kudin – Accessed mode: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13840.

5. Ткач, Ю. Історія виникнення клептографії та її місце в безпеці інформації [Електронний ресурс] / Ю.Ткач, М. Шелест, М. Синенко, Т. Петренко // Технічні науки та технології. – 2023. – №3 (33). – С. 150–161. - Режим доступу: http://tst.stu.cn.ua/article/view/291215.

6. Operation Rubikon [Electronic resource]. – Access mode: https://www.zdf.de/politik/frontal/operation-rubikon-100.html.

7. The NSA Tried This Before – What the 90s Debate Over The Clipper Chip Can Teach Us About Digital Privacy [Electronic resource] // Internet History Podcast. – Accessed mode: https://www.internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/.

8. The intelligence coup of the century [Electronic resource] // The Washington Post. – Accessed mode: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

References

1. Young, A., Yung, M. (1997). Kleptography: Using Cryptography Against Cryptography. Proceedings of EUROCRYPT'97: *Advances in Cryptology, 1233*, 62-74. https://link.springer.com/content/pdf/10.1007/3-540-69053-0_6.pdf.

2. Young, A., Yung, M. (1996). The Dark Side of Black-Box Cryptography, or: Should we trust Capstone? Proceedings of CRYPTO'96: *Advances in Cryptology,* 1109, 89–103. https://link.springer.com/chapter/10.1007/3-540-68697-5_8.

3. Janovsky, A., Krhovjak, J., Matyas, V. (2019). Bringing Kleptography to Real-World TLS. *Genetic and Evolutionary Computing* (pp. 15-27). https://hal.science/hal-02294600/document.

4. Kovalenko, B., Kudin, A. Kleptography trapdoor free cryptographic protocols. (2018). *eprint.iacr.org.* https://eprint.iacr.org/2018/989.

5. Tkach, Yu., Shelest, M., Synenko, M., Petrenko, T. (2023). The history of kleptography and its place in information security. *Technical Sciences and Technology*, (3(33)), 150–161. http://tst.stu.cn.ua/article/view/291215.

6. Operation Rubikon. (2020). *www.zdf.de*. https://www.zdf.de/politik/frontal/operation-rubikon-100.html.

7. The NSA Tried This Before – What the 90s Debate Over The Clipper Chip Can Teach Us About Digital Privacy. (2014). *www.internethistorypodcast.com.* https://www.internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/.

8. The intelligence coup of the century. (2020). *www.washingtonpost.com.* https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

Отримано 18.11.2024

UDC 004.4:056.57

Oleksandr Polevod

PhD Student of Department of Information and Computer Systems
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: oleksandr.polevod23@gmail.com. **ORCID** https://orcid.org/0009-0007-0885-8625

KLEPTOGRAPHY IN INFORMATION SECURITY CONTEXT. CLASSIFICATION OF KLEPTOGRAPHIC ATTACKS

The increasing informatisation of society presents new challenges, as modern information technologies are used not only by regular users but also by individuals engaged in illegal activities, such as criminals, fraudsters, and terrorist groups. These technologies are being exploited for unlawful operations, which requires each state to maintain control over its segment of cyberspace.

The issue of exclusive access and control by specialised services over citizens' information activities is becoming increasingly important as the level of informatisation increases. A key challenge in this area is that kleptography, as a discipline that studies this field, is still in its early stages and is often applied in a rather narrow sense.

An analysis of existing works on this topic has shown that kleptography is still predominantly viewed in the context of cryptography, which provides a narrow and specific perspective on this discipline. The problem of identifying secret channels for information leakage needs to be considered beyond traditional cryptanalysis, as in the current era of widespread digitalization and informatization, attackers are finding increasingly sophisticated ways to carry out illegal information activities.

The purpose of this article is to present kleptography in a broader context than cryptography and to provide a classification of kleptographic attacks.

This study examines kleptography in the modern context, its tasks and challenges, and offers a classification of attacks based on hidden channels. The results show that kleptography has evolved from research focused on cryptographic backdoors to a broader understanding of information security threats. The primary idea of kleptographic attacks is to introduce vulnerabilities during the system's development or operation stages, using hidden channels to leak data. Kleptography encompasses not only cryptography but also hardware and software security, including side-channel attacks such as power consumption or timing analysis. Detecting such attacks is challenging and requires a comprehensive approach that integrates cryptanalysis, engineering, and analysis of physical system processes.

Keywords*: kleptography; cryptography; side-channel; classification! reverse engineering; information security.*

References: 8.

Полевод О. М. Клептографія у контексті захисту інформації. Класифікація клептографічних атак. *Технічні науки та технології.* 2024. № 4(38). С. 208-213.