Тема 19. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЧНИХ СИСТЕМ

На сучасному етапі розвитку існують наступні проблеми криптографічних систем:

- перетворення повідомлень великого об’єму;
- застосування методів стиснення і кодування даних;
- розподіл сеансових ключів;
- знаходження способів вирішення існуючих *NP*-повних задач.

Перейдемо до розгляду суті проблеми. [4]

1. Перетворення повідомлень великого об’єму

Розвиток мереж передачі даних і мультимедійних засобів гостро поставив питання захисту повідомлень великого об’єму.

Мова йде про криптографічне перетворення текстових повідомлень. Тепер починають застосовуватися інформаційні технології, при яких відбувається передача великих об’ємів даних в реальному масштабі часу. До таких технологій можна віднести системи відео конференцій, відео- та голосову пошту, факсимільну та модемну пошту.

В подібних системах необхідно забезпечити надійний захист інформації, що передається з однієї сторони, та високу швидкість перетворення та передачі – з іншої.

Вирішенням такої проблеми може бути застосування методів шифрування даних. Ці методи володіють цілим рядом переваг.

По-перше, вони можуть працювати з блоками даних будь-яких розмірів. При використанні блокових методів шифрування могла виникнути штучна затримка, викликана необхідністю очікування заповнення блока перед початком його перетворення.

По-друге, потокові методи шифрування володіють високою швидкістю перетворення даних. [4]

2. Застосування методів стиснення і кодування даних

Коли розглядалися питання теоретичної та практичної стійкості криптосистем Шеннон показав, що чим вища збитковість тексту, тим більша ймовірність того, що він буде розкритий криптоаналітиком противника.

Відомо, що будь-яка мова володіє певною збитковістю. Наприклад, російська мова менш збиткова ніж англійська. Знаючи заздалегідь частоту появи окремих символів у відкритому тексті, криптоаналітик зможе прочитати шифрований текст достатньо великого об’єму.

Для вирішення цієї проблеми необхідно використовувати в комплексі з методами шифрування також методи стиснення та кодування. Перераховані методи перетворення даних ефективно доповнюю один одного, а їх сумісне застосування дозволить використати відкриті канали зв’язку для передачі повідомлень.

Методи стиснення дозволять значно зменшити об’єм даних, що передаються або даних, що зберігаються, методи кодування – захистять інформацію, що передається, від перешкод і помилок в каналах зв’язку. Шифрування захистить інформацію від прочитання її посторонніми особами.

Таким чином, спочатку відкритий текст повинен стискатися, потім його необхідно зашифрувати, а далі уже закодувати.

Крім того, застосування подібного підходу здатне вирішити проблему криптографічного перетворення повідомлень великого об’єму. [4]

3. Розподіл сеансових ключів

У великих інформаційних системах на сьогоднішній день високу актуальність має проблема розподілу сеансових ключів. Частково ця проблема може бути вирішена за рахунок використання криптосистем з відкритими ключами. Однак, сучасні асиметричні алгоритми володіють великою обчислювальною складністю і їх застосування не завжди виправдане.

Існує два підходи до вирішення даної проблеми: використання центра розподілу ключів (ЦРК) та використання “блукаючих ключів”. Кожен з підходів має свої переваги та недоліки. Перейдемо до їх розгляду.

Перший підхід пропонує наявність у складі інформаційної системи окремого компонента, який відповідає за генерацію і видачу ключів сеансу кожному абоненту. Перед початком роботи сеансу обидві сторони звертаються до такого компонента за ключами, необхідними для роботи.

Переваги такого підходу полягають в наступному: зосередження способів генерації сеансових ключів в одному місці, спрощення адміністрування роботи системи.

Недоліками є висока уразливість системи у випадку виходу з ладу ЦРК. Крім того, зловмисник може створити засіб, який імітує роботу ЦРК,

Другий підхід пропонує заміну ключів взаємодії за деяким правилом, яке відоме лише двом сторонам, що обмінюються. Ключі можуть змінюватися як на початку нового сеансу, так і періодично протягом одного сеансу.

Переваги підходу – більш простий спосіб встановлення зв'язку сторонами.

Недоліки – у випадку порушення правил заміни ключів на одній із сторін, взаємодія сторін буде перервана. Крім того, правила заміни ключів зберігаються у багатьох місцях і можуть бути обчисленні криптоаналітиком противника. [4]

4. Знаходження способів вирішення існуючих *NP*-повних задач

За останнє десятиліття криптографія з відкритим ключем перетворилася з нової концепції в опору криптографічної технології. В майбутньому збережеться тенденція росту кількості випадків застосування асиметричних алгоритмів перетворення. Однак, висока популярність подібних систем притягує до них увагу багатьох криптоаналітиків.

На жаль, технологічна база криптографії з відкритим ключем є недостатньо розвиненою. За виключенням схеми Макеліса, яка була розроблена з ціллю протистояння відомим методам криптоаналізу, фактично всі алгоритми цифрового підпису і криптографії з відкритим ключем в якості *NP*-повної задачі використовують операцію піднесення до степеня по модулю добутку простих чисел.

Таким чином, враховуючи великі досягнення у вирішенні задач розкладу і обчисленні дискретних алгоритмів, вони стають все більш вразливими.

Виходячи з вище сказаного слідує, що при розробці нових криптосистем великого значення потрібно приділяти вибору *NP*-повній задачі. [4]

5. Заключення

На сьогоднішній день існують апробовані і гарно зарекомендувавші себе методи криптографічного захисту даних. Їх стійкість до різного роду атак доведена математично або ж зводиться до вирішення складної математичної задачі. Здавалося б, застосування таких методів в інформаційних системах повинно забезпечити конфіденційність інформації, що захищається.

Тим не менш, у засобах масової інформації періодично з'являються повідомлення про знайдені "дирки" в системах захисту інформації або факти "взлому" таких систем.

Чому так відбувається? Намагатимемося пояснити це.

Як було відмічено раніше, методи криптографічного захисту є лише малою частиною систем захисту інформації. Використання в таких системах стійких методів зовсім не гарантує того, що подібна не може бути взломана порушником.

Для того, щоб побудувати захищену інформаційну систему розробнику необхідно бути підготовленим не гірше потенційного порушника. Розробник повинен знати про всі вразливі місця інформаційних систем та причини їх виникнення. Іншими словами, знаючи способи перемоги систем захисту інформації, легше протидіяти подібним намаганням. Тому особливої важливості набуває аналіз проведених атак на захищені системи з ціллю визначення причин їх ненадійності.

До основних причин ненадійності методів криптографічного захисту інформації можуть бути віднесені:

- експортні обмеження крипто алгоритмів;
- використання несертифікованих засобів захисту інформації;

- помилки, закладені при проектуванні та реалізації систем захисту інформації;
- людський фактор.

Розглянемо більш детально основні причини ненадійності криптографічних методів захисту інформації.

Експортні обмеження криптоалгоритмів

Ця причина пов'язана з експортом крипто алгоритмів або з необхідністю купівлі на них патенту. Наприклад, в США заборонений експорт крипто алгоритмів, що використовують довжину ключа більш ніж 40 біт. Очевидно, що такі алгоритми не можуть вважатися надійними в теперішній час.

В якості прикладів програмних продуктів, що підтвердженні експертним обмеженням можуть бути версії браузерів Інтернет Netscape Navigator фірми Netscape Communications та Internet Explorer фірми Microsoft. У цих продуктах реалізований метод шифрування зі 128-бітним ключем для користувачів всередині США і з 40-бітним ключем для всіх інших.

Інформація, зашифрована таким продуктом з довжиною ключа 40 біт, може бути отримана шляхом повного перебору ключів.

Використання несертифікованих засобів захисту інформації

Сьогодні на багатьох сайтах Інтернету користувачу пропонується велика кількість засобів криптографічного захисту інформації. Рекламні проспекти стверджують, що запропонований продукт (найчастіше вільно розповсюджуваний) забезпечить надійний та гарантований захист ваших даних.

Виникає питання: яким чином можна визначити, чи є алгоритм надійним? Адже результатом роботи як стійкого, так і недостатньо стійкого крипто алгоритму буде незрозуміла для користувача послідовність символів. За зовнішнім виглядом вихідної послідовності практично неможливо визначити, який із алгоритмів був використаний у пропонованому засобі.

Розробник подібного засобу міг використовувати замість перевіреного стійкого алгоритму перетворення свій власний. Крім того, у засіб могли бути внесені не документовані можливості, універсальні ключі, що відкривають будь-який текст і т.п.

З вищевикладеного стає очевидним, що використання несертифікованих засобів захисту інформації може бути фактором ненадійності захищаючої системи.

Помилки, закладені при проектуванні та реалізації систем захисту інформації

Застосування криптографічних методів захисту інформації передбачає використання ключів перетворення даних. Тільки за допомогою ключа перетворене повідомлення може бути прочитане.

При використанні методів криптографії у інформаційних системах гостро постає питання про збереження ключової інформації. Адже подібна інформація буде являти собою великий інтерес для потенційних порушників.

Багато інформаційних систем були взломані тільки тому, що не було виділено необхідної уваги питанням зберігання ключів, паролів і т.д. Можна навести такий приклад: поряд із закритими на замок дверима на цвяшку висить ключ від замка. Неважко здогадатися, що порушник зможе подолати таку систему захисту.

Необхідно також пам’ятати, що проектування та реалізація систем захисту інформації реалізовується людиною, а людині властиво помилятися. Людина може невірно реалізувати алгоритм перетворення даних, спростити алгоритм та наробити багато інших, не менш критичних помилок.

Яскравим прикладом системи, при розробці якої було закладено багато помилок (в тому числі й у підсистему захисту інформації) може бути операційна система Windows.

Людський фактор

В будь-якій критичній системі помилки обслуговуючого персоналу є самими дорогими та приносять найбільшу шкоду. Що стосується методів криптографії, то непрофесійні дії користувачів зводять нанівець стійкий крипто алгоритм і саму коректну його реалізацію.

В першу чергу це стосується використання паролів. Зазвичай, користувачі хочуть використовувати короткі та осмислені паролі. Їх легше запам’ятати користувачу, але їх і легше розкрити противнику. Застосування ж довгих і

беззмістовних паролів призводять до виграшу з точки зору криптостійкості, однак, дуже часто людина не може запам’ятати такий пароль, записує його на папері, який потім може бути загублений чи викрадений порушником.

Крім того, яка б не була надійна система захисту інформації, самим вразливим її місцем є надто довірливий персонал. Зараз порушники не намагаються взламати систему в “лоб”, а стараються застосовувати прийоми соціальної інженерії.

Розглянувши основні принципи ненадійності інформаційних систем можна зробити висновок, що застосування одних тільки методів криптографії не гарантує надійного захисту інформації. Методи криптографічного захисту повинні використовуватися у комплексі з іншими мірами захисту інформації. [4]