УДК 621.391

Марія Мандрона[1], Олег Гарасимчук[2]
1. Кафедра безпеки інформаційних технологій
Національного університету “Львівська політехніка”
Кафедра управління інформаційною безпекою
Львівського державного університету безпеки життєдіяльності
2. Кафедра захисту інформації
Національного університету “Львівська політехніка”

АТАКИ НА ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

The paper discusses and analyzed the use of pseudorandom numbers in the systems of protection. The proposed a classification of attacks on pseudorandom number generators that will allow professionals to effectively prevent the attacks, eliminate their effects, thus strengthening the security systems that use data generators.

Keywords – attack, the generator of pseudorandom numbers, the attacker, cryptanalysis, resistance, cryptosystem.

У статті розглянуто використання псевдовипадкових чисел в системах захисту інформації. Побудовано класифікацію атак на генератори псевдовипадкових чисел, яка дозволять розробникам ефективно запобігати атакам, усунути їх наслідки, зміцнюючи тим самим безпеку системи.

Ключові слова – атака, генератор псевдовипадкових чисел, зловмисник, криптоаналіз, стійкість, криптосистема.

Вступ

У зв'язку з постійним розвитком обчислювальної і вимірювальної техніки, а також із впровадженням досягнень новітніх технологій значно розширилась сфера застосування генераторів випадкових і псевдовипадкових чисел, що ставить нові вимоги до їх проектування та методів оцінки якості. Також існує протиріччя між непередбачуваністю генераторів псевдовипадкових чисел (ГПВЧ) та їх продуктивністю і ефективністю реалізації.

Псевдовипадкові числа – фундаментальний стандартний блок для зміцнення і забезпечення конфіденційності зв’язків радіоелектронними засобами. Вони є основним елементом криптографії, цифрового підпису, протоколів безпеки та іншого забезпечення надійності при зв’язку з використанням комп’ютера. Отже, якість засобів генерації псевдовипадкових чисел, відіграє важливу роль для забезпечення надійних систем захисту інформації.

Значне зростання останніми роками продуктивності обчислювальних систем сприяло появі великої кількості алгоритмів генерування псевдовипадкових послідовностей чисел. На сьогоднішній день ефективно використовуються кілька десятків, як програмних, так і апаратних генераторів псевдовипадкових чисел. Хоча зловмисники також не стоять осторонь цих процесів і постійно вдосконалюють методи та способи атак на ГПВЧ.

Метою даної роботи є опрацювання різноманітних видів атак на генератори псевдовипадкових чисел з метою проведення класифікації таких атак на основі принципів їх здійснення.

Визначення атак на генератори псевдовипадкових чисел

Важливою науково-технічною задачею, на сьогоднішній день, є вивчення та класифікація різноманітних способів атакування ГПВЧ, для ефективного запобігання, протидії та усунення наслідків таких атак, а також для зміцнення систем безпеки.

Атака на генератор псевдовипадкових чисел – атака, спрямована на розкриття параметрів генератора з метою подальшого передбачення псевдовипадкових чисел [6].

Успішна атака може розкрити багато криптографічних систем незалежно від того, наскільки ретельно вони були спроектовані. Проте деякі системи використовують недосконало спроектовані ГПВЧ, або роблять це таким чином, що зменшує складність атак. Більше того, потрібно лише одне єдине успішне проникнення, щоб скомпрометувати всю систему.

Генератори псевдовипадкових чисел орієнтовані на використання в системах захисту інформації і повинні відповідати таким вимогам [7, 13]:

- криптографічна стійкість;
- хороші статистичні властивості (псевдовипадкові послідовності за своїми статистичними властивостями не повинна відрізнятися від істинно випадкової послідовності);
- великий період формованої послідовності;
- ефективна апаратна і програмна реалізація.

При використанні криптостійкого ГПВЧ можна визначити три завдання, які обчислювально, неможливо розв'язати зловмиснику:

-визначення (i-1)-го елемента γ_{i-1} послідовності на основі відомого фрагмента гами $\gamma_i\gamma_{i+1}\gamma_{i+2}\ldots\gamma_{i+b-1}$ кінцевої довжини b;

-визначення (i+1)-го елемента γ_{i+1} послідовності на основі відомого фрагмента гами $\gamma_i\gamma_{i+1}\gamma_{i+2}\ldots\gamma_{i+b-1}$ кінцевої довжини b;

-визначення ключової інформації за відомим фрагментом гами кінцевої довжини [2, 9].

Оцінка ефективності і надійності ГПВЧ – складна науково-технічна задача, тому необхідно проводити аналіз можливих загроз для конкретного типу генератора, що передбачає оцінку його стійкості до різноманітних типів атак.

В результаті проведеного аналізу літературних джерел, нами була запропонована класифікація найбільш відомих класів та видів атак на генератори псевдовипадкових чисел, яка наведена на рис. 1.

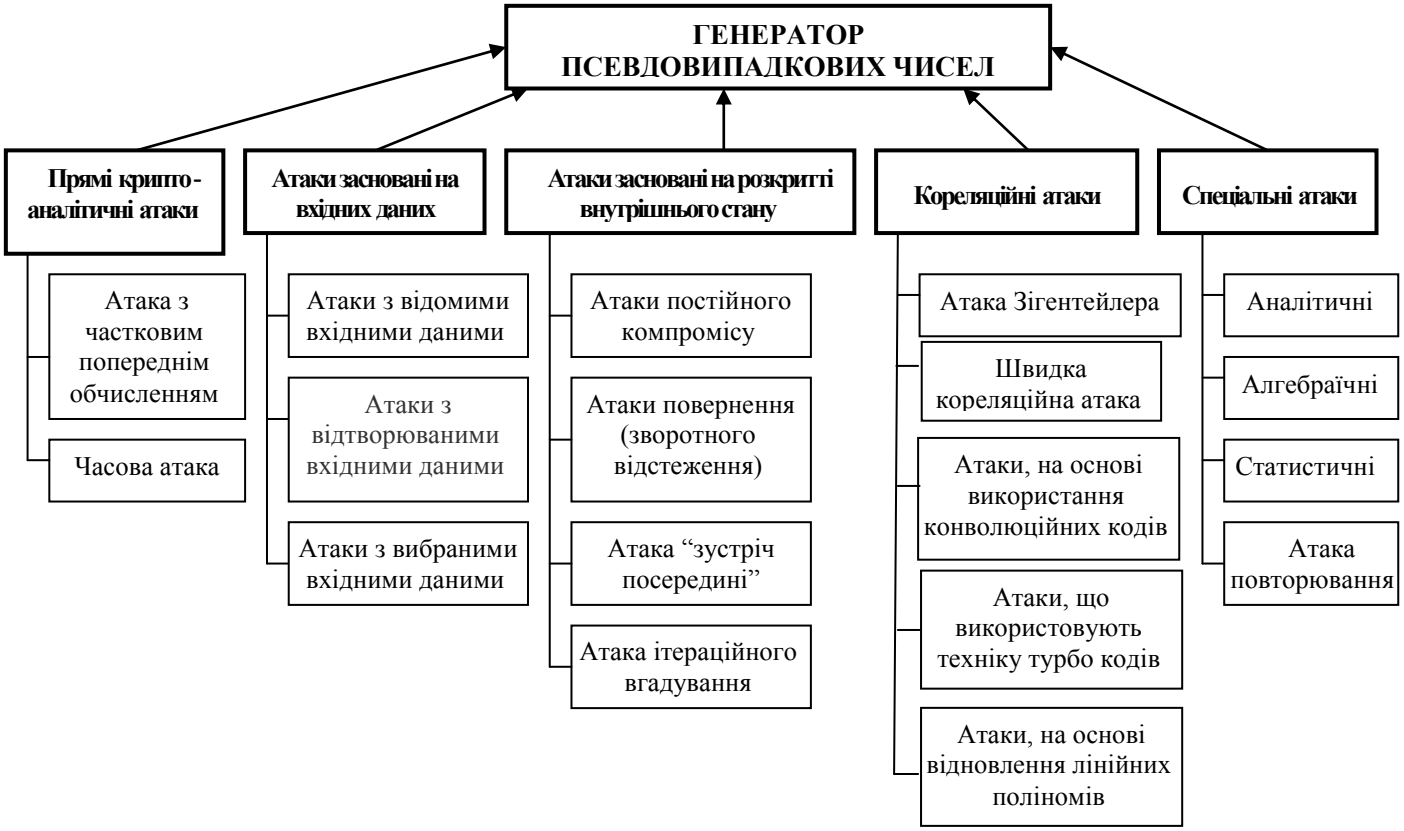

Рис. 1. Класифікація атак на генератори псевдовипадкових чисел

Клас прямих криптоаналітичних атак

Якщо зловмисник здатний безпосередньо відстежувати вихідні дані генератора псевдовипадкових чисел і дослідити закономірність їх появи, то це є пряма криптоаналітична атака. Цей вид атаки поширюється на більшість алгоритмів, що використовують ГПВЧ [4].

Атака з частковим попереднім обчисленням. Ця атака може застосовуватись до будь-якого генератора, який використовує лічильник. Припустимо, що вхідні дані не оброблені, і зловмисник може спостерігати послідовні вихідні дані. У наступному кроці зловмисник повинен обчислити вихідні дані кожного t-го значення лічильника і запам'ятати їх в списку. Одне з t спостережених значень повинно увійти до списку. Після запису вхідних даних у списку, можна знайти внутрішній стан генератора. Всі подальші вихідні дані залишаються відомими до тих пір, поки не будуть оброблені нові вхідні дані [1].

Часова атака. Дана атака використовує той факт, що інкрементація лічильника вимагає різної кількість часу, залежно від передбаченої кількості байтових додавань. Якщо зловмисник може виміряти час, необхідний для інкрементації лічильника, він може зробити висновки по числу нулів в поточному стані лічильника. Можливий також варіант вгадування моменту часу, коли всі байти нижнього порядку є нульові, оскільки тоді для попереднього інкременту необхідно особливо багато байтових додавань. Така ситуація позначається як «слабкий стан» в часовій атаці. Інформація, яка отримується завдяки цій атаці, може бути скомбінована з атакою попередніх обчислень. Це означає, що зловмиснику відомо, коли вигідніше порівнювати вихідні дані зі списку попередніх обчислень [1].

Клас атак на основі вхідних даних

Даний клас атак можливий у випадках, коли зловмисник може використовувати інформацію про вхідні сигнали ГПВЧ або контролювати її. Атаки засновані на вхідних даних можуть бути розділені на атаки з відомими вхідними даними, атаки з відтворюваними вхідними даними і атаки з вибраними вхідними даними [1, 3-5].

Атаки з відомими вхідними даними протягом цієї атаки зловмисник може спостерігати частину вхідних даних, але не може маніпулювати ними. Значення вхідних даних можуть використовуватися для обмеження числа можливих вхідних значень, для зменшення стійкості генератора або для підтримки інших атак. Атаки з відомими вхідними даними можливі, коли оцінка ентропії вхідних даних невірна, або якщо застосовано спостереження за пристроями введення.

Атаки з вибраними вхідними даними. При використанні цієї атаки, зловмисник може безпосередньо маніпулювати вхідними даними генератора. Розглянемо приклад, використовуючи генератор DSA заснований на геш-функції і призначений для вироблення DES ключів. Всі функції додавання відбуваються за mod 2^N, де $160 \leq N \geq 512$. Нехай N=160, тому що це значення представляє найслабшу версію генератора. Генератор містить внутрішній стан X_i, $i \geq 1$. Нове вхідне W_i обробляється кожного разу, коли генеруються вхідні дані. Якщо ніяких вхідних даних немає, то W_i встановлюється в 0. Вихідні дані генеруються як:

$$output[i] = SHA(W_i + X_i (mod 2^{160})) \quad (1)$$

$$X_{i+1} = X_i + output[i] + 1 (mod 2^{160}) \quad (2)$$

$$W_i = W_{i-1} - output[i-1] - 1 (mod 2^{160}) \quad (3)$$

Нові вхідні дані змушують генератор негативно зациклюватися, але не надають ніякої інформації про фактичне значення вхідних даних.

Атаки з відтворюваними вхідними даними можуть використовуватися в тих же ситуаціях, але вимагають менш складних систем злому і менш складного аналізу з боку зловмисника.

Клас атак на основі розкриття внутрішнього стану

При атаках такого класу припускається, що в даний момент зловмисник знає частину внутрішнього стану генератора і намагається лише розширити ці знання до наступних моментів часу, і до попередніх або майбутніх вихідних даних. Така ситуація може виникнути, якщо генеруючий процес був розгалужений в незахищеному стані.

При проведенні такого типу атак зловмисник намагається використовувати раніше успішні атаки на ГПВЧ, що розкрили його внутрішній стан, з метою передбачення стану подальших або попередніх станів ГПВЧ, наскільки це можливо. Такого роду атаки можуть бути успішні в тому випадку, коли ГПВЧ починає свою роботу з відомого або передбачуваного стану. На практиці, дуже складно визначити той факт, що внутрішній стан було скомпроматовано. Саме тому, ГПВЧ повинні протидіяти компроматуванню внутрішнього стану. Можливі 4 варіанти атак такого класу: атака постійного компромісу, атака повернення, атака "зустріч посередині" та атака ітераційного вгадування.

Атаки постійного компромісу можливі для таких систем, в яких одного разу вже був розкритий стан S в момент часу t_0, що робить всі попередні та наступні стани уразливими для подальших атак. Ця атака означає, що генератор ніколи повністю не відновлюється з компрометованого стану. Зловмисник здатний визначити майбутні і навіть попередні вихідні значення. Припустимо, що є можливість знайти ключ K генератора. Оскільки ключ ніколи не змінюється ніякими новими вхідними даними, інформація обробляється до тих пір, поки весь генератор, що включає ключ, не буде переініціалізований. Через певний проміжок часу ми виявимо два послідовних вихідних значення (output[i], output[i+1]). Припускаючи, що поточна тимчасова мітка містить тільки 10 невідомих бітів, які представляють реалістичне значення, існує 2^{10} вгадувань для кожного T_i і $T_{i+1.}$ T_{i+1} може бути обчислено два різними методами:

$$X_i = D_K(T_{i+1} \oplus output[i+1]) \quad (4)$$

$$X_{i+1} = E_K(T_i \oplus output[i]) \quad (5)$$

Для кожного вгадування T_i, T_{i+1} обчислюється і зберігається в сортованій таблиці, згодом обчислення відбувається для кожного T_{i+1}. Правильне значення T_{i+1} виникає як результат обох обчислень. Тому необхідно лише 2^{11} обчислень для виявлення поточного стану T_{i+1} генератора [1].

Атака повернення (зворотнє відстеження) використовує розкритий стан ГПВЧ S в момент часу t_0 з метою відновлення станів ГПВЧ, а відповідно і його виходів в попередні моменти часу. За допомогою генератора легко дізнатися про майбутні вихідні дані та про попередні дані.

Атака ітераційного вгадування використовує знання про стан S в момент часу t_0, і проміжні виходи ГПВЧ, щоб дізнатися S в момент часу $t_0+\Delta t$, коли входи, зібрані протягом цього періоду часу є вгадуваним (але не відомими) для атакуючого. На відміну від атаки постійного компромісу, йому достатньо тільки знання функції вихідних даних. Ітеративна атака вгадування використовує вгадані, але не відомі вхідні дані для визначення стану S в час $t+\xi$ [1]. Наприклад, для генератора ANSI 9.17 легко застосувати цю атаку для $\xi=1$. Припустимо, що відомий поточний стан генератора в час t_i, включаючи K, X_i, output[i], і що відома функція output[i+1]. Використовуючи попереднє припущення, що час містить тільки 2^{10} можливих вхідних значень, і для прогнозування внутрішнього стану X_{i+1} необхідно порівняння результатів з функцією output[i+1].

Атака "зустріч посередині" є по суті поєднанням атаки ітеративним вгадування і атаки повернення. Знання S в моменти часу t_0 і $t_0+2\Delta t$ дозволити зловмисникові відновити стан S в моменти часу $t_0+\Delta t$, а також у всьому часовому проміжку від t_0 до $t_0+2\Delta t$ [1]. Припустимо, що генератор ANSI 9.17 виробляє послідовність з 8-послідовних ключів шифрування для шифрування відкритого тексту. Вихідні дані генератора невідомі, але можна дізнатися стани T_i, T_{i+1} і зашифрований шифротекст, які використовують ключ, вироблений в час t+4. Припустимо, що кожна тимчасова мітка містить 10 бітів ентропії. Атака типу "зустріч посередині" дозволяє знати ключ з набагато меншими витратами, ніж 2^{80} спроб. Тим же способом, який застосовується для атак постійного компромісу, обчислимо $T_{i+1,\ i+2,i+3,i+4}$ та $T_{i+5,i+6,i+7,i+8}$. Як бачимо, необхідно приблизно 2^{41} обчислень. Значення обчислень з обох сторін зберігаються в двох списках і порівнюються один

одним. Буде знайдено 2^{16} збігів. Кінцевий 2^{16} ключовий пошук виявляє правильний ключ для відстежуваного шифротексту [3-5].

Клас кореляційних атак

Найбільш поширеними атаками є кореляційні атаки [3] в силу специфіки побудови потокових шифрів. Ці атаки використовують кореляцію вихідний послідовностей схеми шифрування з вихідною послідовністю регістрів для відновлення початкового заповнення останніх. Робота по розкриттю криптосистеми може бути скорочено і спрощено, якщо нелінійна функція пропускає на вихід інформацію про внутрішні компонентах генератора. Тому для відновлення початкового заповнення регістрів кореляційні атаки досліджують кореляцію вихідної послідовності шифросистем з вихідною послідовністю регістрів.

Серед атак даного класу можна виділити наступні атаки:

1. Базові кореляційні атаки (атака Зігенталера);
2. Швидка кореляційна атака;
3. Атаки, що базуються на використанні конволюціонних кодів;
4. Атаки, що використовують техніку турбо кодів;
5. Атаки, що базуються на відновленні лінійних поліномів.

Аналізуючи кореляційні атаки, можна зробити наступні висновки:

- базові кореляційні атаки є малопридатними для практичної реалізації в силу високої обчислювальної складності та застосовуються для регістрів з $r \geq 60$, де r – довжина регістра;
- швидкі кореляційні атаки вважаються найскладнішими. Ці атаки, засновані на методах декодування з низькою перевіркою парності, застосовуються лише до регістрів з низько ваговими поліномами і відносно низьким ступенем;
- найбільш практичними вважають атаки, які застосовують до регістрів довільної довжини. До таких атак відносяться атаки, що базуються на конволюційних кодах, що використовують техніку турбо кодів, які базуються на відновленні лінійних поліномів, а також швидка кореляційна атака Чепижова, Йоханссона, Смітса;
- атаки, що базуються на конволюційних кодах, і атаки, що використовують техніку турбо кодів, вимагають великих витрат пам'яті при використанні великих регістрів, що накладає обмеження на їх практичне використання;
- найбільш поширеними вважають атаку Йонсона-Йохансона, що базується на відновленні лінійних поліномів, і швидку кореляційну атаку Чепижова, Йохансона, Смітса, що володіють приблизно однаковими обчислювальними труднощами та обсягами необхідної пам'яті [13].

Клас спеціальних атак

Аналітичні атаки. Ці атаки виявляють структурні слабкості і недоліки алгоритму Прикладами є атака на двомісний DES і атака розкладання на множники в RSA.

При виконанні ***алгебраїчної атаки,*** зловмисник аналізує вразливість в математичних частинах алгоритму і використовує його внутрішні алгебраїчні структури. Для прикладу, атака на версію «текстової книги» криптосистеми RSA використовує такі властивості алгоритму, як факт, що при шифруванні 0 виходить 0.

Статистичні атаки виявляють статистичні слабкості в структурі алгоритму – наприклад, якщо вдається виявити статистичний шаблон, наприклад, порівнюючи кількість значень «0» з кількістю значень «1». Це може бути викликано, наприклад, використанням неякісного генератора випадкових чисел. Якщо ключі беруться безпосередньо з видачі ГВЧ, розподіл ключів може бути передбаченим. Знання про статистичну передбачуваності можуть використовуватися для зниження часу на пошук ключів [10-12].

Атаки повторювання. Великою проблемою в розподіленому середовищі є атаки повтору (повтор атаки), при виконанні яких зловмисник перехоплює певні дані, а потім відправляє їх знову, сподіваючись, що пристрій прийме їх за легітимну інформацію. Найчастіше зловмисник

намагається перехопити і повторно використовувати відповідні дані, щоб пройти аутентифікацію в системі від імені легітимного користувача і отримати таким чином несанкціонований доступ до неї.

Контрзаходами проти атаки повторювання є використання штампів часу і номерів послідовності. Якщо пакет має номер, який вже використовувався раніше, це вказує на атаку повтору. Також на пакети можуть ставиться штамп часу. При цьому на кожному комп'ютері налаштовується порогове значення, що визначає часовий інтервал, в рамках якого вказане в пакеті часом буде вважатися коректним. Якщо в пакеті вказано час, що виходить за межі цього інтервалу, це також може говорити про атаку повторювання [13].

Висновок

У цій роботі побудовано класифікацію атак на генератори псевдовипадкових чисел та показано, що різні види атак, мають різну складність для реалізації зловмисником, а отже потребують різної тривалості часу, обчислювальних та інших можливостей. Якість та правильне використання криптографічного алгоритму шифрування даних є дуже важливим чинником, який обов'язково потрібно враховувати при побудові надійної криптосистеми, в тому числі стійкого генератора псевдовипадкових чисел.

Оцінка ефективності і надійності генераторів псевдовипадкових чисел – складна науково-технічна задача. Тому необхідно проводити аналіз можливих загроз для конкретного типу генератора, що передбачає оцінку його стійкості до різноманітних типів атак.

Запропонована в даній роботі класифікація атак, дозволяє чітко визначити напрямки подальших досліджень щодо розробки та реалізації ефективних і надійних генераторів псевдовипадкових чисел.

Література

1. Rock A. Pseudorandom Number Generators for Criptographic Applications / A. Rock. – Salzbuburg, 2005. – p. 57–65.

2. Рябко Б.Я. Основы современной криптографии и стенографии / Б.Я. Рябко, А.Н. Фионов. – М.: Из-тво «Горячая линия-Телеком», 2010. – 232 с.

3. Zenner E. On Cryptographic Properties of LFSR-based Pseudorandom Generators / E. Zenner. – Mannheim, 2004. – p. 102.

4. Kelsey J. Cryptoanalyfic attacks on pseudorandom number generators / J. Kelsey, B. Schceier, D. Wagner, C. Hall. Lecture Note in Computer Science, 1998. – p. 188.

5. Информационная безопасность. [Електронний ресурс] – Режим доступу до ресурсу.: http://dorlov.blogspot.com/2010/10/issp-069.html

6. Атаки на ГПСЧ. [Електронний ресурс] – Режим доступу до ресурсу.: http://ru.wikipedia.org/wiki.

7. Knudsen L.R. Block Ciphers – Analysis, Design, Applicatons // Ph.D. dissertation, Aarhus Unversity, Nov 1994.

8. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М.: КУДИЦ_ОБРАЗ, 2001.

9. Schneier B. Applied Cryptography Second Edition: protocols, algorithms and source code in C. John Wiley & Sons Inc., 1996.

10. Дорошенко А.Н., Ткачев Л.Л. Информационная безопасность. Методы и средства защиты информации в компьютерных систе_мах. Учебное пособие. М.: МГУПИ, 2006. – 143 с.

11. Корнюшин П.Н., Костерин А.С. Информационная безопасность: Учебное пособие. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

12. Стасев Ю.В., Потий А.В, Избенко Ю.А. Исследование методов криптоанализапоточных шифров. [Електронний ресурс] – Режим доступу до ресурсу.: http://www.nrjetix.com/fileadmin/doc/publications/articles/stasev_potiy_izbenko_ru.pdf

13. Diffie W. New directions in cryptography / W. Diffie, M. Hellman / IEEE Trans. Inform. Theory, 22 (1976). P. 644–654.