РИСКИ ГЕНЕРАЦИИ ПАРОЛЕЙ

Вельков Д. Е., Фролов Я. И., Гуринович А. Б.
Кафедра вычислительных методов и программирования, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: velkov@list.ru, iaroslav_frolov@mail.ru

Методы безопасного применения генерации случайных чисел в компьютерных технологиях и в банковском деле. Анализ наиболее популярных и безопасных сервисов для генерации паролей.

Введение

Случайные числа и случайность имеют множество применений в криптографии, науке, играх, искусстве. Для разных задач, требуется генерация разного качества, по этой причине существует потребность в разнообразных методах генерации случайных чисел. Генераторы случайных чисел (ГСЧ) делятся на два основных типа: Генераторы псевдосучайных чисел (ГПСЧ) и Генераторы случайных чисел (ГСЧ). С развитием информационных технологий и интернета, возросла потребность в качественной генерации случайных чисел, не только у специалистов, но и у обычных людей.

I. Генераторы псевдослучайных чисел (ГПСЧ) и Генераторы случайных чисел (ГСЧ)

Из-за простоты и дешевизны чаще всего используются генераторы, созданные как соответствующие программы на ЭЦВМ. С помощью этих программ по некоторому алгоритму получают последовательности чисел. Алгоритм построен так, что знаки 0 и 1 появляются в среднем одинаковое число раз и отсутствует зависимость между появлениями этих знаков и сформированными из них многозначными числами. Числа получаемые с помощью таких генераторов называются псевдослучайными. Генераторы истинно случайных чисел генерируют последовательности случайных чисел на основе измеряемых, хаотически изменяющихся параметров физического процесса. Работа таких устройств часто основана на использовании надёжных источников энтропии, таких, как тепловой шум, дробовой шум, фотоэлектрический эффект, квантовые явления, погодные явления и другие физические процессы.

II. Система безопастности банковских карт и Алгоритмы проверки PIN

PIN-коды для карт могут генерироваться 2 способами. Теперь же перейдём к способу проверки этих самых кодов. На данный момент, в основном, используются следующие 2 алгоритма проверки PIN: Visa PVV и IBM 3624 PIN offset. Visa PVV Данный алгоритм первоначально был разработан платежной системой Visa, но, в настоящее время является рекомендованным алгоритмом проверки PIN как для карт Visa, так и для MasterCard. В основе данного алгоритма лежит значение PVV (PIN verification value), которое является криптограммой, получаемой на основе следующих величин:

- Номер карты (далее PAN);
- Индекс ключа проверки PIN (PIN verification key index, далее, PVKI);
- Ключ проверки PIN (PIN verification key, далее, PVK)
- Сам PIN код карты.

Для получения PVV формируется блок из PAN (последние 11 цифр, кроме контрольного числа карты), PVKI, PIN (строго, первые 4 цифры), который зашифровывается с помощью PVK, после чего из него, с помощью специальной функции, извлекаются 4-х значное число, которое и является значением PVV [1]. Данное значение PVV является эталонным для проверки PIN кода. Т.е. при получении операции с введенным PIN для его проверки на основании PAN, PVKI, PVK формируется новое значение PVV и сравнивается с эталонным PVV для карты. Если значения совпадают, то PIN считается верным, если не совпадают — неверным. К особенностям данного алгоритма можно отнести следующие «ограничения»:

- Принципиальная невозможность восстановления PIN из значения PVV;
- Использование PIN кода размером строго 4 цифры.

IBM 3624 PIN offset Данный алгоритм первоначально был разработан компанией IBM для использования в банкоматах IBM 3624 В настоящее время данный алгоритм считается устаревшим, но используется по следующим причинам:

- карточные системы «старых» регионов (Западная Европа, Северная Америка) достаточно консервативны и, во многом, работают на «достаточно» старых системах;
- данный алгоритм позволяет восстановить значение PIN кода из проверочного значения.

В основе данного алгоритма лежит значение PIN offset (PIN verification value), которое является

криптограммой, получаемой на основе следующих величин:

- Контрольное значение (Validation data, далее VD) — некоторое значение (обычно — часть номера карты, но это не обязательно);
- Децимализационная таблица (Decimalization table, далее DT);
- Ключ проверки PIN (PIN verification key, далее, PVK);
- Сам PIN код карты.

Для простоты дальнейшего описания под ключом проверки PIN в случае метода IBM 3624 PIN offset будем совокупность ключа PVK и значения таблицы децимализации DT. Для получения PIN offset контрольное значение VD заширфовывается с помощью ключа PVK, после чего из полученного значения с помощью таблицы децимализации DT получается блок из 16 десятичных цифр. Из полученного блока берутся первые N цифр, где N — длина PIN (метод IBM 3624 позволяет проверять PIN с длиной до 16 цифр), далее из каждой цифры PIN по модулю 10 вычитается соответствующая цифра полученного блока. Полученное значение и будет значением PIN offset.

III. Проверка PIN

Терминология

Для упрощения дальнейшего описания введем некоторые термины:

- PIN блок — значение PIN кода карты, упакованной в блок из 8 байт;
- Зашифрованный PIN блок — значение PIN блока, зашифрованное по алгоритму DES/3DES выделенного для целей шифрования PIN блока;
- Проверочное значение PIN — PVV или PIN offset;
- Дополнительные данные проверки PIN — данные, кроме PIN и проверочного значения PIN, необходимые для проверки PIN в соответствии с алгоритмами Visa PVV/IBM 3624 PIN offset.

В части проверки PIN можно указать следующие требования:

- Открытые значения PIN и PIN блока не передаваться, храниться или обрабатываться вне специально отведенных программно аппаратных комплексов;
- Зашифрованный PIN блок — значение PIN блока, зашифрованное по алгоритму DES/3DES выделенного для целей шифрования PIN блока.

Как мы уже определились ранее, для проверки PIN нам необходимы следующие данные:

- Сам PIN, который мы будем проверять;
- Проверочное значение PIN;
- Дополнительные данные проверки PIN.

Открытое значение PIN нельзя получить ни при каких условиях. Имеется доступ только к зашифрованному PIN блоку. В дополнение к нему нужен ключ для его расшифровки. Этот ключ называют PPK (PIN protection key). Имеется два варианта хранения проверочного значания:

Первый вариант — это хранение проверочного значения на магнитной полосе карты после поля Service Code. Второй вариант — это хранение проверочного значения в некотором хранилище, обычно, БД системы, отвечающей за выполнение проверок при авторизации карты.

IV. Заключение

Независимо от мпомоба получения информации и получателя, проверка PIN выполняется на HSM, использующий для проверки ключ PPK в защищенном виде, ключ проверки PIN в защищенном виде, зашифрованный PIN блок, проверочное значение PIN и дополнительные данные проверки, в ответ на что возвращается только результат проверки: верный PIN, неверный PIN, прочая ошибка. Т.е. в процессе проверки система, отвечающая за авторизацию, не зависит от открытого значения PIN. Комбинация этих методов обеспечивает минимальные риски при использовании паролей. Для безопасной автоматической генерации паролей целесообразно использовать разнообразные интернет сервисы: Memset, Avast Passwords, ExpressVPN, Norton Password Manager, Random, ClaveSegura, Zoho Vault, Strong Password Generator. Это позволяет точно настроить генерацию, выбрать надёжный пароль и минимизировать риски.

V. Список литературы

1. Visa Payment Technology Standards Manual, Банковское мошенничество
2. Случайные числа и их применение, Иванова В.М., 1984.
3. https://www.belinvestbank.by/individual/page/moshennichestvo-v-seti-internet
4. Feller V. Introduction to the theory of probability and its applications. M.: Мир, 1984.Т.1,2.
5. Gane Samb LO. A Course on ElementaryProbability Theory/Statistics and Probability African Society, (SPAS) Books Series.Saint-Louis, Calgary, Alberta. 2016 – ISBN978-2-9559183-3-3, DOI: http://dx.doi.org/10.16929/sbs/2016. 0003 – 209 p
6. Charles M. Grinstead. Introduction to Probability / Swarthmore College . – 2009. – 520 p.
7. Dimitri P. Bertsekas. Introduction to Probability, lecture notes, Course 6.041-6.431/ Dimitri P. Bertsekas , John N. Tsitsiklis. – M.I.T ,2000– 284 p
8. Kramer G. Mathematical methods of statistics. Moscow: The World, 1976.