Куминов В.П., Сидоренко В.Г.

Решение задач анализа криптографической стойкости генераторов псевдослучайных чисел с использованием машинного обучения

Аннотация: В работе рассматривается использование методов машинного обучения для анализа и предсказания выходных данных криптографически стойких генераторов псевдослучайных чисел на примере алгоритма Fortuna. Проанализированы механизмы его стойкости, включая накопление энтропии и лавинный эффект. Выводы исследования подчеркивают высокий уровень безопасности криптографически стойких генераторов псевдослучайных чисел, что особенно важно для специалистов и студентов в области информационной безопасности.

Ключевые слова: криптографически стойкие генераторы псевдослучайных чисел, машинное обучение, энтропия, шифрование, Fortuna

В современном мире генераторы псевдослучайных чисел (ГПСЧ) играют важную роль в различных элементах IT-инфраструктуры. Они используются в самых разных областях: от розыгрышей ценных призов и случайного выбора победителя до сложных криптографических систем, обеспечивающих безопасность данных и требующих генерации ключа для шифрования информации, например RSA [1-2]. Одной из главных задач является генерация последовательностей чисел, которые максимально приближены к истинной случайности. Псевдослучайные генераторы, несмотря на свою «псевдо» природу, достаточно хорошо решают эту задачу в большинстве случаев, однако остаётся вопрос их устойчивости к предсказанию.

ГПСЧ можно разделить на два основных вида: криптографически стойкие (КСГПСЧ) и некриптографические. Некриптографические ГПСЧ ранее были исследованы на устойчивость к взлому с использованием методов машинного обучения (МО). Например, ГПСЧ xorshift128 быстро создаёт последовательности, которые выглядят случайными, но при

углубленном анализе удалось выявить закономерности, что делает алгоритм уязвимым для предсказания. С помощью МО удалось предсказать дальнейшие числа, зная только четыре предыдущих [1].

Возникает вопрос: можно ли с помощью тех же методов предсказать работу КСГПСЧ?

КСГПСЧ разрабатывались специально для того, чтобы противостоять предсказанию даже при наличии части выходной последовательности. Если такие генераторы так же можно будет успешно предсказать с помощью методов МО, это будет означать серьёзную уязвимость в системах, полагающихся на них для обеспечения безопасности. В данной работе исследуется возможность применения методов МО для анализа КСГПСЧ и предсказания их поведения на основе части выходных данных. Если предсказание окажется возможным, это укажет на необходимость пересмотра подходов к разработке таких алгоритмов. В противном случае, это подтвердит их стойкость и оправдает их использование в различных системах.

Для исследования был выбран алгоритм Fortuna, разработанный Брюсом Шнайером и Нильсом Фергюсоном. Исследуемый алгоритм представляет собой современный КСГПСЧ, более гибкий и безопасный по сравнению с его предшественниками, такими как Yarrow [2]. В отличие от своих предшественников, Fortuna использует несколько пулов энтропии, которые накапливают данные из различных источников, а также шифрование с использованием AES для генерации псевдослучайных чисел. Это делает его особенно интересным объектом для анализа с точки зрения возможности предсказания его работы методами машинного обучения.

Генерация случайных чисел в этом алгоритме осуществляется путём регулярного обновления состояния генератора и его шифрования. Каждое новое состояние шифруется и использует результаты шифрования для формирования псевдослучайных чисел. Благодаря использованию AES как основного криптографического примитива, предсказание будущих выходных данных становится крайне сложной задачей. Даже если часть выходных данных будет известна, это не даст злоумышленнику возможности восстановить внутреннее состояние генератора [3-4].

Одной из ключевых целей данного исследования является попытка определить, может ли нейронная сеть предсказать выходные данные Fortuna, анализируя часть последовательности. Ранее нейронные сети показали эффективность при работе с некриптографическими генераторами, такими как xorshift128 [1], которые содержали линейные зависимости, позволяющие находить закономерности. Однако в случае с криптографическими генераторами используются нелинейные криптографические примитивы и многослойные механизмы управления состоянием, что делает предсказание чрезвычайно трудным.

Важным элементом безопасности КСГПСЧ является использование энтропии как начального значения при генерации. Чем больше энтропии содержится в системе, тем труднее злоумышленнику предугадать последовательность выходных данных генератора. Fortuna собирает данные из множества источников энтропии, это могут быть системные события, ввод с клавиатуры, работа таймеров и аналоговые сигналы, и аккумулирует их в специальные пулы энтропии. Чем более равномерно распределены вероятности событий, тем выше энтропия системы и тем труднее предсказать, какие данные будут сгенерированы в будущем. В случае рассматриваемого алгоритма, данные поступают из множества независимых источников, и каждое из этих событий добавляет свою долю случайности, увеличивая общую энтропию.

Другим важным аспектом работы является использование AES для шифрования внутреннего состояния генератора. Каждое новое число, сгенерированное Fortuna, формируется на основе криптографического шифрования. Это шифрование вводит так называемый «лавинный эффект», при котором даже минимальное изменение во входных данных полностью изменяет выходные данные. Формально это можно выразить как:

$$\Delta_{out} = AES(K, M) \oplus AES\left(K, M^{'}\right), \quad (1)$$

где K – ключ шифрования;
M и M' – входные данные, отличающиеся всего на один бит;
Δ_{out} – разница между выходными значениями.

Этот лавинный эффект гарантирует, что любое небольшое изменение во внутреннем состоянии генератора приводит к радикальным изменениям в выходной последовательности. Таким образом, даже зная несколько предыдущих чисел, злоумышленник не сможет вернуться в исходное состояние генератора, поскольку вся последовательность шифруется с использованием стойких криптографических механизмов.

Когда накапливается достаточное количество энтропии, происходит перезапуск генератора, известный как reseed. Этот перезапуск полностью обновляет внутреннее состояние генератора, используя свежие данные из всех пулов энтропии, что делает предсказание выходных данных ещё более сложным. После перезапуска шифрование с использованием AES обеспечивает дополнительный уровень защиты.

Таким образом, процесс работы алгоритма Fortuna можно представить следующим образом. Сначала генератор собирает случайные данные из различных источников энтропии. Эти данные аккумулируются в пулы энтропии, и по мере их накопления происходит перезапуск генератора. Внутреннее состояние генератора шифруется с использованием AES, и сгенерированное число становится выходным результатом. Благодаря использованию как цифровых, так и аналоговых источников энтропии, каждая сгенерированная последовательность не зависит от предыдущей, что приближает работу Fortuna к истинной случайности.

В ходе рассмотрения возможности использования нейросети для предсказания выходных данных КСГПСЧ, были выделены несколько ключевых моментов для обсуждения. Нейросеть может быть обучена на данных, где входом будет зашифрованное число, а выходом – соответствующее внутреннее состояние генератора. В процессе обучения нейросеть может попытаться выявить закономерности и даже «угадать» ключ шифрования, который использует AES. Тем не менее, даже если нейросеть достигнет некоторого уровня предсказательной способности, её эффективность будет ограничена изменениями в ключе шифрования. Изменение ключа полностью разрушает любые выявленные закономерности, делая все предыдущие знания нейросети бесполезными.

Что касается возможности поймать момент, когда происходит перезапуск генератора (reseed), это также представляет собой сложную задачу. При каждом reseed внутреннее состояние обновляется, и данные из пулов энтропии хэшируются, создавая новое состояние. Если нейросеть пытается предсказать этот момент, она должна иметь доступ к достаточно большой выборке данных, чтобы выявить временные паттерны накопления энтропии. Однако, учитывая, что источники энтропии очень разнообразные, надежно поймать момент перезапуска будет практически невозможно.

В ходе данного исследования сделан первый шаг к пониманию неэффективности методов машинного обучения при попытках предсказания выходных данных КСГПСЧ. Обсуждены механизмы, делающие предсказание крайне сложной и ресурсоёмкой задачей. Даже незначительные изменения во входных данных приводят к радикально различным выходным значениям. Рассмотренные факторы показывают высокий уровень безопасности КСГПСЧ по сравнению с некриптографическими генераторами.

Несмотря на то, что сделан первый шаг в исследовании стойкости КСГПСЧ к атакам с использованием машинного обучения, ограничения по размеру статьи не позволяют углубиться в этот материал более подробно. В будущих исследованиях планируется более детально рассмотреть методы криптоанализа, возможности компрометации источников энтропии и аппаратные уязвимости в реализации генераторов [5]. Выводы данного исследования могут быть полезны студентам в области информационной безопасности и тем, кто использует ГПСЧ, но не осведомлён о различиях между криптографически стойкими и некриптографическими ГПСЧ. Понимание этих различий важно для обеспечения надёжности и безопасности систем, полагающихся на случайные числа в таких разделах, как криптография, защита данных и безопасная аутентификация. Дальнейшие исследования помогут углубить знание о механизмах работы ГПСЧ и их уязвимостях.

Литература:

1. *Куминов В.П., Сидоренко В.Г.* Методы оценки качества генераторов псевдослучайных чисел / Интеллектуальные транспортные системы: Материалы III Международной научно-

практической конференции, Москва, 30 мая 2024 года. – Москва: Российский университет транспорта (МИИТ), 2024. – С. 631-636. – DOI: 10.30932/9785002446094-2024-631-636.

2. *Schneier B., Ferguson N.* Fortuna. A secure pseudorandom number generator. – URL: https://www.schneier.com/academic/fortuna/ (дата обращения 25.09.2024).

3. *Романков С.В.* Методы генерации псевдослучайных чисел // Молодой ученый. – 2022. – № 33 (428). – С. 4-10. – URL: https://moluch.ru/archive/428/94534/ (дата обращения 25.09.2024).

4. *Schneier B., Ferguson N., Kohno T.* Cryptography Engineering: Design Principles and Practical Applications. – Indianapolis: Wiley Publishing, 2010. – 384 p.

5. *Netdata Cloud.* Understanding entropy: the key to secure cryptography and randomness. – URL: https://www.netdata.cloud/blog/understanding-entropy-the-key-to-secure-cryptography-and-randomness/ (дата обращения 25.09.2024).

Ведмедева М.В., Миронова В.Г.

Эволюция информационных систем: от простых решений к комплексным инфраструктурам

Аннотация: В работе рассматриваются особенности отказоустойчивости и безопасности информационных систем в условиях увеличения числа кибератак и расширения поверхности атак. Особое внимание уделено сравнению простых и сложных ИС, их функциональным возможностям, масштабируемости и уровням безопасности. Выявлены основные проблемы, связанные с использованием устаревших методов защиты, и предложены подходы для повышения устойчивости современных ИС.

Ключевые слова: информационные системы, киберугрозы, поверхность атаки, отказоустойчивость, безопасность данных, модели угроз, масштабируемость, безопасность