СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ОБФУСКАЦИЯ JAVASCRIPT КОДА

М.А. БАРТОШИК

Обратное проектирование позволяет анализировать и модифицировать механизмы защиты приложений с целью их несанкционированного использования, что указывает на необходимость разработки технических методов защиты исходного кода.

Лексическая обфускация включает в себя изменение имен идентификаторов, строковых констант, форматирования кода и использование нестандартных кодировок. Данный метод усложняет процесс обратного проектирования, уменьшает объем кода и может повысить производительность приложения.

Методы синтаксической обфускации основываются на модификации потока управления программы. Данные методы, как правило, приводят к ухудшению производительности и не могут применяться в критических для скорости выполнения участках кода. Среди наиболее эффективных методов можно выделить: применение непрозрачных предикатов, добавление «мертвого» и избыточного кода, смешивание и клонирование функций, вставка операторов функций по месту вызова и вынос группы операторов в отдельную функцию, изменение области действия переменных, развертка циклов, подмена вызовов встроенных функций, использование нестандартных способов исполнения кода (eval, Function, setTimeout).

При применении обфускации необходимо учитывать особенности JavaScript: динамическая типизация, доступность исходного кода злоумышленнику, возможность автоматической модификации кода через прокси-сервер, наличие инструментов отладки и анализа потока управления, отличия реализации стандартных функций в браузерах.

В общем случае применение обфускации дает лишь временную защиту приложения от взлома. В случае с JavaScript существует возможность применять различный случайный набор преобразований с определенной периодичностью (например, раз в сутки). Такой подход может сделать взлом приложения нерентабельным.

К РЕШЕНИЮ УРАВНЕНИЙ НАД ПОЛЯМИ ГАЛУА. СОГЛАСОВАНИЕ ПРИМИТИВНЫХ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ И ЕГО РАСШИРЕНИЯ

В.А. БОГРЕЦОВ, В.А. ЛИПНИЦКИЙ

Теория конечных полей Галуа играет большую роль в современной теории помехоустойчивого кодирования и криптографии. Особое место занимают в данных областях алгоритмы решения полиномиальных уравнений над названными полями. Общеизвестно, например, что в процессе декодирования БЧХ-кода, наиболее ресурсоёмкой процедурой является нахождение корней полинома локаторов ошибок [1]. Ещё одним интересным примером, показывающим значимость эффективных алгоритмов решения полиномиальных уравнений в конечных полях, является криптосистема McEliece [2], основанная на применении двоичных кодов Гоппы. Одним из этапов расшифровки сообщения в данной системе является решение полиномиального уравнения над полем Галуа. Данный этап занимает до ¾ всего времени процесса расшифровки. В [3] описан алгоритм решения кубического уравнения в поле Галуа характеристики 2. В основе данного алгоритма лежит сведение исходного уравнения к квадратному, которое может быть решено одним из методов, описанных в [4]. Затем, по найденным корням квадратного уравнения, восстанавливаются корни исходного уравнения. Если степень исходного поля

как расширения простого поля характеристики 2 является нечётным числом, то квадратное уравнение требуется решать в квадратичном расширении исходного поля. В [3] предлагается метод, позволяющий осуществлять переход от квадратичного расширения к его подполю. Однако данный метод приводится без доказательства и, к сожалению, работает не во всех случаях. Существует и иной, более чёткий, способ перехода от расширения к подполю. Он основан на согласовании примитивных элементов мультипликативной группы поля и его расширения. Важным моментом является то, что данный способ может без изменений быть применён не только к квадратичным расширениям конечных полей, но и к произвольным циклическим группам и их подгруппам. В основе рассматриваемого подхода лежит тот факт, что для любого целого x, взаимно простого с целым m, и для любого целого n существует целое t такое, что t взаимно просто с mn и при этом t сравнимо с x по модулю m. Доказательство данного факта выводится из китайской теоремы об остатках.

Литература

1. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007. 239 с.
2. *McEliece R.J.* A public-key cryptosystem based on algebraic coding theory // Technical Report DSN 42-44, JPL, Pasadena, 1978.
3. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. Л., 1990. 288 с.
4. *Богрецов В.А., Липницкий В.А.* Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара. Минск, 2012. С. 57–64.

АНАЛИЗ УЛУЧШЕННОГО АЛГОРИТМА ФОРМИРОВАНИЯ ОБЩЕГО КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н.В. БРИЧ

Создание канала защищенной передачи информации является одной из актуальных задач в различных сферах в настоящее время. Обобщенно защищенная передача может быть описана следующим образом: отправитель зашифровывает сообщение ключом так, что злоумышленник не может прочитать либо внести изменения в передаваемое сообщение. одним подходом в формировании общего секретного ключа является использование искусственных нейронных сетей (ИНС). ИНС — математические модели, программные и аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей. Одним из главных преимуществ нейронных сетей является возможность обучения и синхронизации. Синхронизированные ИНС — ИНС, весовые коэффициенты (ВК) которых одинаковы. Время, необходимое для синхронизации ИНС, много меньше времени, затрачиваемого на обучение ИНС. На основании этого свойства И. Кантер и В. Кинцель предлагают идею использования ИНС для решения проблемы распределения общего секретного ключа. На практике доказано, что изначально алгоритм обладает некоторыми уязвимостями, на основании которых применяется несколько типов атак — с использованием одной ИНС (методом грубой силы, геометрическая) и с использованием нескольких ИНС. Предлагается алгоритм, при использовании которого уменьшается время, необходимое для вхождения ИНС в синхронизм (соответственно, увеличивается криптостойкость протокола). ИНС в процессе синхронизации стремятся подавить вклад тех весовых коэффициентов (ВК),значения которых ошибочны — т.е. работа канала связи для этих весов неэффективна. Соответственно, корректируя ВК для персептрона с наименьшим значением весового коэффициента, мы с большой вероятностью производим шаг к сближению ВК обеих ИНС.При использовании ИНС для формирования общего ключа необходимо вдумчиво