3412_2015_rezhimy_raboty_blochnyh_shifrov_gost_3413_2015. Дата доступа: 23.03.2023.

4. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 1. Кодирование информации: учеб.-метод. пособие для студентов учреждений высшего образования / П. П. Урбанович, Д. В. Шиман, Н. П. Шутько. – Минск: БГТУ, 2019. – 116 с.

УДК [004.056+003.26] (075.8)

Студ. А.К. Карбанович
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ЗАЩИТА WEB-ПРИЛОЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ НА ОСНОВЕ СТЕГАНОГРАФИИ И СТАНДАРТА КОДИРОВАНИЯ BASE64

Проблема защиты web-приложений от несанкционированного использования является актуальной, поскольку с ростом числа пользователей интернет растет и ущерб от утечки конфиденциальной информации [1]. Защита от несанкционированного использования сводится к проблеме защиты от несанкционированного доступа, так как второе предшествует первому.

Стеганография в общем смысле слова обозначает – такой способ передачи или хранения информации, при котором скрывается сам факт этой передачи или хранения, а в применении к цифровой стеганографии – использует различные способы сокрытия данных в изображениях, тексте, аудио/видео -файлах, защиту авторских прав на основе встраивания цифрового водяного знака [2, 3]. Base 64 – это стандарт, который позволяет кодировать информацию, представленную набором байт, используя всего 64 символа ASCII.

Рассмотрим следующие способы защиты web-приложений:

1. Метод, основанный на алгоритме AESи LSB [4]. Алгоритм шифрования и встраивания: текст шифруется с помощью симметричного алгоритма блочного шифрования AES и представляется в виде Base64-строки – это и будет шифротекст. Полученный шифротекст переводится в двоичный вид и встраивается в изображение с помощью LSB. Процесс дешифрования обратный шифрованию.

2. Алгоритм, основанный на подходе End-of-File [5]. Сообщение переводится в Base64-строку, к нему добавляется символ End-of-File (00000011). Полученная строка вставляется в изображение с помощью

стеганографического метода изменения конечного бита голубого цвета пикселя. Декодирование происходит обратным образом покуда не обнаружится символ EndofFile.

3. Комбинация алгоритма RC4, Base64и LSBдля сокрытия данных пользователя [6]. Пользователь вводит сообщение и добавляет изображение, в которое впоследствии будет встроен шифротекст. После валидации данных, сообщение шифруется с помощью потокового шифра RC4 и кодируется в Base64-строку. Полученный шифротекст вставляется в загруженное пользователем изображение с помощью метода LSB. Стегоконтейнер в виде изображения может быть сохранен на устройстве или отправлен на сервер. Тонкости хранения секретного ключа для шифрования или способ встраивания сообщения в контейнер не так важны в данном случае. Главное – общий алгоритм. Конечно, если же эти способы не являются ключевыми при рассмотрении.

Три приведенных способа защиты информации на основе стеганографии и стандарта кодирования Base64 являются наиболее популярными. Существуют и другие разновидности, которые не сильно отличающиеся от выше описанных. Используются, в основном, при передаче информации, так как не затрагивают место, где хранится практически вся информация в web-приложениях – базу данных (БД).

Основная идея нашего предложения состоит в том, чтобы вынести конфиденциальные данные из прямого хранения в ячейке БД и спрятать их в изображениях, файлах и других контейнерах, предварительно зашифровав их. Это обеспечит высокую безопасность при утечке информации из БД, так как данные не хранятся напрямую, а спрятаны.

Преимущества данного подхода:

– при утечке БД конфиденциальные данные остаются защищенными;

– при раскрытии местоположения стегоконтейнера, злоумышленник не сможет узнать сам контент, так как данные зашифрованы;

– защищаются сразу вся конфиденциальная информация, в то время как при передаче данных в вышеописанных подходах – лишь небольшая часть.

Недостатки:

– скорость работы. Данный подход будет медленнее работать, чем если напрямую хранить данные в БД;

– неэффективное использование ресурсов. Помимо самих данных, надо хранить контейнеры, которые могут не нести полезной информации, а использоваться лишь в виде контейнера;

– требования к предоставлению пользователем контейнеров, либо же предварительное их хранение на сервере.

Описанный подход хорошо подойдет для небольших приложений, которые используют личную информацию о пользователях, к примеру адрес электронной почты, мобильный телефон, дату рождения, адрес проживания и т.д. Все эти данные легко можно хранить в предоставляемых пользователем контейнерах и при взломе БД, они останутся в безопасности.

Понятие небольшого приложения требует пояснения. Это такое приложение, при котором доступ к контенту будет сравним по времени или немного отличаться в большую сторону по отношению к приложению, хранящему данные напрямую в БД. Это обосновано тем, что скорость работы является одним из ключевых требований, предъявляемых к web-приложениям и при его несоблюдении приложение будет неконкурентоспособным.

ЛИТЕРАТУРА

1. InternetGrowthStatistics [Электронный ресурс]. – Режим доступа:https://www.internetworldstats.com/emarketing.htm. – Дата доступа: 15.04.2023.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

3. Блинова, Е. А., & Урбанович, П. П. (2021). Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG. Журнал Белорусского государственного университета. Математика. Информатика, 3, 68-83. https://doi.org/10.33581/2520-6508-2021-3-68-83

4. StegoCrypt Scheme using LSB-AES Base64 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/profile/De-Rosal-Ignatius-Moses-Setiadi/publication/338362617_StegoCrypt_Scheme_using_ LSB-AES_Base64/links/5e16a00c92851c8364bd472a/StegoCrypt-Scheme-using-LSB-AES-Base64.pdf. – Дата доступа: 19.04.2023.

5. Base64, End of File and Steganography to Improve Security in Website [Электронный ресурс]. –Режим доступа: https://nceca.in/2021/49Base64_End_of_File_and_Steganography_to_Improve_Security_in_Websites.pdf. – Дата доступа: 17.04.2023.

6. Combination RC4 Algorithm and Base64 Encryption on The Least Significant Bit Method [Электронный ресурс]. –Режим доступа: https://www.academia.edu/98005578/Combination_RC4_Algorithm_and_Base64_Encryption_on_The_Least_Significant_Bit_Method. – Дата доступа: 19.04.2023.