Список литературы

1. Gallager R.G. Low Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.
2. Jian-Bing H.A.N., Chen H.E., He Yun H.E. Research on regular LDPC codes with better performance than turbo codes // Materials of International Conference on Information Engineering ICIE '09.

ИНВАРИАНТНОСТЬ ЦИФРОВОГО ОТПЕЧАТКА УСТРОЙСТВА ПОЛЬЗОВАТЕЛЯ, ИСПОЛЬЗУЕМОГО ДЛЯ ЕГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

О.А. Хожевец, Т.В. Борботько

Идентификация пользователя информационных ресурсов предполагает использование некоторой уникальной информации, которая известна непосредственно пользователю, а также хранится в информационной системе для выполнения процедуры его аутентификации. В качестве такой информации выступает, как правило, некоторые сведения (логин, пароль и т.д.) вводимые пользователем для проверки его подлинности.

Учитывая особенности программных средств, применяемых пользователями сети интернет для доступа к информационным ресурсам, можно выделить следующие признаки таких средств, позволяющих выполнить процедуру идентификации его устройства: javascript, user agent, IP, flash, ActiveX, содержание кэша браузера, cookie, supercookie, настройки используемого программного обеспечения. Формирование из вышеперечисленных признаков массива данных и вычисление его хэш суммы позволяет получить цифровой отпечаток (фингерпринт) устройства пользователя, который будет неизменным в течение достаточно длительного времени.

Необходимо отметить, что во всех существующих браузерах есть широкий спектр переменных с большой инвариантностью, которые позволяют, даже не подготовленному пользователю, изменять цифровой отпечаток своего устройства перед подключением к информационному ресурсу. Наиболее простыми способами, являются: использование нового браузера или новой версии, изменение масштаба окна браузера, изменение часового пояса устройства, изменение языка браузера. Экспериментально установлено, что варьируя значениями указанных переменных можно получить от 1000 до 230000 уникальных цифровых отпечатков устройства, в зависимости от используемого браузера. Таким образом, для снижения ошибок первого и второго рода необходимо формировать базу цифровых отпечатков устройства пользователя, которая, в дальнейшем, может быть использована для его идентификации.

БЕЗОПАСНОСТЬ REACT-ПРИЛОЖЕНИЙ

М.П. Хоронеко, Н.В. Харитонов, М.А. Медунецкий, В.Я. Анисимов

ReactJS – самая популярная JavaScript библиотека для построения пользовательских интерфейсов по данным Google Trends на 2019 год [1]. Приложения на ее основе используют большое количество js-кода, поэтому справедливо предположить что атаки типа XSS могут принести злоумышленникам определенный результат.

Практика использования ReactJS в мире показывает, что библиотека содержит большое число компонентов поддержания безопасности приложения. Например, спецсимволы, без которых невозможно осуществить XSS атаку, автоматически заменяются управляющей последовательностью при их использовании в строчных значениях в JSX (синтаксис, подобный HTML, в основе которого лежат теги, позволяющий использовать JS-код непосредственно при построении разметки) [2]. Тем не менее, проблемы, связанные с внедрением скриптов, могут быть результатом использования неподходящих практик программирования и не всегда являются очевидными. Среди них:

– создание React-компонентов из объектов, поставляемых пользователем;
– отображение ссылок с href-атрибутом, определяемым пользователем;
– явное задание свойства dangerouslySetInnerHTML у элемента;

– передача пользовательской строки в функцию eval();
– неправильная реализация серверной отрисовки (SSR).

Несмотря на то, что ReactJS сама по себе является довольно продвинутой с точки зрения защиты от внедрения скриптов библиотекой, основная ответственность по обеспечению безопасности приложения ложится на команду разработки. Только внимательность, осведомленность и использование верных подходов, а также тщательное и регулярное тестирование безопасности продукта может гарантировать его надежность.

Список литературы

1. Thomas M. React in Action. Manning Inc., 2018. 5 p.
2. Geary D. Building React.js Applications with Redux. Syngress Publishing, 2018. 29 p.

ВЛИЯНИЕ ИСКАЖЕНИЙ ИЗОБРАЖЕНИЯ НА РЕШЕНИЕ ЗАДАЧИ РАСПОЗНАВАНИЯ

Н.В. Царенков, А.В. Сергеенко, А.Ю. Липлянин

На сегодняшний день обработка изображений является неотъемлемой частью нашей повседневной жизни. Она используется в системах охраны государственных границ и общественного порядка, медицинской техники, системах контроля за лесными ресурсами и др. К задачам обработки изображений относятся распознавание образов и объектов, восстановление изображений, фильтрация, оценка параметров изображения, сжатие изображений. Одним из наиболее активно развивающихся, но при этом наиболее трудоемких и сложных с научной точки зрения направлений является распознавание объектов. Для решения данной задачи широкое распространение получили оптоэлектронные системы распознавания.

В реальных оптоэлектронных системах изображения непременно подвергаются воздействию дестабилизирующих факторов. Такими факторами выступают [1]: помехи сенсора, движения наблюдаемого объекта, погодные условия, оптические дефекты объективов и т.д. Например, воздействие природных явлений, таких как турбулентность атмосферы, погодные условия, а также перемещение объекта наблюдения негативно сказываются на качестве изображений (вызывая расфокусировку, помехи и смазывание), и, как следствие, снижают эффективность работы системы распознавания (не зависимо от метода распознавания). Снижение эффективности работы системы распознавания влечет за собой снижение качества работы всей системы охраны в целом.

Для компенсации воздействия мешающих факторов применяется предварительное восстановление изображения. Для предварительного восстановления изображения могут использоваться различные методы, основанные на пространственной и частотной фильтрации и др [2]. Использование данных методов позволяет улучшить качество изображения, при чем критерий качество выбирается исходя из целевой функции оптической системы. Улучшения качества изображения влечет улучшение эффективности работы системы распознавания. Исходя из вышесказанного, можно сделать вывод, что внедрения этапа восстановления изображений в системы распознавания, а также совершенствование существующих методов и алгоритмов восстановления изображений, применяемых в данных системах, является сложной и важной задачей. Выполнение которой влечет за собой увеличение эффективности работы различных систем в состав которых входят системы распознавания, например, системы охраны общественного порядка.

Список литературы

1. Бейтс Р., Мак-Доннелл М. Восстановление и реконструкция изображений. М.: Мир, 1989. 336 с.
2. Анализ методов восстановления оптико-электронных изображений, смазанных при движении / А.Ю. Липлянин [и др.] // Доклады БГУИР. 2018. № 2. С. 40–46.