процедура P_N, представляющая основную программу (главный блок begin…end, функцию ёmain() и т.п.). Вычисленные оценки формальных параметров P_N (им соответствуют поступающие от пользователя данные) должны иметь значение «опасный». Параметры, для которых это не выполняется, являются потенциально уязвимыми. Анализируя путь, по которому была получена оценка, можно выявить причину возникновения уязвимости и предложить способы её устранения.

В общем случае можно сформулировать 5 правила, описывающие процесс назначения оценок и проверки web-приложения на наличие уязвимостей к SQL-инъекциям.

1. В качестве in-параметра с оценкой S должны передаваться только данные, имеющие оценку S.
2. В качестве in-параметра с оценкой U могут передаваться любые данные.
3. Переменным, переданным в процедуру в качестве out-параметров, назначается оценка, совпадающая с оценкой соответствующего out-параметра процедуры.
4. При наличии у переменной или out-параметра нескольких различных оценок выбирается «наихудшая», т.е. в случае бинарной оценки предпочтение отдаётся оценке U.
5. При наличии у in-параметра нескольких различных оценок выбирается «наилучшая», т.е. в случае бинарной оценки предпочтение отдаётся оценке S.

Предлагаемая модель позволяет обнаруживать не только эксплуатируемые, т.е. действительно позволяющие злоумышленнику провести атаку, уязвимости, но и потенциальные — не позволяющие провести атаку в данной версии приложения, но способные стать эксплуатируемыми после внесения изменений в исходный код web-приложения, причём необязательно в проблемный участок кода.

Между тем, поскольку в некоторых случаях процедуры web-приложения могут, выполняя определённые преобразования, произвести фильтрацию данных, которая не будет распознана в рамках модели, целесообразно предусмотреть дополнительную оценку UDS (User-Defined Safe), которая позволит программисту явно обозначить те или иные параметры процедур, как безопасные, независимо от результатов анализа. Использование такой оценки позволяет сократить число ложных срабатываний.

Предложенная модель может использоваться как в качестве самостоятельного инструмента, для анализа web-приложений на предмет уязвимости к SQL-инъекциям, так и в качестве вспомогательного инструменты при обеспечении качестве web-приложений, поставляющего исходные данные (сведения о количестве и расположении проблемных участков кода) для модели качества.

Список использованных источников:

1. OWASP Top 10-2013. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. — Режим доступа: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf. — Дата доступа: 31.10.2013.

АЛГОРИТМ ПОВЫШЕНИЯ ТОЧНОСТИ ЗАШУМЛЕННЫХ ГЕОДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Базаревский В.Э.

Бранцевич П.Ю.,к.т.н, доцент

Развитие социальных сетей, а так же мобильных технологий (в том числе повсеместное внедрение точных акселерометров, компасов и gps-локаторов) позволило с относительно малой трудоемкостью создавать удобные геоприложения различной бизнес-направленности.

В качестве одного из таких приложений может быть рассмотрено приложение поиска субъекта в незнакомой местности (например,это может быть новый незнакомый район или город во время заграничнойпоездки). К сожалению, не смотря на относительную точность датчиков современных мобильных устройств (погрешность 50 м), этого недостаточно для точного определения “визави” в людных местах, когда на площади 50*50 метров может находиться несколько сотен людей. Более того, точность такого геопозиционирования зачастую оказывается еще меньше в помещениях, что объясняется искажением магнитных полей от железобетонных конструкций, а так же искажением распространения радиоволн в разных материалах.

Зачастую, основным решением, предлагаемым в качестве решения проблемы точности геопозиционирования является использованием так называемых beacon-ов, датчиков, работающих по bluetooth протоколу на небольшом расстоянии (при этом мобильное устройство так же может выступать в качестве beacona). Такой подход хорошо работает при необходимости обнаружить, в какой конкретно геоточке находится пользователь в данный момент с большой точностью (такой подход используется, например, при показе таргетированной рекламы в торговых центрах), однако плохо работает при поиске необходимой конкретной точки. Это объясняется тем, что beacon-ы работая по bluetooth протоколу могут сообщать информацию только о том, насколько силен сигнал до beacona, с возможностью последующей аппроксимации этих данных в расстояние до устройства. Такимобразом возможно получение только метрики приращения расстояния, без возможности получения информации о изменении относительных координат

объекта по осям x,y,z. Более того, так как beacon-ы работают по протоколу bluetooth, на больших расстояниях до объекта (более 5-10 метров) данные о сигнале так же подвержены искажениям при распространении сигнала в пространстве.Следовательно, существующие аппаратные возможности мобильных устройств не могут быть использованы для установления точных координат пользователя.

С другой стороны, если проанализировать цели приложения можно выделить несколько факторов:

а) целью приложения является определение относительных координат визави, а не абсолютных;

б) так как оба устройства находятся примерно в одном и том же месте, возможно допущение, что иногда относительное искажение обоих характеристик может быть одинаковым.

Таким образом, рассматривая каждую из характеристик как сильно зашумленную, с помощью фильтра Калмана и существующих данных об абсолютных координатах, скорости каждого из устройств, расстояния между ними (измеренного на каждом из устройств), а так же изменения положения устройства относительно компаса можно построить математическую модель, значительно уточняющую направление, в котором находится устройство визави.

Список использованных источников:

1. Ingvar Strid & Karl Walentin (2009), (Block Kalman Filtering for Large-Scale DSGE Models), Computational Economics (Springer) . — Т. 33 (3): 277–304
2. Martin Møller Andreasen (2008), (Non-linear DSGE Models, The Central Difference Kalman Filter, and The Mean Shifted Particle Filter)

ПРИМЕНЕНИЕ МЕТОДОВ ЛИНЕЙНОЙ КЛАССИФИКАЦИИ ДЛЯ ИДЕНТИФИКАЦИИ ПЛИС

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Витенко А. А.

Иванюк А. А. – д-р. техн. наук, профессор

В данном докладе рассматривается применение методов линейной классификации для решения задач идентификации программируемых логических интегральных схем (ПЛИС) по импульсам, генерируемым аппаратной реализацией физически неклонируемых функций. Приводятся и анализируются результаты экспериментальных исследований классификации выходных сигналов физически неклонируемых функций типа RO-PUF, реализованных для FPGA Xilinx SPARTAN-3E и Artix 7.

В наше время из-за глобализации индустрии производства цифровых устройств остро встал вопрос их защиты от несанкционированного копирования или модификации. В процессе производства возможно внесение изменений, которые могут существенно влиять на работу устройства: похищать информацию, изменять логику, вплоть до полного отключения устройства по какому-то событию. Пользователь должен убедиться в том, что он может доверять этому устройству, что он использует именно то устройство, которое задумывал разработчик.

Одним из механизмов борьбы с этим является использование физически неклонируемых функций, которые основаны на использовании непредсказуемых и невоспроизводимых отклонений в физической структуре интегральной схемы при её производстве. Одной из возможных реализациий физически неклонируемой функции является кольцевой осциллятор (RO-PUF). Он состоит из нечётного числа инверторов, объединённых в цепь. Выходной сигнал с последнего инвертора подаётся на вход первого. За счёт задержек, возникающих при переключении состояния элемента, эта цепь начинает генерировать импульсы. Параметры импульса зависят от числа элементов, включённых в цепь. С увеличением количества элементов, суммарная задержка растёт, и частота генератора снижается. А из-за непредсказуемых отклонений в физической структуре интегральной схемы даже генераторы, состоящие из одного числа элементов и размещённые на одном кристалле, дают на выходе сигналы с разной частотой, которая незначительно меняется со временем.

Это особенность была использована для генерации большого объёма тестовых данных. На одном кристалле размещалось от нескольких десятков до нескольких сотен генераторов. В качестве характеристики генератора бралась длительность замера и число зарегистрированных возрастающих фронтов сигнала. Повторные измерения с увеличением длительности замера проводились для каждого компонента Эти параметры составили пространство признаков. Таким образом, вектор признаков для каждого объекта состоит из двух атрибутов: время замера и число зарегестрированных возрастающих фронтов сигнала.

В ходе изучения известных методов классификации был выбран метод опорных векторов (SVM), также известный как метод классификатора с максимальным зазором. Основная идея метода – перевод исходных векторов в пространство более высокой размерности и поиск разделяющей гиперплоскости с максимальным зазором между классами. Изначально метод опорных векторов – это линейный бинарный классификатор. Однако он может быть использован и для классификации объектов, принадлежащих более чем двум классам. Достигается это при помощи использования различных стратегий (one-versus-one, one-vs-rest). Для перевода векторов признаков в другое пространство используются различные функции ядра.