Литература

1. Машинное обучение и искусственный интеллект: итоги за 2017 год [Электронный ресурс] – URL: https://dev.by/lenta/main/iskusstvennyy-intellekt-i-glubokoe-obuchenie-itogi-za-2017-god. (дата обращения: 17.05.2018).

МЕТОДЫ И МОДЕЛИ ДЛЯ СХЕМОТЕХНИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИБОРОВ СИЛОВОЙ ЭЛЕКТРОНИКИ

В.Т. Ханько, В.Р. Стемпицкий

Электрические модели полупроводниковых приборов силовой электроники являются важнейшим элементом для надежного и точного моделирования силовых электронных схем [1]. В течение последних 10 лет к самому перспективному поколению электрических моделей можно отнести модели семейства HiSIM, которые основаны на анализе поверхностного потенциала в качестве переменной состояния, что позволяет исключить региональный подход к построению моделей и использовать единое физически обоснованное выражение для подпороговой области вольт-амперной характеристики (ВАХ), а также области умеренной и сильной инверсии. Данный подход позволяет охватывать большое количество разнообразных структур устройств, таких как высоковольтный полевой МОП-транзистор или биполярный транзистор с изолированным затвором. Существует 5 электрических моделей, предназначенных для схемотехнического моделирования приборов силовой электроники: HiSIM-HV, HiSIM-UMOS, HiSIM-SJ, HiSIM-Diode, HiSIM-IGBT [2]. Данные электрические модели пользовались низким спросом до недавнего времени, поскольку поведение силовых цепей в основном определялось внешними емкостями и индуктивностями, а точность сигналов была несущественной из-за низких частот переключения, потери мощности были обусловлены статическим сопротивлением. Постепенно все изменилось, поскольку для современных силовых цепей с низкими потерями мощности, которые применимы в автомобильной электронике, мобильной связи, в интеллектуальных сетях с использованием возобновляемых источников энергии, очень важны более высокие частоты переключения.

От модели и области ее применения зависят методы. В зависимости от цели моделирования применяют стратегии экстракции параметров, отличающихся по числу используемых приборов (по группе транзисторов, по одному транзистору) и типу оптимизации параметров модели (с помощью глобальной оптимизации или локальной оптимизации).

В качестве примера была проведена экстракция параметров модели HiSIM-IGBT. Относительная погрешность схемотехнического моделирования с использованием экстрагированного набора параметров в сравнении с экспериментальными данными составила не более 7 %.

Литература

1. Денисенко В. Компактные модели МОП-транзисторов для SPICE в микро- и наноэлектронике. Москва : ФИЗМАТЛИТ, 2010. 408 с.

2. The HiSIM compact models of high-voltage/power semiconductor devices for circuit simulation / H.J. Mattausch [et al.] // IEEE 12th International Conference on Solid-State and Integrated Circuit Technology. 2014. P. 1415–1418.

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ BLOCKCHAIN

И.В. Хмурович, Ю.А. Скудняков

Одним из современных способов защиты информации является blockchain. Особый вид ведения реестра и учета при помощи криптографии имеет множество очевидных достоинств. Основные преимущества – это сложность фальсификации внесенных в систему blockchain данных и наличие информации у всех участников, подключенных к системе. Технология blockchain предлагает более безопасные транзакции, защиту от определенных хакерских атак и даже, в определенной степени, избавляет от необходимости паролей. Все данные blockchain хранятся на компьютерах пользователей blockchain-сети. Все пользователи сети равноправны и могут делать все, что угодно, в том числе безуспешно пытаться обмануть других

пользователей [1]. Запретить им никто не может, потому что все находятся в равных условиях, обладают равными правами и могут в равной степени исполнять и даже нарушать свои обязанности. Все пользователи blockchain образуют собой сеть компьютеров, на каждом из которых хранится копия данных blockchain. Обычно это полная копия всех блоков, но, в принципе, можно хранить лишь нужные на конкретном компьютере данные. Благодаря этому выключить или сломать blockchain практически невозможно, поскольку для этого надо выключить или сломать все компьютеры. Пока есть хоть один пользователь, blockchain существует [1]. Каждый новый пользователь расширяет и укрепляет эту сеть. Причем все компьютеры равноправны, там нет организаторов, модераторов, контролеров и менеджеров. Каждый отвечает за себя сам. Криптография – это основа blockchain, которая обеспечивает работу системы. Криптография в blockchain гарантирует безопасность, причем основанную на прозрачности и проверяемости всех операций. Различные криптографические техники гарантируют неизменность журнала транзакций blockchain, решают задачу аутентификации и контролируют доступ к сети и данным в blockchain в целом. Исходя из вышеизложенного, можно сделать вывод о том, что использование описанной технологии позволяет достаточно надежно осуществлять защиту информации. Рассмотренная технология достаточно успешно используется авторами работы.

Литература

1. Antonopoulos, A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014. 298 p.

МЕТОДЫ ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ

М.П. Хоронеко, М.А. Медунецкий, А.С. Летохо

SQL-инъекции были и остаются наиболее критичными уязвимостями приложений. Обычно атаки типа SQL-инъекций рассматривают относительно web-приложений, однако данной уязвимости подвержены любые клиент-серверные и сервис-ориентированные приложения, работающие с системами управления базами данных. SQL-инъекция – это атака, при которой злоумышленник производит вставку вредоносного кода в строки, передающиеся на сервер СУБД для синтаксического анализа и выполнения. Данная уязвимость состоит в том, что веб-приложение некорректно проверяет данные от пользователя, которые в дальнейшем используются для генерации SQL-запросов к базе данных.

SQL-инъекции можно классифицировать следующим образом:

1) по месту нахождения в запросе (инъекции в строковом параметре и в числовом параметре);

2) по способу внедрения инъекции (обычные и «слепые»).

Для успешного внедрения SQL-инъекций необходимо знать следующие параметры: способ передачи данных в веб-приложении, тип и версию СУБД, имя текущего пользователя, назначенные роли и системные привилегии.

В зависимости от назначенных текущему пользователю ролей и привилегий злоумышленник может попытаться извлечь хэши паролей пользователей СУБД, получить структуру БД и конфиденциальные данные или выполнить команды ОС, а также доступ к функциональным возможностям СУБД, а в некоторых случаях – к операционной системе сервера, на котором функционирует СУБД.

Приведем основные методы защиты веб-приложений:

– максимально возможная фильтрация данных;

– использовать при сравнении кавычки SELECT ...WHERE name='$name';

– фильтрация символов “%” и “_” при использовании SQL-функции LIKE.

– создание белого списка запросов на которые будет отвечать приложение.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ANGULAR ПРИЛОЖЕНИЙ

А.Л. Хотеев, А.С. Дроздов, Н.В. Харитонов, Е.И. Нехведович

Мир программного обеспечения эволюционирует с огромной скоростью. Всего пару лет назад настольные компьютеры и ноутбуки являлись основными устройствами, под которые