АУДИТ ЗАВИСИМОСТЕЙ RAILS ПРИЛОЖЕНИЙ НА ПРЕДМЕТ УЯЗВИМОСТЕЙ

М.В. Стержанов, М.А. Медунецкий, М.П. Хоронеко

Классификацией векторов атак и уязвимостей занимается международная некоммерческая организация OWASP (Open Web Application Security Project). В 2017 году OWASP опубликовал обновленный список из десяти самых опасных векторов атак на Web-приложения, получивший название OWASP TOP-10 [1]. Одним из важных направлений атак является использование компонентов с известными уязвимостями.

Современные Rails-приложения написаны с использованием специальных библиотек или гемов, которые поставляются сторонними компаниями. В большинстве случаев эти компоненты имеют открытый исходный код, что дает миллионам разработчиков по всему миру возможность изучения и анализа на предмет уязвимостей.

Крайне важно использовать последние версии компонентов и следить за появляющимися известными уязвимостями на сайтах типа securityfocus.com.

Ресурс Rubysec содержит текстовую базу данных уязвимостей Rails приложений, которая регулярно обновляется и поддерживается Rails сообществом. База представляет собой набор директорий, имена которых соответствуют именам руби гемов на сайте rubygems.org. Каждая директория содержит один или более справочный текстовый файл, имя которого включает в себя идентификатор CVE (Common Vulnerabilities and Exposures). Каждый справочный файл содержит описание уязвимости в формате YAML.

Для проверки зависимостей Rails проекта сообществом Rubysec предлагается бесплатная утилита bundler-audit, которая устанавливается в проект в виде гема и проверяет наличие потенциально уязвимых зависимостей при помощи анализа файла Gemfile.lock.

Литература

1. OWASP Top 10 – 2017 [Электронный ресурс]. – URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf. (дата обращения: 18.05.2018).

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ 3D-ПРИНТЕРОВ

В.А. Столер

Использование трехмерной печати для быстрого прототипирования изделий предполагает наличие 3D-принтеров с широкими функциональными возможностями. Большинство имеющихся на рынке принтеров имеют свои недостатки, что ограничивает их применение. В работе рассматриваются пути конструктивной и программной модернизации таких принтеров на примере принтера CubeX от 3D Systems (США).

CubeX – современный полупрофессиональный принтер, который по своим параметрам подходит для изготовления изделий небольшой фирмой. Вместе с тем использование принтера CubeX [1] выявило ряд недостатков, влияющих на его работоспособность, а именно: многочисленные изломы прутка пластика, из-за неоправданного длинного маршрута его прохождения к печатной головке (экструдеру); частые «срывы» изделия с рабочего стола-элеватора, из-за отсутствия его подогрева, что в свою очередь ограничивает количество пластиков (филаментов), используемых для печати; 3) невысокая скорость печати, из-за небольшого диапазона варьирования параметрами печати в прилагаемом к принтеру ПО.

Перечисленные проблемы были решены конструктивными изменениями 3D-принтера, а также обновлением его программного обеспечения. Так без больших переделок был значительно сокращен маршрут подачи филамента к экструдеру за счет применения специального крепления для катушек с пластиком, распечатанное самим принтером. Вторая конструктивная проблема решается путем замены элеватора 3D-принтера на поверхность с подогревом и возможностью регулирования температуры нагрева. Последняя доработка принтера коснулась замены фирменного программного обеспечения на программу-слайсер KISSlicer 1.6.2, скачанную с интернета и адаптированную к CubeX, что дало возможность влиять на такие параметры как скорость печати, температуру, форму и толщину слоя печати и подложки, а также позволило менять режимы обдува заготовки при печати, изменяя геометрию получающегося изделия.

Выполненные конструктивно-программные доработки позволяют создать 3D-принтер с расширенными функциональными возможностями, который в обновленном виде способен будет печатать с увеличенной скоростью многими видами пластика без потери качества печати.

Литература

1. Столер В.А. Особенности использования трехмерной печати при решении инженерно-технических задач // Технические средства защиты информации: тезисы докладов XIV Белорусско-российской науч.-техн. конф. Минск, 25–26 мая 2016 г. С. 70.

КИБЕРУГРОЗЫ И ОТКАЗОУСТОЙЧИВОСТЬ

Судани Хайдер Хуссейн Карим, М.Б. Абросимов

Киберугрозы – это возможность (вероятность) несанкционированного проникновения в распределенные информационные системы для копирования, модификации, уничтожения находящихся в них данных или для затруднения или приостановки функционирования программной или аппаратной части информационной системы. Киберугрозы, в основном, исторически будучи формой деятельности отдельных высококвалифицированных преступников, к настоящему времени превратились в форму политического и военного воздействия спецслужб государств и террористических групп, систематически ведущих активную борьбу за передел международных сфер влияния. Объектами вмешательства становятся информационные системы государственного, военного, экономического и социального управления, а также устройства с выходом в Интернет отдельных граждан от чиновников и предпринимателей высокого ранга, известных лиц до рядовых служащих и несовершеннолетних детей. При реализации киберугроз возможные отказы и затруднения в работе информационных устройств, сбои и ошибки при информационных запросах способны привести в масштабе страны к значительным экономическим, военным и социальным последствиям и к ощутимым материальным ущербам. В этой связи, обеспечение отказоустойчивости информационных систем, как способности сохранять свою работоспособность в условиях реализации киберугроз, является актуальной научно-технической задачей, имеющей важнейшее социально-политическое значение. Для решения данной задачи следует определить всю номенклатуру киберугроз для заданной распределенной информационной системы. Каждой киберугрозе необходимо поставить в соответствие ожидаемый информационный, экономический, социальный, военный или иной ущерб, который произойдет в случае ее реализации применительно к рассматриваемой информационной системе. Необходимо оценить способность информационной системы выполнять свои функции в условиях реализации отдельной угрозы или их совокупности. Далее, исходя из результатов оценки, следует определить диапазон мер информационной защиты, а также состав резервных элементов программного и аппаратного обеспечения, который заменит вышедшие из строя элементы системы. Эффективность защиты от киберугроз будет измерена на интервале времени как отношение предотвращенного ущерба от реализации данного вида угрозы к стоимости мер защиты от данного вида угрозы и стоимости резервных элементов программного и аппаратного обеспечения. Уровень отказоустойчивости информационной системы применительно к номенклатуре киберугроз будет определяться заданным уровнем эффективности, для которой защищенность системы вначале будет спроектирована разработчиком, а в процессе эксплуатации будет постоянно совершенствоваться в ответ на возникающие новые формы киберугроз.

МОДИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ИЗМЕНЕНИЯ МЕЖДУСТРОЧНОГО РАССТОЯНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА

А.А. Сущеня, Е.А. Блинова, П.П. Урбанович

Предлагается модификация стеганографического метода изменения смещения междустрочного расстояния электронного документа, так называемого line-shift coding. В его стандартной реализации предлагается скрывать сообщение в изменении междустрочных интервалов. Однако такой метод имеет несколько существенных недостатков: обладает малой