КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПРОЦЕССЕ РАЗРАБОТКИ И ЭКСПЛУАТАЦИИ

А.Ф. Марко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

При разработке и эксплуатации программного обеспечения (ПО) для систем перемещений важной задачей является обеспечение их целостности, которая позволяет предотвратить использование ПО с незапланированные изменениями. Контроль за целостностью в предложенном ПО обеспечивается на этапе разработки с помощью внедрения соответствия версий в интегрированную среду разработки Visual Studio (VS), на этапе эксплуатации – с помощью формирования и сравнения контрольных сумм.

Алгоритмы соответствия версий обновляют версии файлов с расширениями dll и exe при изменении их исходного кода. Алгоритмы обновления версий реализованы в виде расширения для среды VS, которая может взаимодействовать как с централизованной системой управления версиями Team Foundation Server (TFS), так и с децентрализованной системой Git. Пользовательский интерфейс расширения встроен в интерфейс среды VS, что позволяет контролировать соответствие версий и разрабатывать ПО в одном окружении [1]. Алгоритмы расширения определяют модифицированные компоненты ПО, формируют новые версии, присваивают их компонентам и сохраняют изменения в систему TFS или Git [2].

Алгоритмы формирования и сравнения контрольных сумм в процессе эксплуатации реализованы в виде отдельного модуля ПО системы управления. ПО для системы управления состоит из множества различных объектов: исполняемые файлы, файлы данных, объекты баз данных. Формирование контрольных сумм выполняется для каждого типа по-разному. Также учитывается тот факт, что некоторые объекты, например, SQL-таблица базы данных, содержащая реквизиты для входа пользователей системы, постоянно изменяется в процессе эксплуатации, следовательно, отслеживать изменения в ней не требуется и контрольные суммы формировать не нужно [2]. Для формирования контрольных сумм объектов используется алгоритм SHA-2, который создает контрольные суммы от 224 до 512 бит, что обеспечивает высокую степень надежности и защиты от подделки или изменения файла [3]. Кроме того, SHA-2 является стандартом безопасности для многих приложений и операционных систем.

Таким образом разработанные алгоритмы позволяют автоматически верифицировать целостность ПО в процессе его разработки и эксплуатации и тем самым предотвращают его использование вместе с незапланированными изменениями.

Список литературы

1. Шарп Дж. Microsoft Visual C#. Подробное руководство. СПб.: Питер; 2017. 848 с.

2. Марко, А.Ф. Методы соответствия версий и контроля целостности программного обеспечения для систем перемещений в режиме реального времени // Информационные технологии и системы 2022 (ИТС 2022): материалы междунар. науч. конф., Минск, 23 ноября 2022 г. С. 63–64.

3. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Диалектика, 2004. 432 с.