В. В. Широков, М. А. Щиголева

Формирование прироста универсальных учебных и профессиональных достижений в дисциплине «Операционные системы» подготовки IT-специалистов

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) г. Санкт-Петербург, Россия

Аннотация. *Рассмотрено применение принципов модернизации образования подготовки IT-специалистов в высшей школе с формированием у обучаемых осмысленного наращивания универсальных учебных достижений в ходе изучения специальных дисциплин IT-подготовки. Приведён опыт преподавания дисциплины «Операционные системы»направлений подготовки «Информационные системы и технологии» и «Компьютерная безопасность». На примере Методики изучения механизмов безопасных вычисленийформируется мотивация освоения материала в широте и глубине тематического охвата предметной области с возможностью осознанного прироста индивидуальных достижений для предстоящей профессиональной реализации. В Методике изучения актуальных неотъемлемых IT-механизмов безопасных вычислений рассмотрен пример реализации в операционной системе Linux средств построения безопасных контейнеров.*

Ключевые слова: модернизация образования; IT-подготовка; механизмы контейнеризации; изоляция процессов; видимость каталогов;ограничение ресурсов процессов

На современном этапе быстро развивающихся технологий информатизации, компьютеризации, цифровизации подготовка IT-специалистов имеет специфику сочетания качеств разработчика и пользователя этих технологий, что требует обладания высокой профессиональной мобильностью. IT-специалисту, как разработчику, необходимо предвосхищать тенденции информационного спроса в решении всё более широкого круга задач, высокой компьютерной оснащенности пользователей, стабильно возрастающей и укрепляющейся информационно-компьютерной грамотности пользователей. От выпускника требуется не только обладание запасом современных знаний, но и способность воспроизводства фундаментальных основ этих знаний для создания новых технологий, методик и средств решения реальных задач современного развитого информационного технически оснащенного общества. IT-специалисту необходимо обладать высоким уровнем знаний предметной профессиональной подготовки и одновременно навыками и умениями решения практических профессиональных задач для создания новых продвинутых технологий и средств информатизации, компьютеризации, цифровизации с учётом тенденций их последующего развития и совершенствования.

Высокая профессиональная мобильность IT-специалиста возможна только при привитом навыке постоянного профессионального продвижения за счёт формирования прироста универсальных учебных и профессиональных достижений; выявления тенденций развития, усовершенствования, обновления предметной области; универсального характера и смежного сочетания предметных

областей; сочетания фундаментальных знаний, неотступного самообразования, продуктивного научного исследования.

В методологии обучения IT-специалиста необходимо сочетание предметно-ориентированного пространства и технологических средств освоения и преобразования этого пространства для достижения искомых результатов – решения поставленной научной или производственной задачи. Предметно-ориентированным пространством является сформированная образовательная среда из отобранных предметных областей: смежных дисциплин, дисциплин расширения предметной области, сочетания предметных и управленческих / организационных / коммуникативных областей. Технологическими средствами освоения и преобразования этого пространства будут технологии, приемы, подходы, методы, методики, механизмы из инструментария этих предметных областей.

Сфера деятельности IT-специалиста подразумевает осмысление теоретических предметных знаний с переносом их в реальные области труда, производства, жизнедеятельности. Для приобретения опыта практической работы учебный и образовательный процессы формируют знания – умения – навыки – компетенции в задачах, ориентированных на реальные задачи предметных областей направлений подготовки. Комплексное отображение этих элементов профильного образования в учебно-методических средствах освоения, применения и оценивания своих знаний и умений позволяет обучаемому сформировать свой подход для последующего прироста своих профессиональных достижений при решении новых профессиональных задач.

В представленном материале примером комплексного отображения выделенных компонентов обучения при подготовке IT-специалистов направлений «Информационные системы и технологии» и «Компьютерная безопасность» является Методика изучения механизмов безопасных вычислений в дисциплине «Операционные системы».

Изучение возможностей и способов использования механизмов безопасных вычислений, заложенных в основу операционных систем, в дисциплине «Операционные системы», следует считать необходимым и актуальным как в качестве теоретического материала, так и в качестве инструментов практического применения в профессиональной деятельности. Для направлений подготовки «Информационные системы и технологии» и «Компьютерная безопасность» в качестве средств современных информационных технологий широкое применение получили средства, называемые контейнерами. Контейнеры позволяют внутри себя запускать программы таким образом, что последние не могут навредить, умышленно или вследствие ошибок, внешнему окружению. Построение таких безопасных контейнеров базируется на ряде принципов, к числу которых относятся пространства имен и безопасные вычисления [1]. Не смотря на то, что механизм безопасных вычислений появился в операционных системах довольно давно, ему не уделяется достаточного внимания в базовых учебных курсах, посвященных операционным системам.

В данной работе рассматривается Методика изучения механизма безопасных вычислений, которая апробирована на практических занятиях по дисциплине «Операционные системы».

Методика содержит следующие этапы:

1. Знакомство с сутью механизма и базовыми принципами его реализации в операционной системе. И оценка их сложности.

2. Изучение программного интерфейса (API), позволяющего с помощью специальной библиотеки упростить программирование действий для обеспечения контроля над вызовами потенциально опасных системных функций операционной системы.

3. Написание тестовых примеров по обеспечению контроля за потенциально опасными системными функциями.

4. Создание заключительно примера, имитирующего запуск приложения внутри контейнера с контролем за потенциально опасными системными функциями.

Суть механизма безопасных вычислений заключается в формировании специального фильтра для ограничения системных вызовов и передачи этого фильтра в ядро операционной системы [2].

Передача фильтра в ядро производится специальным системным вызовом prctl() с параметром PR_SET_SECCOMP и указателем на структуру – фильтр системных вызовов.Фильтр основан на механизмах BPF (BerkeleyPacketFilters), онпредставляет собой структуру, которая содержит наборполей.К таким полям относятся:

▪ номер системного вызова, который следует проверять;

▪ действие, которое необходимо выполнять при совпадении фильтруемого системного вызова с текущим вызовом;

▪ действие, которое необходимо выполнять при несовпадении фильтруемого системного вызова с текущим вызовом.

Построение подобного фильтра представляет собой сложную задачу и выходит далеко за рамки текущего курса «Операционные системы».

Для облегчения задачи существует библиотекаlibseccomp [3], которая предоставляет удобный программный интерфейс для формирования фильтров и также предлагается к изучению.

Библиотека включает в себя четыре функции:

▪ инициализация фильтра seccomp_init();

▪ добавление правилв фильтр seccomp_rule_add() (добавлять правила можно для любого числа потенциально опасных вызовов);

▪ загрузка фильтра seccomp_load();

▪ очистка фильтра seccomp_reset().

Знаний, полученных из предыдущих разделов курса «Операционные системы», вполне достаточно, чтобы освоить технологию работы с библиотекой libseccomp.

На следующем этапе изучения механизма безопасных вычислений обучающимся предлагается создать ряд примеров, позволяющих в рамках одного вычислительного процесса обеспечить фильтрацию системных вызовов. Здесь они познакомятся с возможными действиями, которые допустимы при выполнении фильтруемого вызова (например, завершение процесса, аудит, трассировка).

Часто возникает вопрос, как осуществить фильтрацию потенциально опасных вызовов для внешней программы. Поэтому на заключительном этапе изучения библиотеки libseccomp учащимся предлагается построить макет контейнера, в котором родительский процесс формирует фильтры, а затем с помощью вызовов fork() и семейства exec() [4], [5] проверяется возможность фильтрации в дочернем процессе, играющем роль внешней программы.

Выводы. Освоение технологии безопасных вычислений в рамках предложенной Методики позволит существенно повысить квалификацию обучаемых направлений подготовки «Информационные системы и технологии» и «Компьютерная безопасность» в рамках базового курса «Операционные системы». Полученные знания будут необходимы в практической деятельности будущих специалистов при построении средств, предназначенных для обеспечения безопасности выполнения вычислительных процессов. У обучаемых будут сформированы знания, умения и навыки обращения к заложенным в основу операционных систем принципам. Для образовательного процесса Методика поддерживает методологию обучения с сочетанием фундаментального и практически ориентированного материала базовой дисциплины обучения, показывает универсальность подготовки по двум направлениям обучения «Информационные системы и технологии» и «Компьютерная безопасность» и используется для освоения инструментов практического применения в последующей профессиональной деятельности.

Список литературы:

1. Seccomp – механизм ядра Linux [электронный ресурс] – режим доступа – URL: https://habr.com/ru/companies/selectel/articles/322046/ (дата обращения 29.02.2024).

2. Защита контейнеров с помощью фильтров Seccomp[электронный ресурс] – режим доступа – URL: https://habr.com/ru/companies/ruvds/articles/689184/ (дата обращения 29.02.2024).

3. Seccomp. Контейнеры и безопасность [электронный ресурс] – режим доступа – URL:https://selectel.ru/blog/kontejnery-i-bezopasnost-seccomp/(дата обращения 29.02.2024).

4. Перевод системного вызова процесса в состояние безопасных вычислений. SecureComputing, Seccomp [электронный ресурс] – режим доступа – URL:https://ru.manpages.org/seccomp/2 (дата обращения 29.02.2024).

5. Перевод системного вызова процесса в состояние безопасных вычислений. SecureComputing, Seccomp. Возвращаемое значение. Ошибки. Версии. Стандарты. Замечания. Примеры [электронный ресурс] – режим доступа – URL:https://man7.org/linux/man-pages/man2/seccomp.2.html(дата обращения 29.02.2024).

V. V. Shirokov, M. A. Schigoleva

Formation of an increase in universal educational and professional achievements in the discipline "Operating systems" for training IT specialists

Saint Petersburg Electrotechnical University, Russia

Abstract. The article considers the application of the principles of modernization of education for training IT specialists in higher education with the formation of a meaningful increase in universal educational achievements among students during the study of special disciplines of IT training. The experience of teaching the discipline "Operating systems" in the areas of training "Information systems and technologies" and "Computer security" is given. Using the example of the Methodology for studying the mechanisms of secure computing of the discipline, motivation is formed for mastering the material in the breadth and depth of the thematic coverage of the subject area with the possibility of a conscious increase in individual achievements for the upcoming professional realization. In the methodology of studying the actual integral IT mechanisms of secure computing, an example of the implementation of secure container construction tools in the Linux operating system is considered.

Keywords: modernization of education; IT training; containerization mechanisms; isolation of processes; directory visibility; limitation of process resources