



Анализ кода и информационная безопасность

Осенний семестр 2019 г.



МГУ / ВМК / СП

Лекции

- Лектор — Соловьёв Михаил Александрович.
- Блок 01.
 - Лекция 01. Технологии разработки безопасного ПО.
 - Лекция 02. Основные понятия безопасности информации.
 - Лекция 03. Ошибка типа «переполнение буфера».
- Блок 02.
 - Лекция 04. Статический анализ исходного кода с целью поиска ошибок.
 - Лекция 05. Абстрактная интерпретация.
 - Лекция 06. Отладка и инструментирование.
 - Лекция 07. Фаззинг и символьное выполнение.
 - Лекция 08. Слайсинг.

Лекции

- Блок 03.
 - Лекция 09. Анализ бинарного кода.
 - Лекция 10. Статическое дизассемблирование.
 - Лекция 11. Восстановление потока управления и функций программы.
 - Лекция 12. Слайсинг по трассе и анализ помеченных данных.
 - Лекция 13. Анализ обращений к памяти в бинарном коде.
- Блок 04.
 - Лекция 14. Введение в сетевую безопасность.

Практические задания

- Все задания сдаются через сайт курса.
- У каждого студента будет индивидуальный вариант по каждому заданию.

- Задание 01. Ошибка типа «переполнение буфера».
 - От 0 до 20 баллов.
 - Предполагаемые сроки: с 20.09 по 04.10.
- Задание 02. Динамическое инструментирование бинарного кода.
 - От 0 до 10 баллов.
 - Предполагаемые сроки: с 18.10 по 01.11.
- Задание 03. Анализ трассы выполнения программы (две части).
 - От 0 до 30 баллов.
 - Предполагаемые сроки: с 22.11 по 13.12.

Экзамен и итоговая оценка

1. Экзамен в устной форме:
 - в билете два вопроса;
 - возможны дополнительные вопросы по всему лекционному материалу;
 - устный ответ оценивается по пятибалльной системе – E .
2. Набранные баллы за практические задания переводятся в оценку за практику по таблице – P . Таблица вывешена на сайте.
3. Итоговая оценка выставляется как функция E и P . Также вывешена на сайте.

Необходимые знания и умения

1. Работа в UNIX-окружении – практические задания будут выдаваться в виде образов виртуальной машины с ОС Debian.
2. Язык Си.
3. Язык ассемблера для x86 (16-, 32- или 64-разрядные варианты). На лекциях и в практических заданиях работа ведётся с 64-разрядным кодом. Перед началом работы с ассемблерным кодом на лекциях будет дана краткая справка по 64-разрядной архитектуре x86-64.
4. Базовые представления о компиляторных технологиях (граф потока управления, отношение доминирования, SSA-форма, распределение регистров в ходе кодогенерации).
5. Базовый математический аппарат: полурешётки, решётки.
6. Потребуется читать литературу на английском языке.

Техническое обеспечение

- Сайт курса: <https://caiscourse.ru/>.
 - Аннотации, слайды лекций и ссылки на литературу автоматически становятся доступны в момент начала соответствующей пары.
 - Для сдачи практических заданий необходимо будет зарегистрироваться на сайте.
 - Это можно будет сделать после лекции 09.09 или 16.09.
- Электронная почта: 2019@caiscourse.ru.
- Telegram-канал: @caiscourse2019.