

Вопросы к государственному экзамену
Магистерская программа "Технологии программирования"

1. Основные понятия дедуктивной верификации. Методы доказательства корректности программ.
2. Основные понятия дедуктивной верификации. Методы доказательства завершимости программ.

Список рекомендованной литературы

1. Буздалов, Корныхин, Панфёров, Петренко, Хорошилов. *Практикум по дедуктивной верификации программ: учебно-методическое пособие.* – М.: МАКС-Пресс, 2014.
 2. Б.Мейер. *Объектно-ориентированное конструирование программных систем* – М.: Русская Редакция, 2005.
-

3. Основные сведения об объектном языке ограничений (OCL): состав OCL-выражения, навигация по ассоциациям, виды коллекций, операции с коллекциями, учёт наследования в выражениях и наследование ограничений. Примеры использования OCL.
4. Способы объектно-реляционного отображения для классов и атрибутов, бинарных и N-арных ассоциаций, классов ассоциаций, иерархий наследования. Примеры применения этих способов. Моделирование схемы реляционной базы данных с помощью диаграммы классов.
5. Образцы (паттерны) проектирования, их классификация и способ описания. Примеры образцов: структурного, поведенческого и порождающего.

Список рекомендованной литературы

1. Арлоу Д., Нейштадт А. *UML 2 и унифицированный процесс. Практический объектно-ориентированный анализ и проектирование.* - СПб.: Символ-Плюс. - 2008. Глава 25.
 2. Рамбо Дж., Блаха М. *UML 2.0. Объектно-ориентированное моделирование и разработка.* - СПб.: Питер. - 2007. Главы 3 и 19.
 3. Гамма Э. и др. *Приемы объектно-ориентированного проектирования. Паттерны проектирования.*: Пер. с англ. - СПб.: Питер, 2016.
-

6. Основные понятия безопасности информации: конфиденциальность, целостность, доступность. Виды защиты информации. Модель Белла-Лападулы. Понятие ошибки, уязвимости в программном обеспечении, примеры.
7. Ошибка типа «переполнение буфера». Выполнение произвольного кода на исполнимом стеке. Противодействие выполнению кода на стеке: «канарейка», DEP. Выполнение произвольного кода на неисполнимом стеке. Return-to-libc, return-oriented programming (ROP).
8. Статический анализ исходного кода с целью поиска ошибок. Типы обнаруживаемых ошибок. Путь распространения ошибки: source, propagation, sink. Поточковая и контекстная чувствительность. Качество результата анализа: false/true positive/negative. Интерпретация результатов анализа.
9. Применение отладки для оценки возможности эксплуатации уязвимостей. Технологии отладки. Отладка пользовательского кода. Полносистемная отладка в виртуальной машине. Статическое и динамическое инструментирование. Фаззинг. Разновидности фаззинга: черный ящик, белый ящик, серый ящик.
10. Символьное выполнение: основные понятия. Схема работы системы символьного выполнения. Предикат пути, предикат безопасности. Проблема экспоненциального взрыва, стратегии выбора следующего состояния.

Список рекомендованной литературы

1. Brian Chess, Jacob West. *Secure Programming with Static Analysis* / Addison-Wesley Professional, 2007.
 2. *Aleph One. Smashing the Stack for Fun and Profit*
 3. Edward J. Schwartz, Thanassis Avgerinos, and David Brumley. *Q: Exploit Hardening Made Easy*.
 4. Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, Dawson Engler. *A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World*.
 5. William R. Bush, Jonathan D. Pincus, David J. Sielaff. *A Static Analyzer for Finding Dynamic Programming Errors*.
 6. Eli Bendersky. *Серия статей "How debuggers work"*.
 7. Chow J., Garfinkel T., Chen P. M. *Decoupling dynamic program analysis from execution in virtual environments* // USENIX 2008 Annual Technical Conference on Annual Technical Conference. – 2008. – С. 1-14
 8. Nethercote N., Seward J. *Valgrind: a framework for heavyweight dynamic binary instrumentation* // ACM Sigplan notices. – ACM, 2007. – Т. 42. – №. 6. – С. 89-100.
 9. Амини П., Самтон М., Грин А. *Fuzzing: исследование уязвимостей методом грубой силы*. — Символ-Плюс, 2009.
 10. Edward J. Schwartz, Thanassis Avgerinos, David Brumley. *All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask)*, 2010
 11. C. Cadar, D. Dunbar, D. Engler. *KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs*, 2008.
-

11. Критерии полноты тестирования. Доменные, функциональные, структурные и проблемные критерии полноты. Использование графов, грамматик и логических выражений для построения критериев полноты тестирования. Типовые критерии покрытия кода
12. Методы контроля качества ПО. Верификация и валидация. Виды верификации. Экспертиза. Статический и динамический анализ. Формальные методы верификации. Проверка моделей.
13. Интегрированные подходы построения тестов. Элементы технологии UniTESK. Программные контракты. Уточнение и формализация требований. Построение сценария теста на основе требований и заданного критерия полноты тестирования. Архитектура тестового набора UniTESK. Организация тестирования распределенных систем. Семантика чередования. Событийные контракты.

Список рекомендованной литературы

1. Д. Месарош. *Шаблоны тестирования xUnit*. М.: Вильямс, 2008
 2. *Материалы курса В.В.Кулямина "Тестирование программного обеспечения": <http://mbt-course.narod.ru>*
-

14. Спецификация и верификация параллельных программ. Синхронная и асинхронная параллельность. Справедливость планировщика. Темпоральная логика линейного времени (LTL). Проблема взаимного исключения процессов.
15. Абстрактные модели: ошибки первого и второго родов (false positives, false negatives). Предикатная абстракция программ и уточнение абстракции по контрпримерам (CEGAR). Ее использование для верификации программ на языках программирования.

Список рекомендованной литературы

1. Ю.Г. Карпов. *Model Checking. Верификация параллельных и распределенных программных систем*. — СПб.: БХВ-Петербург, 2010.

16. Информационная безопасность. Шифрование данных. Криптографическая стойкость. Симметричная криптография. Блочный шифр (DES) и его режимы. Ассиметричные схемы (RSA и Диффи-Хеллмана). Код аутентификации (MAC). Цифровая подпись (DSA).
17. Понятие анонимности пользователя в сети. Идентификаторы пользователя в сети на разных уровнях (устройства, ОС, ПО). Подходы к деанонимизации и способы защиты. Концепция анонимных сетей (Mix и Tor). Луковая маршрутизация. Виды атак на анонимные сети.

Список рекомендованной литературы

1. Эндрю Таненбаум, Дэвид Уэзеролл. *Компьютерные сети. Пятое издание.* — СПб.: Питер, 2012.
2. Jon Mark Allam. *OS and Application Fingerprinting Techniques.* — SANS Institute, 2007.
3. Grahn, K. J., Forss, T., & Pulkkis, G. *Anonymous Communication on the Internet. Proceedings of Informing Science & IT Education Conference (InSITE) 2014 (pp. 103-120).*