

АНАЛИЗ МЕТОДОВ ДИАГНОСТИКИ ВСТРАИВАЕМЫХ СИСТЕМ И РАЗРАБОТКА ТРЕБОВАНИЙ К ДЕТЕРМИНИРОВАННОМУ ВОСПРОИЗВЕДЕНИЮ ВЫПОЛНЕНИЯ ПРОГРАММ

Лесников А.А. (ИТМО)

Научный руководитель – кандидат технических наук, доцент Пинкевич В.Ю. (ИТМО)

Введение. Современные методы отладки встраиваемых систем сталкиваются с проблемой недетерминированного поведения программ, особенно в условиях параллельного выполнения и взаимодействия с периферийными устройствами. Традиционные подходы диагностики, основанные на тестировании в реальном времени, не подходят для встраиваемых систем из-за сложности воспроизведения ошибок. Инструменты, направленные на решение этой проблемы, ориентированы на узкое применение и не подходят для встраиваемых систем из-за высокой зависимости от физического оборудования и значительных накладных расходов. Эти факторы делают существующие методы диагностики недостаточно эффективными и требуют разработки нового подхода.

Основная часть. В ходе исследования были изучены и проанализированы существующие методы тестирования встроенных систем, направленные на регистрацию и анализ выполнения программного кода. Рассмотрены механизмы фиксации состояний системы, журналирования событий и моделирования работы оборудования. Проведен сравнительный анализ существующих решений по таким критериям, как точность воспроизведения, применимость к системам с ограниченными ресурсами, зависимость от аппаратной платформы и влияние на производительность. В результате выявлены ограничения традиционных методов, которые не позволяют гарантировать детерминированное воспроизведение выполнения программы и удобную диагностику ошибок.

На основе проведённого анализа были определены требования к новому методу для решения обозначенных проблем. В качестве основы предложен подход, в котором выполнение программы представляется в виде конечного автомата с фиксацией ключевых переходов в журнал. Такой метод позволит восстанавливать выполнение программы с высокой точностью, обеспечивая детерминированное воспроизведение выполнения для удобного анализа ошибок.

Выводы. Проведен анализ методов тестирования вычислительных систем для решения проблемы недетерминированного поведения программ, определены основные требования к методу для решения этой проблемы.

Список использованных источников:

1. Kurikka J. Testing Embedded Software in a Simulated Environment: Master's Thesis. – University of Oulu, Finland, 2022.
2. Feng B., Mera A., Lu L. P2IM: Scalable and Hardware-independent Firmware Testing via Automatic Peripheral Interface Modeling // Proceedings of the 29th USENIX Security Symposium. – 2020.
3. Clements A. A., Gustafson E., Scharnowski T., Grosen P., Fritz D., Kruegel C., Vigna G., Bagchi S., Payer M. HALucinator: Firmware Re-hosting Through Abstraction Layer Emulation // Proceedings of the 29th USENIX Security Symposium. – 2020.
4. Joshi C. V. Software Emulation of STM32 Controller for Virtual Embedded Design/Test Environment: Master's Thesis. – Eindhoven University of Technology, Netherlands. – 2019.

5. Zaddach J., Bruno L., Francillon A., Balzarotti D. Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares // Proceedings of the 21st USENIX Security Symposium. – 2012. – pp. 851–866.

6. Andrzej Radecki, Tomasz Rybicki. Simulation-Oriented Layer of Embedded Software Architecture for Rapid Development of Custom Embedded Systems Virtual Simulators Used in Didactics. Institute of Automatic Control, Lodz University of Technology, 90-537 Lodz, Poland. – 2022.

Лесников А.А. (автор)

Пинкевич В.Ю. (научный руководитель)