УГРОЗЫ ДЛЯ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ИНТЕРНЕТ-ПРИЛОЖЕНИЙ

Костевич А. Л.

НИИ ППМИ БГУ, Минск, Беларусь, e-mail: kostevich@bsu.by

В настоящее время широкое распространение получили мобильные и интернет–приложения, распределенные информационные системы, компоненты которых связаны с помощью Интернет. Особенностью таких информационных систем является использование открытых каналов связи для обмена данными. При этом открытые каналы характеризуются возможностью перехвата и модификации передаваемых данных, недоверием к подлинности сторон–участников обмена. В качестве модели угроз для таких информационных систем используется модель Долева-Яо [1]. Это требует от каждого приложения решать задачи обеспечения конфиденциальности, целостности и подлинности данных, а также задачу аутентификации сторон. Перечисленные задачи традиционно решаются с применением криптографических алгоритмов — шифрования, контроля целостности и выработки/проверки ЭЦП, — а также с применением криптографических протоколов — аутентификации и распределения ключей. Это позволяет получать теоретически обоснованные оценки стойкости в выбранной модели угроз.

Однако предположением, при котором обеспечивается стойкость, является отсутствие уязвимостей в реализации механизмов защиты: как в самом приложении, так и в реализации средств защиты информации, в используемых системных компонентах (реализации стека протокола используемой операционной системы, реализации виртуальной машины и т.п.). Анализ последних результатов в области компьютерной безопасности показывает, что:

- существуют эффективные технологии автоматизированного поиска уязвимостей в программном обеспечении; их применение приводит к выявлению все новых уязвимостей во всем спектре существующего программного обеспечения;
- разработчики операционных систем и средств защиты информации внедряют механизмы, повышающие трудоемкость компрометации информационных систем при наличии в них (неустраненных) уязвимостей, однако
- существуют эффективные технологии использования уязвимостей в программном обеспечении; их применение не требует высокой квалификации, что приводит к массовой компрометации информационных систем.

Можно сделать вывод о том, что отсутствие в жизненном цикле разработки программного обеспечения этапов моделирования угроз, применения технологии поиска уязвимостей и выпуска обновлений приводит к выпуску некачественного программного обеспечения, которое с высокой вероятностью может быть (будет) скомпрометировано даже несмотря на применение криптографических методов.

Литература

1. Chen Q., Zhang C., Zhang S. Secure Transaction Protocol Analysis: Models and Applications // Lecture Notes in Computer Science / Programming and Software Engineering, vol. 5111, 2008.