

Литература

1. A novel block encryption scheme based on chaos and an S-box for wireless sensor networks / Tong Xiao-Jun, Wang Zhu, Zuo Ke // Chin. Phys. B Vol. 21, No. 2(2012), URL: <http://cpb.iphy.ac.cn/fileup/PDF/2012-2-020506.pdf>

СИСТЕМА ЗАЩИТЫ WEB-ПРИЛОЖЕНИЯ НА ОСНОВЕ АСПЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ

С.А. Зайкова, О.Ю. Рыжко

Одним из основных требований, предъявляемых к современным информационным ресурсам и сервисам, является их широкая доступность. Наиболее активное развитие получили web-приложения, в которых роль клиента играет браузер, а роль сервера — web-сервер. В связи с этим встает вопрос об организации разграничения доступа и защите информации. Современные web-приложения имеют многослойную структуру и сложность кода, порой, возрастающего в геометрической прогрессии. Отдельные модули приложений разрабатываются разными командами, которые могут знать о другом модуле только его интерфейс. Актуальность исследования вытекает из необходимости выработки методов выделения функционала обеспечения безопасности web-приложения в отдельный независимый модуль, с возможностью повторного использования кода в совместимых проектах. Это позволит изменять политики безопасности web-приложения централизованно и без изменения бизнес-логики проекта. Проблематика заключается в тесной интеграции инструментов аспектно-ориентированного программирования с кодом целевого web-приложения, сложности внедрения аспектно-ориентированного программирования в проект, а также большом влиянии аспектов на производительность web-приложения, что, в свою очередь, зависит от типа внедрения аспектов и архитектуры приложения. Как показало исследование, использование annotation-driven подхода при разработке, а также конфигурация web-приложения через xml файлы позволяет значительно сократить объем кода приложения, но может вызвать дополнительные временные затраты на отладку и проверку совместимости зависимых библиотек. Разработанная система безопасности является проектно-независимой и может быть применена в другом web-приложении, при условии совместимости интерфейсов в контрактном программировании.

Литература

1. *Safonov V.O.* Using aspect-oriented programming for trustworthy software development — Wiley Interscience: John Wiley & Sons, 2008. — 338 с.

СЛУЧАЙНЫЕ ПРОСТРАНСТВЕННО-ВРЕМЕННЫЕ КОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ШИРОКОВЕЩАТЕЛЬНЫХ КАНАЛАХ

Т.М. Казубович, С.Б. Саломатин

Современные системы связи и беспроводного доступа широко используют широкополосные многолучевые каналы передачи информации. При этом актуальной является задача защиты каналов связи от подслушивания.

Один из методов решения такой задачи основан на применении технологии ММО с обратной связью и случайного пространственно-временного кодирования.

Технология ММО позволяет осуществить эффективный прием информации в условиях многолучевого распространения сигнала за счет создания пространственно-временной избыточности на приемной и передающих сторонах и измерения характеристик канала. Предполагается, что многолучевые каналы имеют существенные различия в разных точках приема. Передающая сторона имеет информацию о состоянии канала связи H с авторизованным пользователем. Подслушивающая сторона такой информации не имеет и вынуждена использовать методы слепой оценки многолучевого канала.

Для защиты информации передающая сторона случайным образом выбирает веса W антенной системы с условием выполнения равенства $HW = A$, где A — диагональная матрица с положительными диагональными элементами. Авторизованный пользователь принимает сигнал $y = HWx + n$, где n — вектор шума. Оценивая мощность принятого сигнала, и вычисляя обратную к A матрицу A_i , авторизованный пользователь детектирует информацию $x = A_i y$. Случайная весовая матрица пространственно-временного кода имеет две составляющих. Одна составляющая выбирается из условия нормальной рандомизации вектора передаваемого сообщения, а вторая составляющая учитывает информацию о состоянии канала.