XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VII: С. 46-47, 2003.

УДК 681.391.1

А.Б. Бубликов (асп., каф. 42, СПб ГУАП);
М.Б. Сергеев, д.т.н., проф., каф. 44, СПб ГУАП

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ПОТОКОВОЙ ИНФОРМАЦИИ МЕЖДУ УЗЛАМИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ

ABSTRACT: In the work the problem of a guard of an information in the distributed monitoring systems and management is considered. Is marked, that the classical cryptosystems in such applications have a number of defects. The problem use of simple methods of a guard based on transformation of the managers, inspecting and answer-back is discussed.

На сегодняшний день развитие IP-сетей общего доступа привело к их использованию при построении информационно-управляющих систем в качестве коммуникационной среды [1-3], которая изначально не предоставляет сервисов с защитой информации. Любая распределенная информационно-управляющая система имеет несколько типов коммуникаций. Во-первых, коммуникации типа устройство-устройство (или сервис-сервис), проходящие обычно без участия человека, хотя он и может быть инициатором начала коммуникации между устройствами. Такие коммуникации характерны для корпоративных сетей, когда центральный сервис (производитель) периодически обменивается информацией с региональными сервисами. Во-вторых, коммуникации пользователя информационно-управляющей системы (и/или администратора системы) с узлами (сервисами) для получения статусной информации, контроля, управления узлами или системой в целом. И в первом, и во втором случаях использование сетей общего доступа, предполагает надежную защиту передаваемой/получаемой информации.

Вне зависимости от типа коммуникаций в процессе обмена информацией участвуют два модуля – серверный и клиентский. Спецификой серверного модуля является то, что объемы входящего и исходящего потоков информации для данного модуля примерно равны, в то время как клиентский модуль обычно получает информации гораздо больше, чем отдает. Исходящий поток информации для клиентского модуля – это управляющие команды. Кроме того, серверный модуль обычно хранит в себе информацию, требующую повышенных мер защиты. Иногда предполагается доступ к серверному модулю сторонних лиц (для обслуживания). Все вышеперечисленное приводит к требованию защищенности не только передаваемой, но и хранимой на сервере информации.

Таким образом, информационный поток в системе может быть двух типов - поток, несущий в себе статусную информацию о системе или пользовательскую информацию (например, видео) и поток, представляющий собой команды управления системой. Для второго случая (команд управления) на сегодняшний день известно достаточно много способов обеспечения безопасности передачи - таких, как, например, разграничения доступа к ресурсам. С другой стороны, организация защищенного канала для передачи потоковой информации обычно остается слабым местом распределенных информационно-управляющих систем. Организация передачи потоковой информации от сервера к клиенту предполагает значительную удаленность клиента, что накладывает требование, заключающееся в максимальной простоте установки защищенного соединения. Основной метод организации защиты передачи потоковой информации через каналы сетей общего доступа заключается в применении поточных шифров.

Поточные шифры делятся на две большие группы: синхронные и самосинхронизирующиеся.[4] Синхронные шифры требуют синхронизации между приемником и передатчиком, а самосинхронизирующиеся способны синхронизировать приемник и передатчик

посредством передаваемой ими информации [4]. В нашей системе использован один из синхронных шифров.

На сегодняшний день известны утратившие актуальность генераторы гаммы, опубликованные в открытой литературе преимущественно в 1970-1980-х годах, - генератор Геффе, генератор Плеса, Генератор-мультиплексор Дженнингса, Пороговый генератор, генератор скалярного перемножения, генератор Вольфрама, генератор "1/*p*", генератор суммирования, ранцевый генератор, аддитивный генератор, генератор Гиффорда. Эти работы послужили основной базой для создания в 80-е годы поточных шифров, которые используются и посей день – A5, RC4, SEAL.

Дальнейшие работы в области потокового шифрования приводят к появлению в конце 90-х годов таких работ как: фильтр-генератор на основе алгоритма сжатия данных Зива-Лемпела, модифицированный линейный конгруэнтный генератор (Чамберса), каскад с неравномерным движением (Чамберса), алгоритмы WAKE, PIKE, GOAL, ORYX, генератор ISAAC.

Современные направления в потоковой криптографии связаны с появлением алгоритма псевдослучайного генератора Шамира и генератора Блюма-Микали, развитием которых стали генератор квадратичных вычетов и широко известный сегодня RSA генератор. Предлагаются и другие способы потоковой шифрации, основанные на использовании простых булевых преобразований. В работе [8] отмечается преимущество такого подхода в ряде перспективных приложений, связанных с коммуникациями типа устройство-устройство. Показано, что нахождение булевых преобразований устройством осуществляется достаточно просто, однако из-за неоднозначности доопределения получаемых слабоопределенных булевых функций криптоаналитику (незаконному перехватчику сообщений) даже при большом числе перехваченных пар сигналов практически невозможно восстановить выбранную устройством (сервером) функцию. Использование простых, быстровычислимых булевых функций может существенно расширить области применения средств защиты информации в случаях работы с большим количеством контролируемых и управляемых объектов.

Анализ алгоритмов поточных шифров показал, что для построения систем взаимодействия модулей распределенной информационно-управляющей системы наиболее подходящими являются: алгоритм RC4, сочетающий в себе достаточную надежность и скорость шифрации; булевы преобразования, описанные в [8].

Однако, теоретические выводы на сегодня предстоит исследовать с помощью реализации алгоритма RC4 для организации защищенного канала передачи потоковой информации, представляющей собой видеопоток, в информационно-управляющей системе на базе IP-платформы [1].

ЛИТЕРАТУРА

1. Астапкович А.М., Востриков А.А., Сергеев М.Б., Чудиновский Ю.Г. Информационно-управляющие системы на основе Internet // Информационно-управляющие системы. - 2002. - № 1. - С. 12 - 18.
2. www.embedded.com/internet
3 .www.telemed.ru
4. Поточные шифры. Результаты зарубежной открытой криптологии. - Москва, 1997.
5. www.bezpeka.com
6. www.secur.ru
7. www.sec.ru
8. Ерош И.Л. Защита информационных потоков в системах распределенного контроля и управления // Информационно-управляющие системы. - 2002. - № 1. - С. 40 - 48.