Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 111-114 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INSTALLATION FOR STUDY OF DATA PROTECTION TECHNIQUES IN COMMUNICATION CHANNELS

Nataliia Tmienova 1, Bohdan Sus 2.
Faculty of Information Technology, Taras Shevchenko National University of Kyiv 1
Institute of High Technologies, Taras Shevchenko National University of Kyiv 2

ABSTRACT. The growing threat of computer crime puts forward new urgent tasks. The relevance of information security depends on the growing threat of cybercrime in modern hardware and software intellectual and telecommunications systems. Modern electronic devices allow you to control most of the channels for data collecting, processing and transmitting. The need for practical training of specialists in protection of information using laboratory workshops becomes evident. Laboratory work on the study of data protection capabilities based on the achievements of modern microelectronics such as programmable microcontrollers, receivers, transmitters, repeaters and communication channels can be very effective means of training specialists. The article describes a demonstration installation that can be used in such lab activity.

Keywords: cryptography, hardware encryption systems, programmable microcontrollers, security, privacy, forensics analysis, embedded systems.

1 Актуальность разработки

В настоящее время наблюдается растущая тенденция нарушения безопасности данных. Утечки информации часто происходят вследствие неэффективного управления кибербезопасностью или в результате применения устаревших или неправильно реализованных процедур безопасности. Шифрование данных с применением соответствующих схем управления ключами может уменьшить утечку данных. Однако при использовании методологии с ключами шифрования возникают такие проблемы как генерирование и безопасная передача ключей участникам взаимодействия; установка безопасного канала передачи информации между участниками взаимодействия; аутентификация. Существуют симметричная и асимметричная технологии шифрования. Каждая методология использует свои собственные процедуры и способы распределения ключей, типы ключей, а также алгоритмы шифрования и расшифровки ключей [1].

Хотя криптография с использованием известных стандартов, современных алгоритмов и библиотек является достаточно эффективной, разработка аппаратных комплексов шифрования остается актуальной задачей [2, 3]. Программные средства обеспечения информационной безопасности являются потенциально уязвимыми, поскольку весь процесс кодирования данных выполняется во внутренней памяти вычислительных устройств, к которой может получить доступ любое запущенное на компьютере приложение. Это означает, что существует возможность проводить разноуровневые атаки на любое программное обеспечение, в том числе и на предназначенное для обеспечения безопасности обрабатываемой информации. Таким образом, построить высокоуровневую защиту исключительно программными средствами практически невозможно [4]. Для ограничения доступа к средствам, выполняющим криптографические преобразования, необходимо перенести их из ЭВМ на закрытую аппаратную подсистему. В результате чего злоумышленник не сможет получить непосредственный доступ к процессам кодирования данных. Прежде всего аппаратная реализация алгоритма шифрования гарантирует неизменность самого алгоритма, тогда как программной алгоритм может быть намеренно модифицирован. Кроме того, аппаратный шифратор исключает вмешательство в процесс кодирования. Другое преимущество - использование аппаратного датчика случайных чисел, который гарантирует абсолютную

случайность генерации ключей шифрования и повышает качество реализации различных криптографических алгоритмов. Кроме того, аппаратный шифратор позволяет напрямую загружать ключи шифрования в устройство кодирования, минуя оперативную память, тогда как в программном шифраторе ключи находятся в памяти даже во время его работы. Также важен и тот факт, что на базе аппаратного шифратора возможно создавать различные системы разграничения и ограничения доступа к вычислительным системам. Также применение аппаратных систем затрудняет возможность сокрытия доказательств вмешательства в каналы связи.

В данной работе для исследования аппаратных возможностей уменьшения вероятности несанкционированного доступа к информации предлагается аппаратное устройство для демонстрации шифрования данных на базе программируемых микроконтроллеров. Комплекс позволяет совместное использование различных каналов связи. Оптико-волоконные линии связи позволяют обеспечить передачу информации с минимальными искажениями, что позволяет улучшить технологии защиты передачи информации.

Дополнительный интерес вызывает использование в комплексе поляризационной модуляции света. Работа таких устройств основана на применении электронно-управляемых анизотропных сред.

Данный комплекс может использоваться для успешного изучения студентами технологий, алгоритмов и физических методов шифрования и безопасной передачи сигналов в каналах связи.

2 Описание комплекса

Для оценки эффективности алгоритмов шифрования данных был разработан ряд практических решений, включающих в себя программные коды и аппаратную реализацию на базе встроенных систем. В настоящее время по оптическому каналу связи передается большое количество информации, и есть риск того, что она может попасть к злоумышленникам, которые имеют необходимые ресурсы и оборудование. Поэтому предлагается сочетание стандартных оптических каналов с радиоканалами, которые переключаются по специальному алгоритму. Возможность использования аппаратного датчика случайных чисел гарантирует случайность генерации ключей шифрования и повышает качество реализации различных криптографических алгоритмов. Предложенное шифрования не устраняет возможности перехвата данных через оптический канал, но делает похищенную информацию малополезной для злоумышленников.

Комплекс создан на базе высокопроизводительного микроконтроллера. У комплекса шифрования информации доступны такие основные функции:

- передача и прием сигналов по отдельным оптическим каналам;
- передача и прием сигналов по общему оптическому каналу с использованием спектрального мультиплексирования;
- передача сигналов или ключа шифрования по радиоканалу;
- возможность синхронной коммутации каналов связи.

Для кодирования сигналов используется библиотека x-cube-cryptolib, в которой поддерживаются алгоритмы шифрования данных AES-128, AES-192, AES-256, ECB (Electronic Codebook Mode), CBC (Cipher-Block Chaining).

Программа посылает сообщение, которое в свою очередь может быть дополнительно зашифровано программным образом. При использовании программного шифрования информация всех типов сначала разбивается на пакеты малой фиксированной длины, содержащие заголовки (так называемые ячейки). Дальше происходит их мультиплексирование

в цифровом канале.

Сообщение вводится в окно программы терминала модуля передатчика. Для наглядности при передаче информации оптическим каналом использованы излучатели излучения красного, зеленого и синего цветов.

Для передачи данных также используется радиоканал на доступных модулях MX-F01 и MX-RM-5V. Связь между радиомодулями и микроконтроллером организована через периферийный интерфейс USART. Количество излучателей можно изменять в соответствии с количеством каналов.

При передаче закодированного сообщения осуществляется коммутация каналов (переключение передатчиков и приемников в соответствии с определенным алгоритмом шифрования). Эффективность приёма изменяется в зависимости от скорости передачи и задержки между пакетами данных.

В демонстрации может использоваться также комбинация оптических каналов со спектральным уплотнением сигналов и алгоритм динамического плавающего кода.

Дешифрованное сообщение выводится в окно программы терминала последовательного порта, который получает данные из микроконтроллера, который выступает в качестве приемника.

Такое кодирование особенно эффективно для передачи коротких пакетов данных. В таком режиме возможно дополнительное кодирование информации в оптическом канале с помощью изменения поляризации излучения. Использование поляризационных ячеек на жидких кристаллах и анализаторов меняется в соответствии с алгоритмом шифрования. Небольшая скорость передачи информации в таком режиме связана с использованием недорогих микромеханических электронных систем для поворота поляризаторов.

3 Выводы

Растущая опасность компьютерной преступности выдвигает набор новых актуальных проблем. При этом разработка аппаратных комплексов шифрования может быть эффективной на пути преодоления некоторых из них.

Описанный демонстрационный комплекс позволяет оценить эффективность шифрования потоков данных в каналах, сравнивать пакеты, принятые от передатчика, с числом отправленных, анализировать спектр зашифрованного сигнала и шумы радиоканала.

Данный комплекс может удачно использоваться в следующих областях: банковской сфере, военной и медицинской отраслях, телекоммуникациях.

К основным достоинствам можно отнести надежность передачи, простоту реализации, гибкость функционала и возможностей применения.

Также, демонстрационный комплекс возможно использовать для проведения лабораторных занятий по созданию протоколов передачи информации и фильтров обработки сигналов.

Комплекс дает возможность проводить физические эксперименты по мониторингу сигналов в оптическом волокне и радиоканале связи для выбора оптимального алгоритма устойчивости шифрования.

Предложенные подходы можно использовать для модификации оборудования передачи данных и оценки надежности шифрования.

Библиография:

1. Введение в криптографию (авторизованный перевод статьи Дж. Чандлер "Cryptography 101") [Электронный ресурс]. Режим доступа: http://citforum.ck.ua/security/cryptography/crypto_1.shtml
2. Безопасность информационных систем [Электронный ресурс]. Режим доступа: http://intuit.valrkl.ru/course-1312/index.html.
3. Security with STM32 & Secure Elements [Electronic Resource]. Mode of access: http://www.emcu.it/SILICA-STDay2016/X/Presentazioni/2_STM32&SecureElements.pdf
4. Stallings W. Cryptography and network security: principles and practice. – New York: Prentice Hall, – 2006. – 680 p.