www.volsu.ru

# ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.1.1

УДК 004
ББК 32.966.093

## ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

**Владимир Витальевич Баранов**

Кандидат военных наук, доцент,
заведующий кафедрой информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
baranov.vv.2015@yandex.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

**Эльнур Решатович Алиев**

Магистрант, инженер кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
elnur913@gmail.com
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

**Аннотация.** В статье разработан робототехнический комплекс и система, позволяющая управлять этим комплексом по надежному криптографически стойкому соединению. Основным элементом данной системы является криптографический чип STM32F415. Он позволяет уменьшить нагрузку на центральный процессор для выполнения алгоритмов управления, освободив его от криптографических операций, тем самым, гарантируя выигрыш во времени.

**Ключевые слова:** канал управления, киберфизические системы, роботизированные системы, криптографические алгоритмы.



Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях – космос, химическая

технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт и потребительские устройства. Такой класс систем часто рассматривается как киберфизические системы [1; 2].

С целью проверки работы криптографического ускорителя была разработана роботизированная система (рис. 1), состоящая из следующих частей:

– BeagleBone Black (главный процессор роботизированной системы);

– Mini Maestro 18-Channel USB Servo Controller (драйвер-двигатель);

– MG996R (сервоприводы);

– STM32F415 (криптографический чип);

– Блок питания;

– Wi-Fi адаптер.

Управление роботизированной системой осуществляется использованием Wi-Fi адаптера в качестве передатчика радиосигнала [3; 4].

Для обеспечения криптографически стойкого протокола управления в роботизированной системе используется микроконтроллер с 32-разрядным ядром ARM Cortex-M4F с криптографическим ускорителем STM32F415rgt производства компании «STMicroelectronics».

Используя техническую документацию, был проведен анализ выводов криптографического чипа с выводами микроконтроллера STMF0, после которого было принято решение внедрить чип в плату STM32f0discovery, заземлив несколько контактов (рис. 2).

Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования использовался AES с длиной ключа 128 бит. Данный алгоритм был выбран за своё быстродействие и криптостойкость.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи – Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

Функциональная схема криптографически стойкого протокола управления роботизированной системой представлена на рисунке 3.

В качестве центрального процессора и электронного мозга для робота был выбран одноплатный компьютер BeagleBone Black (BBB).

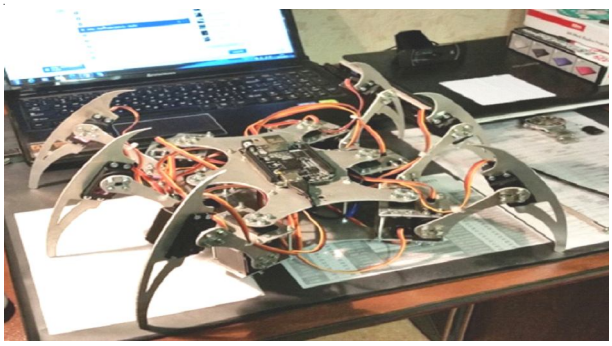

Рис. 1. Роботизированная система в сборке

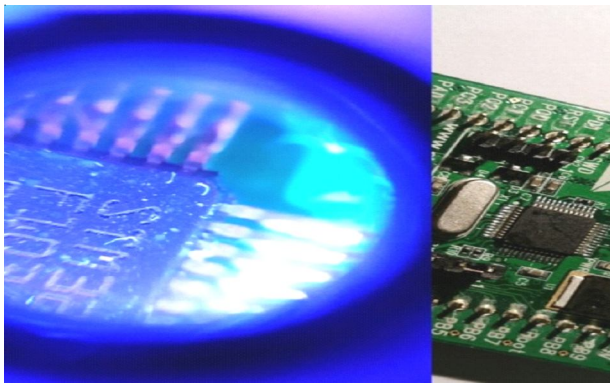

Рис. 2. Криптографический чип STM32F415

С целью подключения драйвера-двигатель (Mini Maestro 18-Channel USB Servo Controller) к главному процессору (BeagleBone Black) по UART-интерфейсу был взят конвертор ADuM1201, который предназначен для преобразования электроэнергии одних параметров или показателей качества в электроэнергию с другими значениями параметров или показателей качества. На рисунке 4 изображена плата перед вытравкой, нарисованная в программе P-CAD 2006.

Для того, чтобы провести исследования реализованной криптографической системы на предмет обнаружения проблем и ошибок, был осуществлен перехват и анализ передаваемых пакетов с помощью программы Wireshark.

С помощью Клиентской программы, передается сообщение «ololololo» роботу в открытом (незашифрованном) виде.

Предварительно авторизовавшись в Wi-Fi сети, нужно запустить Wireshark, с помощью которого будут перехвачены передаваемые пакеты. На рисунке 5 видно отправляемое слово.

Теперь передаем зашифрованное слово. Находим передаваемый пакет и видим шифрованный текст длиной в 16 байт (см. рис. 6).

Анализ пакетов реализованной криптографической системы на предмет обнаружения проблем и ошибок с помощью программы Wireshark показал, что команда, передаваемая роботизированной системе, является зашифрованной, а шифрование Wi-Fi сети (WPA2), в отличие от технологии

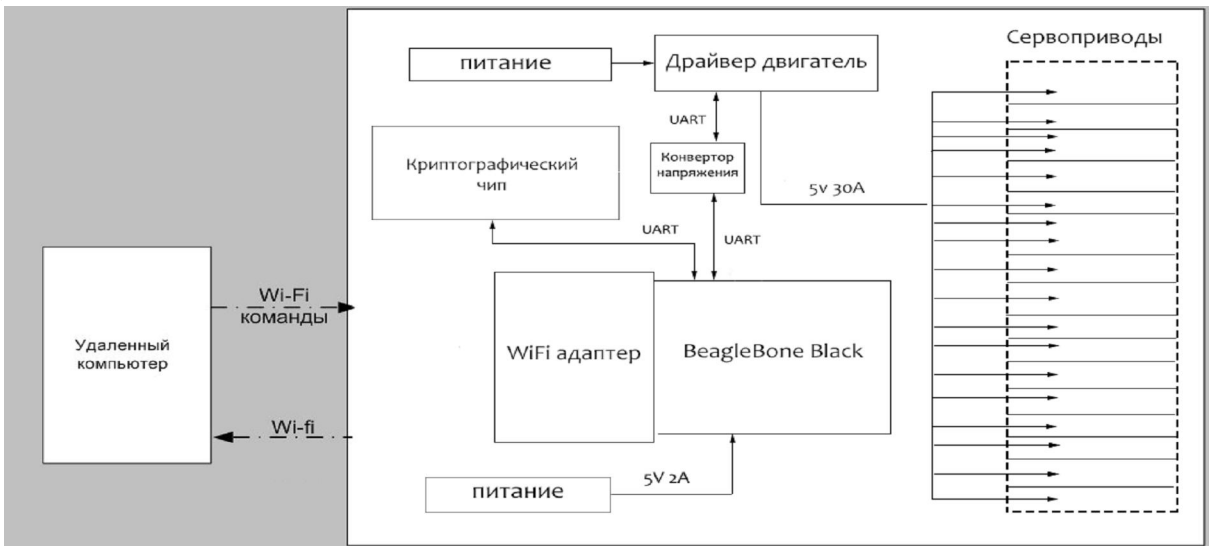


Рис. 3. Функциональная схема

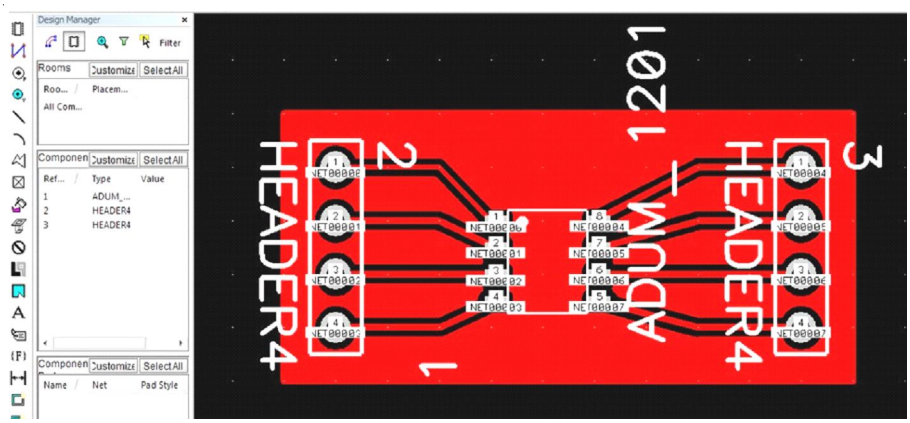


Рис. 4. Схема конвертора

Bluetooth, является дополнительным препятствием к расшифрованию секретной команды злоумышленником. Кроме этого, организована постоянная смена криптоключей, тем самым исключена возможность их подбора.

Таким образом, в настоящей статье представлен пример создания роботизированного комплекса, как элемента КБС, с защищенной системой управления им на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кроме того, для защиты от атаки «грубого перебора» криптографического ключа в системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

## *СПИСОК ЛИТЕРАТУРЫ*

1. Схема обмена ключами Диффи – Хеллмана. – Электрон. текстовые дан. – Режим доступа: http://kaf403.rloc.ru/POVS/Crypto/DiffieHellman.html . – Загл. с экрана.

2. Hexapod – робот под управлением ROS. – Электрон. текстовые дан. – Режим доступа: http://www.pvsm.ru/diy–ili–sdelaj–sam/62026. – Загл. с экрана.

3. Reference manual STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced ARM®–based 32–bit MCUs. – Электрон. текстовые дан. – Режим доступа: https://www.manualslib.com/

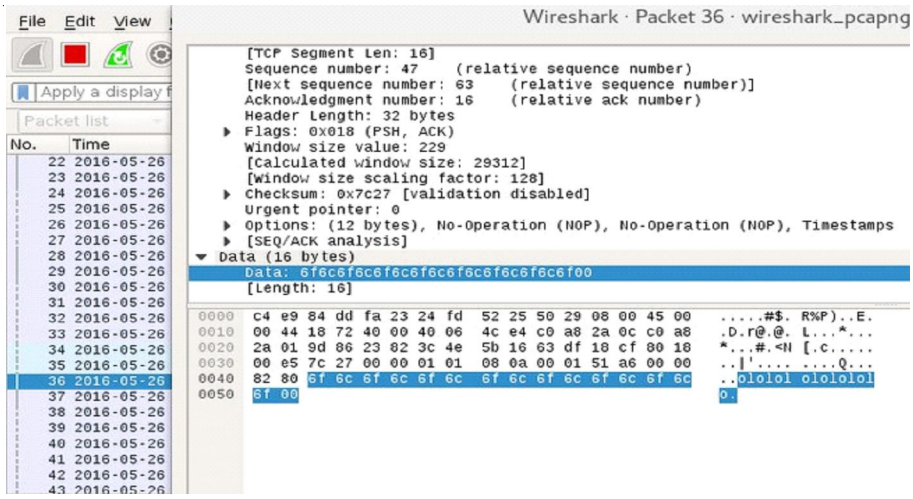


Рис. 5. Перехват незашифрованного сообщения с помощью программы Wireshark

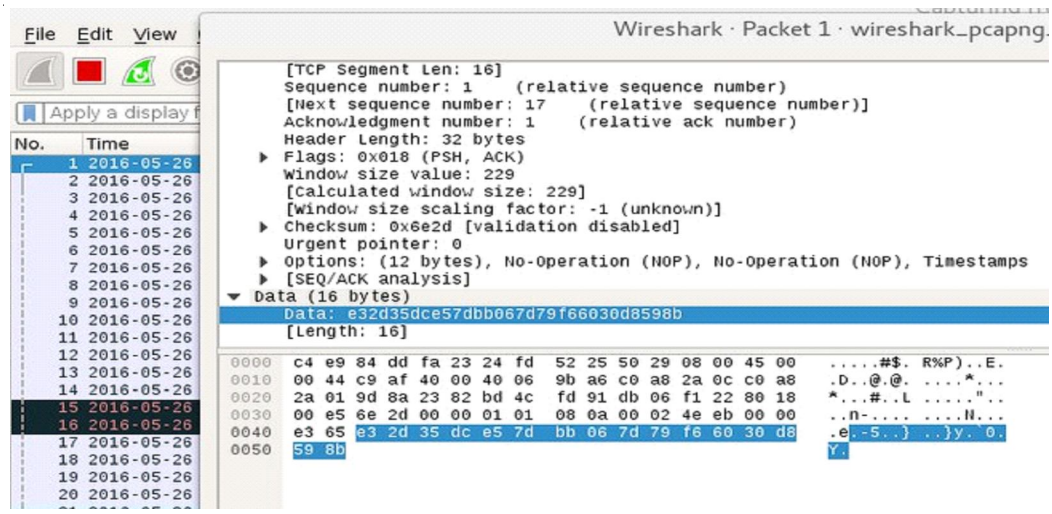


Рис. 6. Перехват зашифрованного сообщения с помощью программы Wireshark

manual/1249201/Stmicroelectronics-Stm32f405.html // STMicroelectronics, 2016. – 1744 с. – Загл. с экрана.

4. [BeagleBone Black] Enable All UART Ports at Boot. – Электрон. текстовые дан. – Режим доступа: https://billwaa.wordpress.com/2014/10/13/beaglebone–black–enable–all–uart–ports–at–boot. – Загл. с экрана.

### *REFERENCES*

1. *Skhema obmena klyuchami Diffi – Khellmana* [Diffie-Hellman Key Exchange Scheme]. URL: http://kaf403.rloc.ru/POVS/Crypto/DiffieHellman.html.

2. *Hexapod – robot pod upravleniem ROS* [Hexapod – A Robot Running ROS]. URL: http://www.pvsm.ru/diy–ili–sdelaj–sam/62026.

3. Reference Manual STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 Advanced ARM®-Based 32-Bit MCUs. *STMicroelectronics*, 2016. 1744 p. URL: https://www.manualslib.com/manual/1249201/Stmicroelectronics-Stm32f405.html.

4. [*BeagleBone Black*] *Enable All UART Ports at Boot*. URL: https://billwaa.wordpress.com/2014/10/13/beaglebone–black–enable–all–uart–ports–at–boot.

## PROTECTING THE MANAGEMENT CHANNEL OF ROBOTIC SYSTEMS

**Vladimir V. Baranov**

Candidate of Military Sciences, Associate Professor,
Head of the Department of Information Security,
South-Russian State Polytechnic University (NPI) named after M.I. Platov
baranov.vv.2015@ yandex.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

**Elnur R. Aliyev**

Master Student, Engineer, Department of Information Security,
South-Russian State Polytechnic University (NPI) named after M.I. Platov
elnur913@gmail.com
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

**Abstract.** Automated and robotic systems have an indissoluble connection between computing and physical elements included in them. Today, the representatives of such systems can be found in a wide variety of areas – space, automotive, chemical technology, civil infrastructure, energy, health, manufacturing, transportation, and consumer devices. This class of systems is often considered as cyberphysical systems.

The article presents an example of creating a robotic complex, as an element of the CBS, with a secure control system based on the AES encryption algorithm, which is currently the most crypto-resistant.

In addition, to protect against a brute-force attack on a cryptographic key, the management system must implement a key distribution algorithm to generate a new key each time before executing the command.

The article developed a robotic complex and a system that allows you to manage this complex for a reliable cryptographically stable connection. The main element of this system is the STM32F415 cryptographic chip. It allows you to reduce the load on the CPU to perform control algorithms, freeing it from cryptographic operations, thereby ensuring a gain in time.

**Key words:** channel control, cyber-physical systems, robotic systems, cryptographic algorithms.