На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XIX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина 2

Одеса
22 квітня 2019 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XIX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22 квітня 2019 р. - Одеса, Видавництво ОНАХТ, 2019 р. - 68 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Організаційний комітет

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

Наступний етап: необхідно на датчику руху повернути за годинниковою стрілкою до упору два потенціометра. Це буде означати, що максимальна чутливість стане близько 7 метрів. При необхідності чутливість можливо змінити в меншу сторону, обертаючи потенціометр в зворотному напрямку. Другий потенціометр відповідає за тривалість після спрацьовування. Максимальне значення 5 хвилин; це максимальне значення даного датчика, після чого надійде сигнал на мікроконтролер, який сигналізує про припинення русі в приміщенні і відключиться освітлення. При появі руху світло знову включиться. Після складання він має бути увімкненим, датчик руху почне автоматичне калібрування, яка триває одну хвилину. Після завершення калібрування наше пристроєм можна користуватися.

IV. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Представлена реалізація дозволяє продемонструвати застосування розвитку сучасних мікроконтролерів для розробки пристрою розумного освітлення з метою економії електрозатрат.

V. ВИСНОВКИ ТА ВИСНОВОК

Нами були розглянуті компоненти, що дозволяють зробити не пристроєм не тільки з дистанційним управлінням, а й інтелектуальним, тобто розумне пристрій, який не тільки слухається команд, але й саме спостерігає за тим, що відбувається.

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ПРОТОКОЛУ MODBUS RTU ВІД ЗЛОВМИСНОГО ВТРУЧАННЯ

Болмосова Д.Д., студентка, Стопакевич О.А., доцент
Одеський національний політехнічний університет

Метою роботи є дослідження захищеності відомого протоколу Modbus RTU реалізованого на базі мережі RS-485 від зловмисного втручання.

Протокол Modbus розроблений для використання в запрограмованих логічних контролерах і в даний час є досить поширеним. Протокол Modbus має два режими передачі даних: Modbus ASCII (American Standart Codetfor information Interchange), Modbus RTU (RemoteиTerminal Unit).Перевагами протоколу Modbus є відсутність необхідності в спеціальних інтерфейсних контролерах і простота програмної реалізації. Він дозволяє уніфікувати команди обміну завдяки стандартизації номерів (адрес) регістрів і стандартизації функцій їх читання і запису [1].

Modbus RTU розташований на другому шарі моделі ISO / OSI, він спілкується по послідовній лінії, як правило, на RS485 або RS232. Це протокол master-slaves, в якому частиною однієї мережі може бути лише один ведучий і не більше 247-ми пристроїв типу Slave. Запит може бути відправлений в одноадресний або широкомовний режим, він вимагає, щоб у кожного підлеглого була унікальна адреса. Майстер запускає тільки одну транзакцію за

один раз. Пристрої ніколи не передають дані без отримання запиту від головного вузла і ніколи не зв'язуються один з одним. Протокол Modbus не забезпечує захист від несанкціонованих команд або перехоплення даних. Оскільки Modbus був розроблений в кінці 1970-х років для зв'язку з програмованими логічними контролерами, чисельність типів даних обмежена тими, які були зрозумілі програмованим логічним контролерам у той час. Великі виконавчі об'єкти не підтримуються. Modbus не підтримує ідентифікації і шифрування, це призводить до того, що вся комунікація здійснюється у незахищеному режимі.

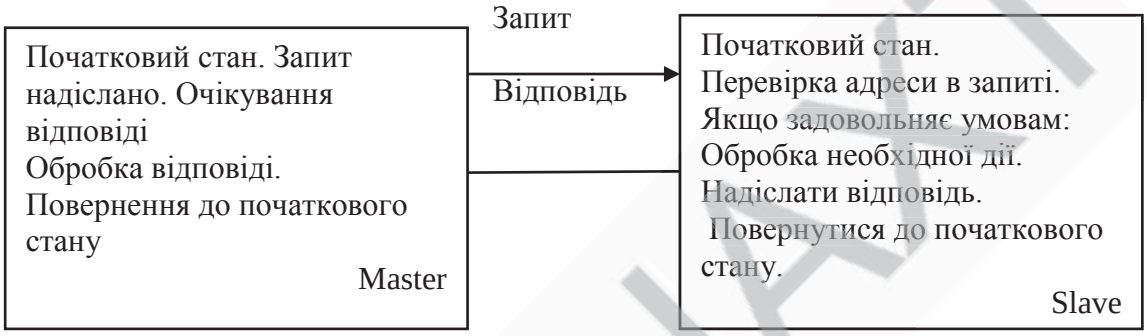

Рис. 1- Одноадресний зв’язок Modbuc RTU

Нашою першою метою було визначити мету зловмисника. Як бачимо, багато недоліків можна знайти через відсутність двох найважливіших складових безпеки властивостей конфіденційності та цілісності. На Рис.1 ми бачимо, що зловмисник керує чотирма слабкостями протоколу, це кореневі елементи дерева атаки. По-перше, це перехоплення даних, яке включає в себе, наприклад, моніторинг каналу, потім переривання зв'язку - це може бути викликане, наприклад, DoS-атакою, третя - модифікацією повідомлень, а останньою є фабрикування даних .

Нашою другою метою було розкрити, як зловмисник може досягти цих цілей, всі кореневі елементи можна досягти за допомогою MITM-атаки (атака «людина посередині»), наприклад, посадка шлюзів або скомпрометовані slave або master-пристрої у мережі.

1) Перехоплення

Під час перехоплення зловмисник захоплює повідомлення, відправлені по мережі, отримуючи таким чином інформацію про параметри і роботу системи, тому в цій атаці втрачається конфіденційність даних і системи.

2) Переривання

Мета атакуючого полягає в погіршенні ефективності системи. Наприклад погіршення економічної ефективність, або подібні параметри, маніпулювати ними, або просто перевантаження системи, щоб вивести її із строю. Пошкодження нормальної роботи системи викликає пошкодження цілісності даних або системи.

3) Модифікація

Неавторизовані особи змінюють повідомлення, надіслані по каналу, що призводить до пошкодження цілісності даних або системи.

4) Виготовлення

Під час виготовлення зловмисник визначає себе як авторизований користувач і надсилає сфабриковане повідомлення учасникам системи. Через цю атаку втрачено багато властивостей безпеки, такі як цілісність даних, аутентифікація або конфіденційність.

Список літератури

1. Гайнуллина А. А., Байтимиров А. Д. Особенности организации передачи данных между программируемыми логическими контроллерами по протоколу Modbus // Вестник Казанского технологического университета. – 2013. – №23. – с.2-4.

СИСТЕМА РОЗПІЗНАВАННЯ ГОЛОСОВИХ КОМАНД ДЛЯ КОМП'ЮТЕРНИХ СИСТЕМ

Гавенко О.М., Студентка СВО «Магістр» ф-ту КІПтаК
Науковий керівник – Артеменко С. В., д.т.н., завідувач кафедри КІ ОНАХТ

Сучасний прогрес суспільства обумовлений розвитком автоматизованих та комп'ютерних технологій. Комп'ютери та портативна техніка невід'ємний атрибут людського життя. Науково-технічна проблема створення засобів для взаємодії користувачів з комп'ютерними системами (КС) завжди було на перше-етапною задачею.

Очевидно одним з перспективних шляхів вирішення даної проблеми може стати використання людської мові в управлінні цими системами, веденням голосових команд, які будуть розпізнані КС.

Актуальність теми роботи

Набір текстів програм здійснюється з клавіатури, що потребує хороших навичок при роботі з нею та великої уваги та напруги зору. Цей спосіб є достатньо ресурсо затратний. Вирішення цієї проблеми може стати автоматизоване ведення та керування за допомогою розпізнавання голосових команд. Таким чином, актуальність ведення та розпізнавання голових команд може полегшити життя не тільки спеціалістів але і всіх користувачів КС[1].

Основні завдання дослідження:

1. Розгляд основних методів розпізнавання мовного сигналу.
2. Аналіз методів обробки звукового сигналу, для подальшого їх використання .
3. Розробка методу визначення голосових команд, які будуть виконуватися.
4. Реалізація створеного методу в програмному продукті, аналіз ефективності з існуючими методами розпізнавання мови, виявлення переваг і недоліків.