Students vs IoT security

What is this talk about.

- A project for the minor Security Lab
- Project’s aim was to combine Security and IoT devices
- The choices we made during the project

What was the project.

- Make 2 devices communicate securely using the ESP8266 (NodeMCU)
- Devices need to be securely updatable
- Devices need to give feedback to the user
- Devices needs to be wireless

Timetable

- 5 week project
- 1 week preparing
- 3 weeks of programming/prototyping
- 1 week for making marketing material (posters and a commercial) and presenting

How do we program the esp8266

- Lua or Arduino IDE
- More comfortable with Arduino
- Flashing Lua did not always work
- Arduino had better support (in my opinion)

Connecting to the internet

- Create captive portal for configuration
- Portal was protected with a password
- Connect to a Wi-Fi network
- Reset when local network is not found

Sending data to the server

- Received a VM from my school
- Bought domain name with Github student pack
- Used Letsencrypt for the Certificate
- Used TLS with certificate pinning for the connection
- Message was not encrypted. (Encryption libraries too slow or large)
- Server was a python server made with Flask

Saving the data

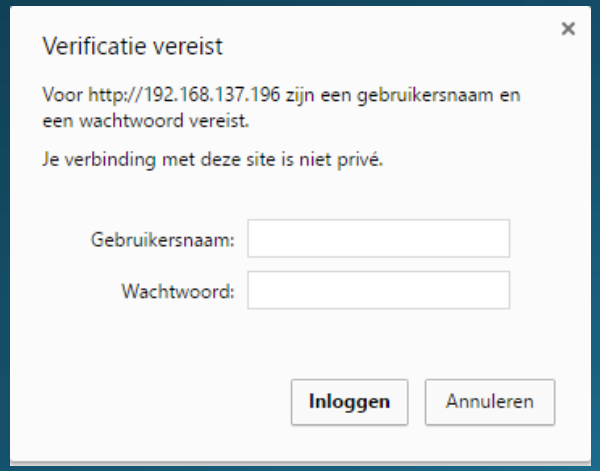
- Message was SenderID|ReceiverID|store|message
- SenderID and ReceiverID were stored in the Database and on the EEPROM of the devices
- If the IDs matched with IDs in the database save the data
- Any other case provides an error
- How did we protect against brute force?
  - Make the IDs very long!

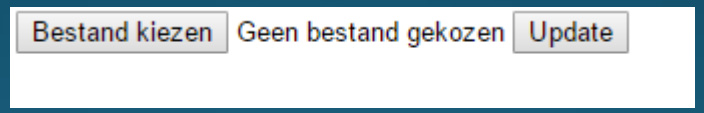
Retrieving data

- Almost the same system as saving the data SenderID|ReceiverID|retrieve
- After retrieving the message the message is deleted from the database
- Privacy friendly, no user information anywhere

Updating the device

- Local website on the device for uploading new firmware
- Wireless updates were faster then updates with USB
- Username/password protected
- Automatic updating took too much time to do right





Hardware fun

- Led indicators for send , receive, Wi-Fi status and errors
- Pre-programmed led sequence for errors, no message, send and receive
- Buttons for send and receive
- 3D printed design.

Any questions?

References

- https://www.arduino.cc
- https://github.com/esp8266/Arduino
- http://www.esp8266.com/
- https://github.com/tzapu/WiFiManager
- http://flask.pocoo.org/