ET0731 IOTS Presentation Slides

Done by: Group 7

Lim Zheng Long (2032555)

Lim Jun Hong (2032568)

Wang Zheng (2032638)

Title: Secure IoT Lock

Content

1. Overview of Secure IoT Lock
2. Features of Secure IoT Lock
3. Security Features of IoT Lock
4. Diagrams
5. Code Pre-requisites
6. TR64 Compliance Checklist
7. Threat Modeling
8. Security Testing

Overview of Secure IoT Lock

- Unlocked wirelessly via webpage
- Provides security features like data encryption and 2 Factor Authentication
- Easy to use
- Cost effective

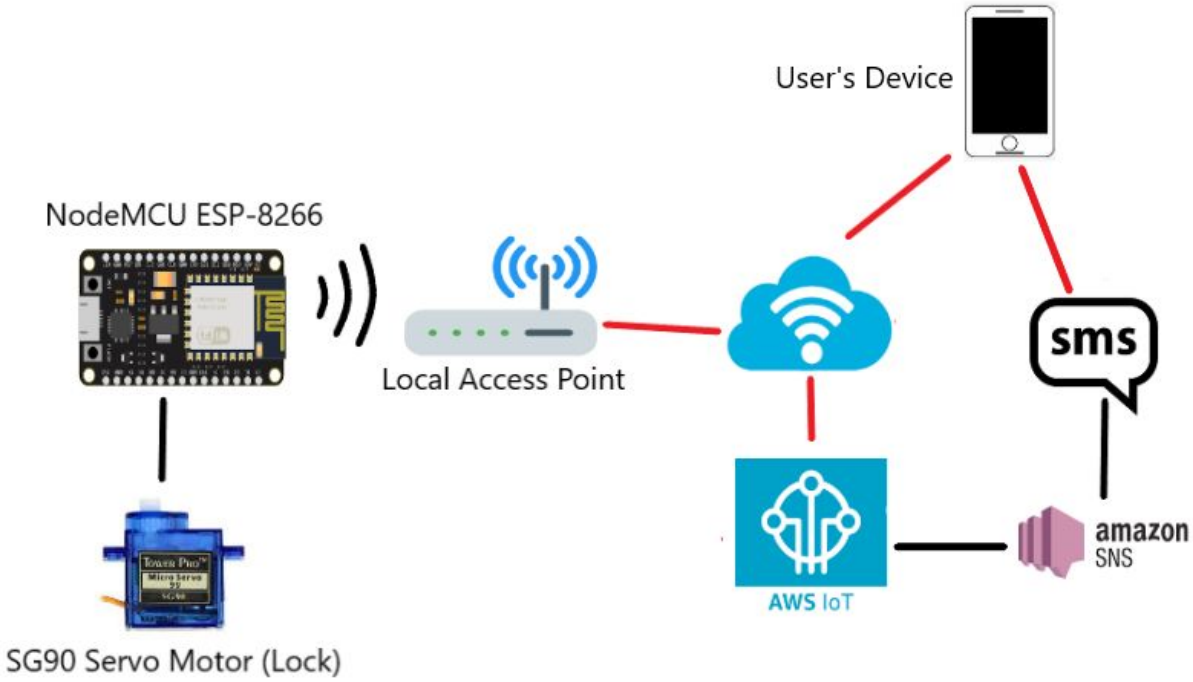
Features / Components of Secure IoT Lock

- NodeMCU ESP-8266
- SG90 Servo Motor
- AWS SNS
- Web Page Login System

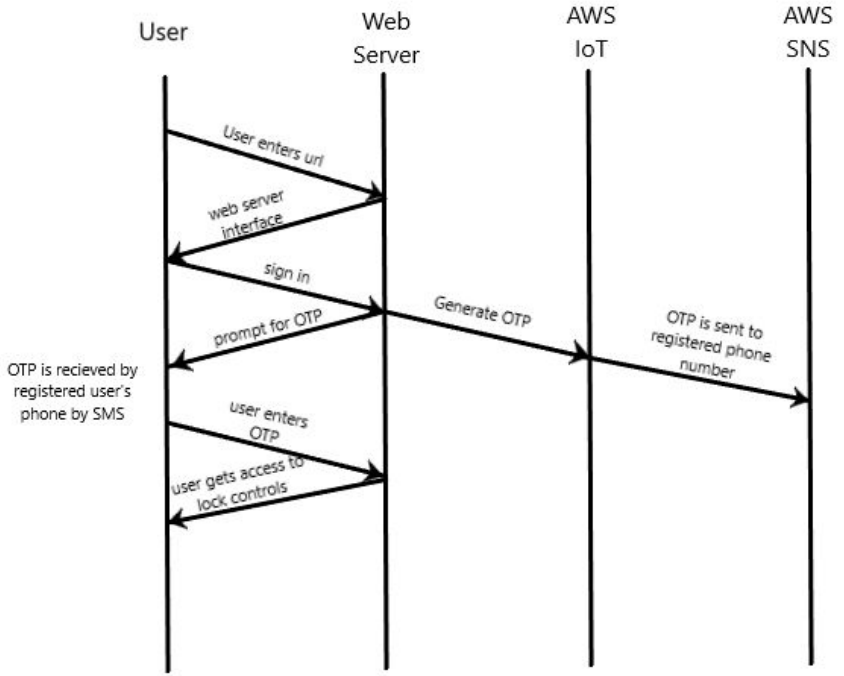
Security features of Secure IoT Lock

- 2 Factor Authentication’
- Account Lockout
- AWS Security

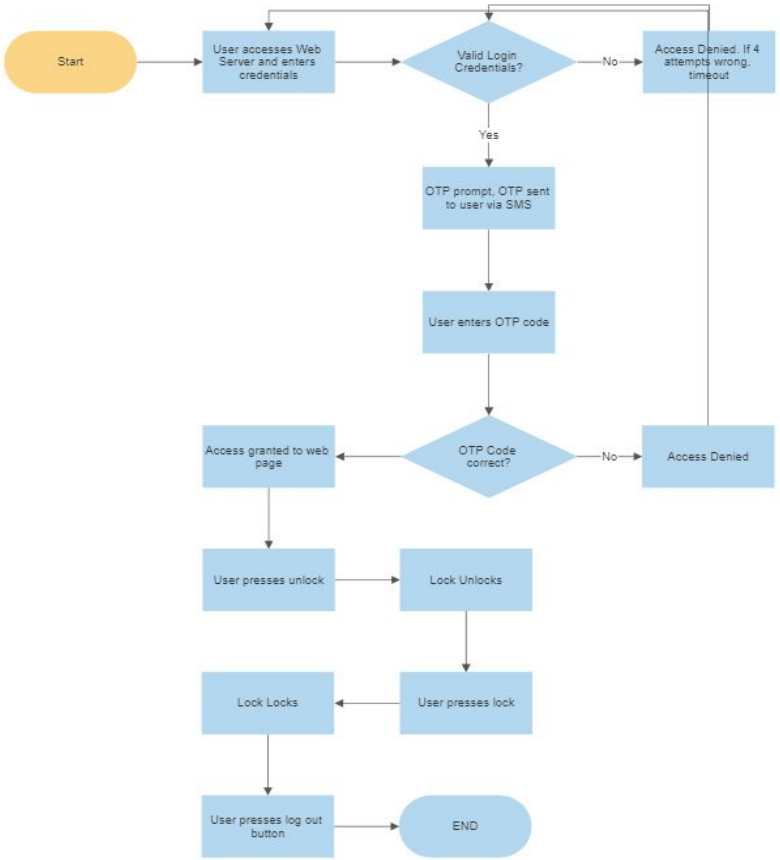
Diagrams


User's Device
NodeMCU ESP-8266
Local Access Point
sms
AWS IoT
amazon
SNS
SG90 Servo Motor (Lock)

Diagrams


User
Web Server
AWS IoT
AWS SNS
User enters url
web server interface
sign in
Generate OTP
OTP is sent to registered phone number
prompt for OTP
OTP is recieved by registered user's phone by SMS
user enters OTP
user gets access to lock controls

Diagrams


Start
User accesses Web Server and enters credentials
Valid Login Credentials?
No
Access Denied. If 4 attempts wrong, timeout
Yes
OTP prompt, OTP sent to user via SMS
User enters OTP code
Access granted to web page
OTP Code correct?
No
Access Denied
User presses unlock
Lock Unlocks
Lock Locks
User presses lock
User presses log out button
END

Code Pre-requisites

Needed to set up AWS IoT Core and AWS SNS

1. Creating Thing
2. Create Policies and download certificates linked to thing
3. Register user’s phone number to SNS Topic
4. Create Rules in AWS SNS

TR64 Compliance Checklist

Attack Surface	Check List	TR64 Reference	Description
Web Page	Device control on web page is secured against unauthorised access, 2FA used for access, lockout for repeated unauthorised login attempts	CK-IA-01 CK-AP-01	Unique username and password with 2-factor authentication used to access webpage, account lockout after too many unsuccessful logins
AWS	For MQTT, TLS is used to encrypt the connection between device and the broker. Data in transit to and at rest in AWS IoT is secured by using TLS and is encrypted	CK-NP-03 CK-DP-01	AWS message broker encrypts all communication in transit using TLS version 1.2 All data in AWS IoT at transit and at rest are encrypted
Hardware (SG90 Servo Motor & ESP-8266)	Housed in tamper resistant box, no exposed wires and ports	CK-AP-03 CK-AP-04	Hardware components are not easily accessed, wires and ports cannot be connected to
Security Audit	Logging of significant events	CK-AU-01	Logging of successful and unsuccessful attempts to access webpage, logging of lock control
System Wide	Conducted threat modelling to identify, analyse and mitigate as much threats as possible	CK-LP-01	Conduct threat modelling using STRIDE framework

Threat Modeling

Threat modelling checklist	Y/N	Supporting materials
Identify the potential target(s) to be protected	Y	Authorised users of the lock Access to the web server controlling the lock
Define the security problem	Y	Brute force attacks to login to the website and gain access to the lock (Elevation of privilege)
Conduct risk assessment	Y	High reproducibility, exploitability and discoverability
Determine the security objectives	Y	Unauthorised users should be stopped from gaining access to the lock
Define the security requirements	Y	Brute force attempts can be mitigated with a lockout Authentication of authorised users
Design and implement the capabilities	Y	Users will be unable to log in after multiple failed attempts User will need a SMS OTP to log in to access the lock
Validate and verify that the capabilities address the security requirements adequately	Y	Account lockout and OTP for 2 Factor Authentication works and is able to prevent unauthorised access into the webpage

Security Testing

Planned to use Kali Linux and Aircrack to crack password to wireless network.

1. Plug in network adapter that supports monitor mode
2. Install Aircrack-ng
3. Enable monitor mode
4. Type command to show target network’s BSSID / MAC address
5. Deauthenticate BSSID to capture necessary data for password cracking
6. Download password wordlist from online sources
7. Type in command to start password cracking process
8. Eventually either password to network is found or passwords in wordlist is used up and password to network cannot be found