# Threat Analysis and Risk Assessment (TARA)
# NTI – Team 3 SEITech

# Team Members

- Eslam El-Sayed Refaat
- Mohamed Abd El-Naby Mohamed
- Rana Abd EL-Salam Mahmoud
- Salma Mohamed Hashim
- Shaimaa Mahmoud Samir
- Sherif Atef Sadek
- Youssef Ahmed Mohamed

# Identify Assets, Threats, Vulnerability, and attack analysis

## Use Case : Exchange data between OBU and RSU (Traffic Light)

| **Violation of the Security Property :** | **Integrity** |
|---|---|
| Of the Asset : | Data Between ECU and RSU |
| May lead to : | Modified Data, that may lead to people being injured. |
| By using the (STRIDE) Threat | |
| Due to the Vulnerability ; | Unsecure data change |
| With the Attack : | An Attacker is changing the exchanged data by using sharing the same RSU msg |
| Causing impact on Security Objective : | Safety |

# Impact Assessment

## Use Case : Exchange data between OBU and RSU (Traffic Light)

| Impact Level Assessment | | | | | |
|---|---|---|---|---|---|
| Safety Impact | Financial Impact | Operational Impact | Privacy Impact | Impact Value | Impact Level |
| High (200) | Low (20) | LOW (5) | Low (5) | 230 | HIGH |
| High Probability to make an accident if data between RSU and OBU changed that cause an accidents | If Data Changed the Driver may handle the situation manually using the drive wheel. | No change in vehicle behavior. | No Sensitive data like credit card detail between OBU and Traffic Light. | | |

| | |
|---|---|
| 0 | No Impact (0) |
| [1-19] | Low (1) |
| [20-99] | Medium (2) |
| [100-999] | High (3) |
| >999 | Critical (4) |

# Feasibility Assessment

## Use Case : Exchange data between OBU and RSU (Traffic Light)

| Feasibility Level Assessment | | | | | |
|---|---|---|---|---|---|
| Expertise | TOE | Window Opportunity | Equipment | Threat Value | Thread Level |
| 2 | Public (0) | Medium (5) | Standard (0) | 7 | LOW |
| Doesn't Need Expert Person do make an attack. | No Sensitive Data | In The Period of connected to RSU | Just Need To Simulate RSU Node with the same name and public key. | | |

# Determine Security Level

Use Case : Exchange data between OBU and RSU (Traffic Light)

Due to High Impact and Low Fess ability, System has High Security Level

| Security Level (SL) | | Impact Level (IL) | | | | |
|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 |
| Threat Level (TL) | 0 | QM | QM | QM | QM | Low |
| | 1 | QM | Low | Low | Low | Medium |
| | 2 | QM | Low | Medium | Medium | High |
| | 3 | QM | Low | Medium | High | High |
| | 4 | Low | Medium | High | High | Critical |

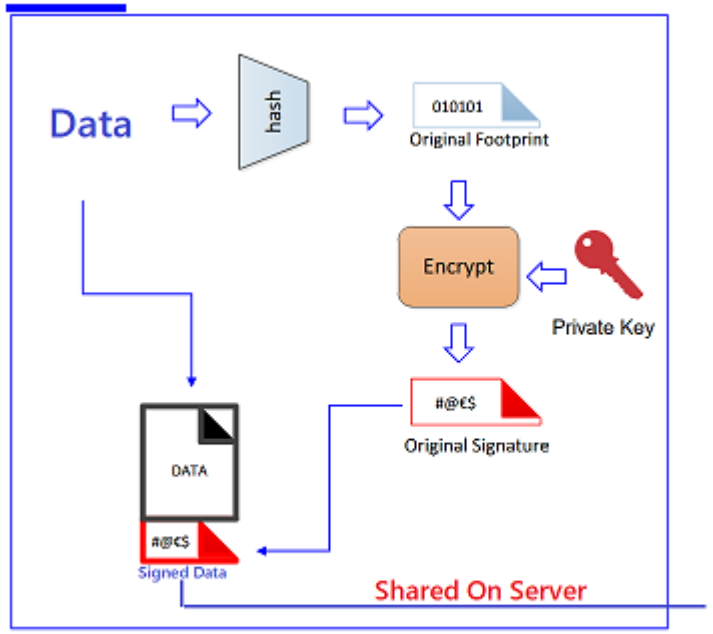
# Mitigation

Use Case : Exchange data between OBU and RSU (Traffic Light)

To Mitigate Changing in data Threat Must Design Digital Signature Mechanism:
Private Key: Signing the Vehicle and RSU with the private key
Public Key : Downloaded into ECU only.
Signed Firmware : Provide to RSU provider.
Noted That: Only Signed Data is accepted to/from RSU
Digital Signature Covers The Integrity and Authentication and don't cover Availability

# Mitigation

## Server Side (RSU)




Server Side

Example

{"Service":"TrafficLight","CRC":52,"State":"s\\x9b\\x1bo&\\x11\\xe6Z\\x90\\xaa\\xe4\\xc4\\x8b(J\\x89J\\x8d\\x11\\xd9\\xf4\\x99\\xd5g\\x04"}

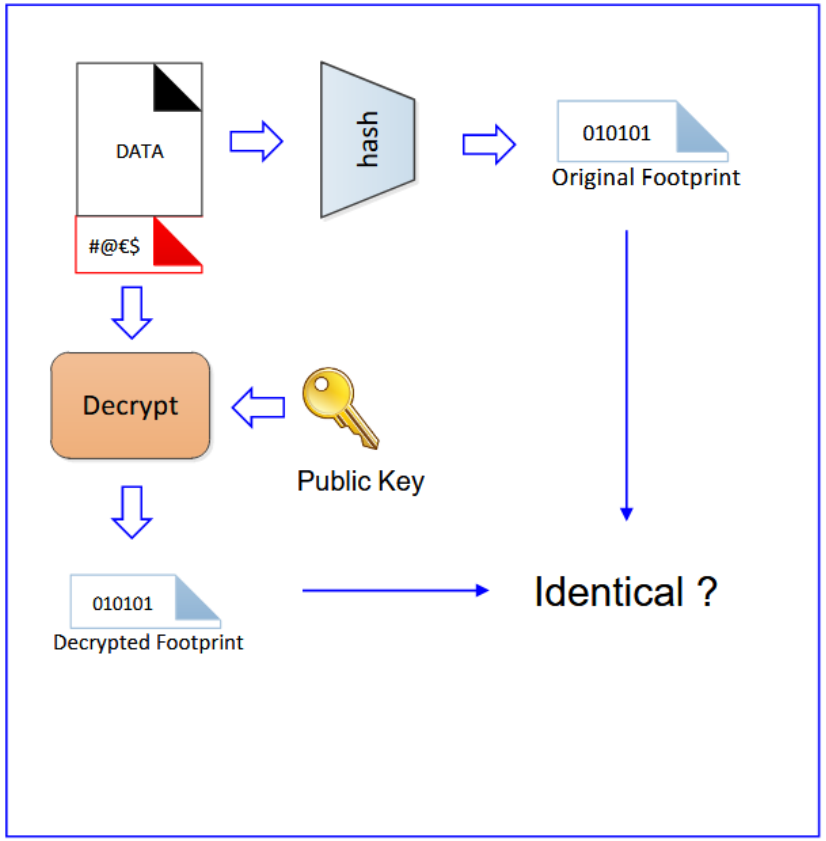
Service Name

Intigraity

Encrypted Data with Key based on AES

# Mitigation

## Client Side (OBU)




<u>Extract Information After OBU Connected to RSU</u>:

Service: TrafficLight

CRC: 0x34

State: TL_STATE:_RED_LED_ACTIVE_

Calculated CRC: 0x34

DATA:VALID

# NUCLEO32-F303RE

- Has Hardware CRC Module
- Hasn’t HSM Module