# Residential Temp Sensor Security

ROHAN MALIK

# Idea

- A Residential Freeze/Humidity Warning Sensor
- Security concerns in residential space differs from commercial or public
  - The device is physically safe and the end-user can generally be trusted
  - the device needs to be secured on the network from outsiders who could leverage vulnerabilities to access the internal network

# Physical Considerations

- Plastic enclosure
  - no easy access to internal part numbers
  - USB is not accessible
- External power supply
  - A real product would not use a development board, so this would be handled
- Disabling JTAG/enabling Secure Boot is not necessary

# Software Considerations

- Each device has its own certificate, RSA private/public key, and MQTT client ID
- Serial console left on, but has a password for the root commands
- Communicates the minimum amount of information
  - Publishes topic with temperature & humidity
  - no subscribed topics

```
esp_mqtt_client_config_t mqtt_cfg = {
    .uri = mqtt_broker_url,
    .cert_pem = AWS_ROOT_CA,          // AWS CA
    .client_cert_pem = DEVICE_CERT,   // Device Certificate
    .client_key_pem = PRIV_KEY,        // Private key
    .client_id = "IoT_Board"           //Client ID
};
```

# AWS IoT Setup

- Policies
  - Separate policy for connect and publish
  - Easier to manage and audit devices/data
- MQTT over TLS with X.509 Client Certificates
- Uses Amazon SNS to sent an email

# AWS IoT Connect Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "Bool": {
                    "iot:Connection.Thing.IsAttached": [ "true" ]
                }
        },
        "Effect": "Allow",
        "Action": "iot:Connect",
        "Resource": "arn:aws:iot:us-east-1:149959063004:client/${iot:Connection.Thing.ThingName}"
        }
    ]
}
```

# Publish Policy

| Policy effect | Policy action | Policy resource |
| --- | --- | --- |
| Allow | iot:Publish | arn:aws:iot:us-east-1:149959063004:topic/env_data |

# SNS Action

```
SELECT temperature, humidity FROM 'env_data' WHERE temperature > 50 AND
humidity > 30
```

# Example Email

phone <no-reply@sns.amazonaws.com>
Mon 4/11/2022 2:26 AM

To: Malik,Rohan

[External Email]

{"temperature":69.7,"humidity":46.38}