Edge Computing based Security Designs

Dr. Kewei Sha

Dept. of Computing Sciences & Cyber Security Institute

University of Houston – Clear Lake

sha@uhcl.edu

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Agenda

- Introduction
- Edge-based Security Design
  - EdgeSec: Design of an Edge-based security service
  - Edge-based two-phase authentication protocol
- Open Research Problems
- Conclusion

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Pervasive Security Threats

- Smart home
  - Home network is compromised after breaching one device
- Smart grid
  - False data insertion disturbs the system state estimation
- Smart vehicle
  - Vehicles is remotely stopped when driving
- Smart community
  - Smart devices are compromised and controlled to launch DDoS attack

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

IoT: New Security Challenges

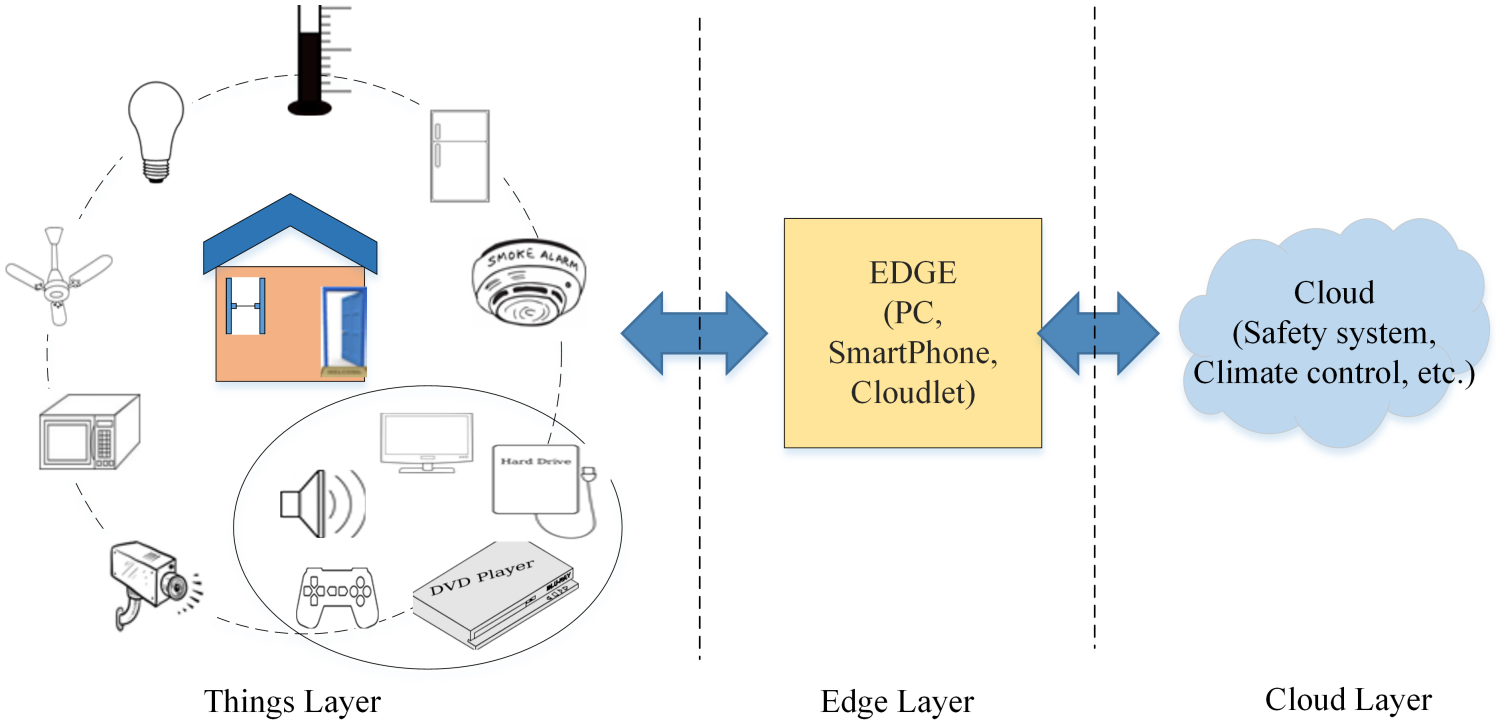
- Constrained resources
- Extremely large scale
- Heterogeneous devices & communication channels
- Direct impact on physical systems
- Tradeoff between security and usability
- Higher privacy requirements
- Trust management

University of Houston Clear Lake

Introduction of Edge Computing

- An extension of Cloud Computing
- A support of IoT applications
- Features
  - Heterogeneity, from cloudlets to gateways
  - Flexibility, created and extended as needed
  - Extensibility, relocation of distributed cloud services
  - Locality, moving computing close to data
  - Connectivity, a direct hub to connect and support IoT Things

Edge Computing Architecture



Cyber Security Institute
University of Houston-Clear Lake

Cloud, Edge & Things

Cloud	Edge	Things
Rich in resources	Rich or reasonable rich	Resource-constrained
Well protected environment	Protected environment	Poorly protected environment
Professionally administrated	Administrated from cloud or ad hoc	Mostly self-administrated
Service provider	Local service provider	Sensors & actuators
Global information	Regional information	Local information
Far away from the physical world	Close to the physical world	Coupling with physical world
Mostly trustable	Somehow trustable	Not very trustable

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Why Edge Supported Security

- ❑ More resources than the Things layer
- ❑ Close to the Things layer
- ❑ More available information than the Things layer
- ❑ Relative more stable relationship with Things
- ❑ High-speed connection with the Cloud
- ❑ Flexible enough to deploy various services

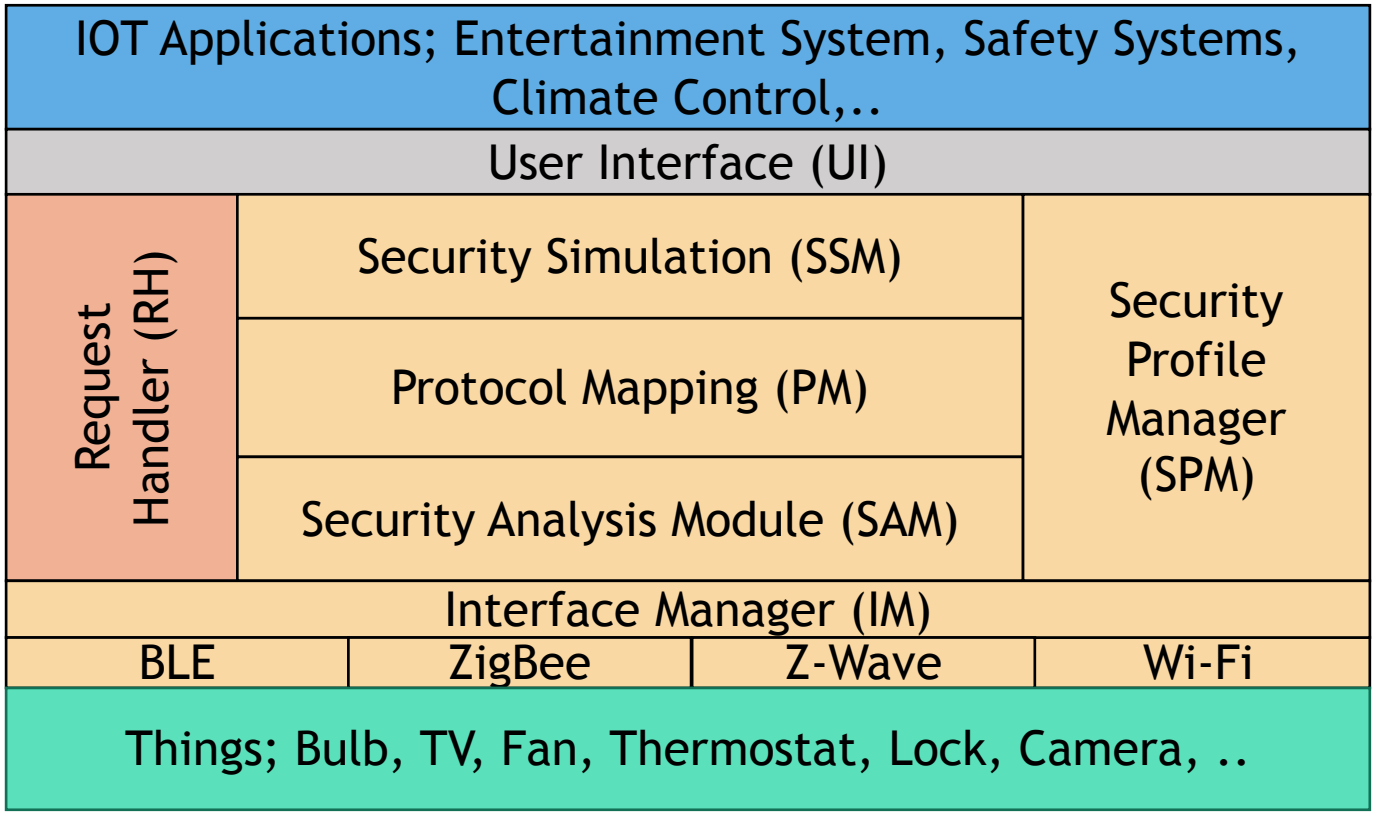
University of Houston Clear Lake

Edge Computing: A Layer to Design & Deploy Security Solutions for IoT applications

University of Houston Clear Lake

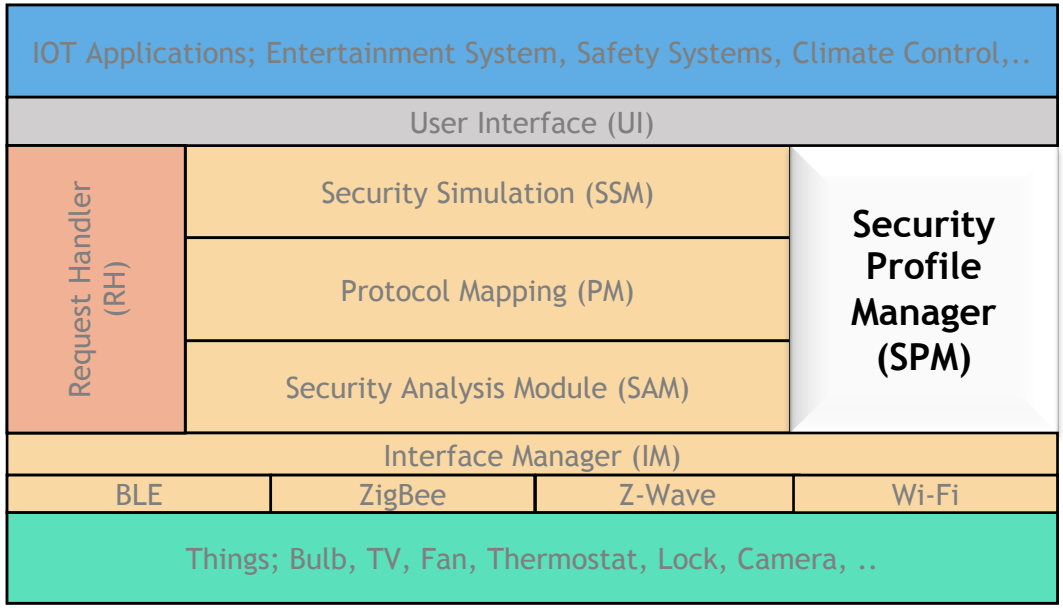
Case Study 1: EdgeSec

EdgeSec: the design of Edge layer security service



Security Profile Manager (SPM)

- Device Registration
- Profile Creation
  - Device Category
  - Type of data
  - Type of actions



Cyber Security Institute
University of Houston-Clear Lake

Examples of Device Categories

Category	RAM	ROM	Source of Power Supply	Security mechanisms supported	Communication Protocols	Example devices
Constrained	Up to 10KB	Up to 128KB	Battery	Do not support any traditional security mechanisms	IEEE 802.15.4	Phillips Hue
Limited	10-32KB	128-512KB	Battery	Support Symmetric key protocols	IEEE 802.15.1/4	August smart lock
Restricted	32-128KB	512 KB - 10MB	Battery/AC power supply	Support Symmetric and light weight asymmetric key protocols	IEEE 802.15.4 , IEEE 802.11	Nest smoke detector
Normal	128KB and above	10MB and above	AC supply with optional battery backup	Supports all traditional security protocols	IEEE 802.11 , IEEE 802.15.1, IEEE 802.15.4	Nest Learning Thermostat, Samsung Smart TV

University of Houston Clear Lake

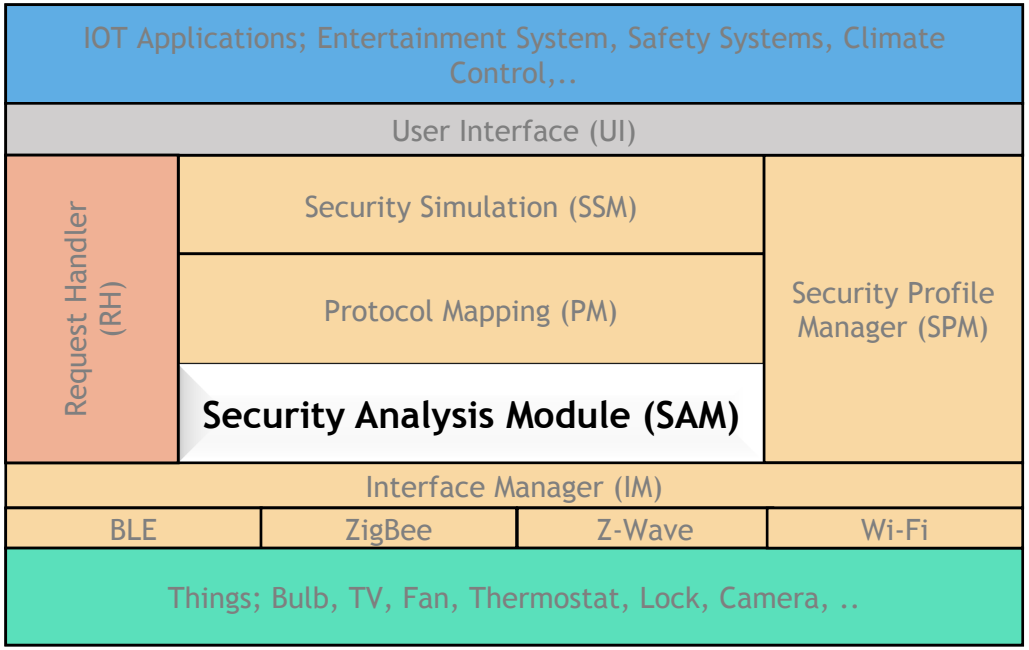
Examples of Device Security Profiles

Devices	Category	Type of data	Type of action
Smart TV	Normal	Internal	Risky
Smart Bulb	Constrained	Internal	Controlled
Smart Lock	Limited	Confidential	Critical
Camera	Normal	Confidential	Controlled
Thermostat	Normal	Internal	Risky

University of Houston Clear Lake

Security Analysis Module (SAM)

- Security functions deployment
- Security dependency analysis



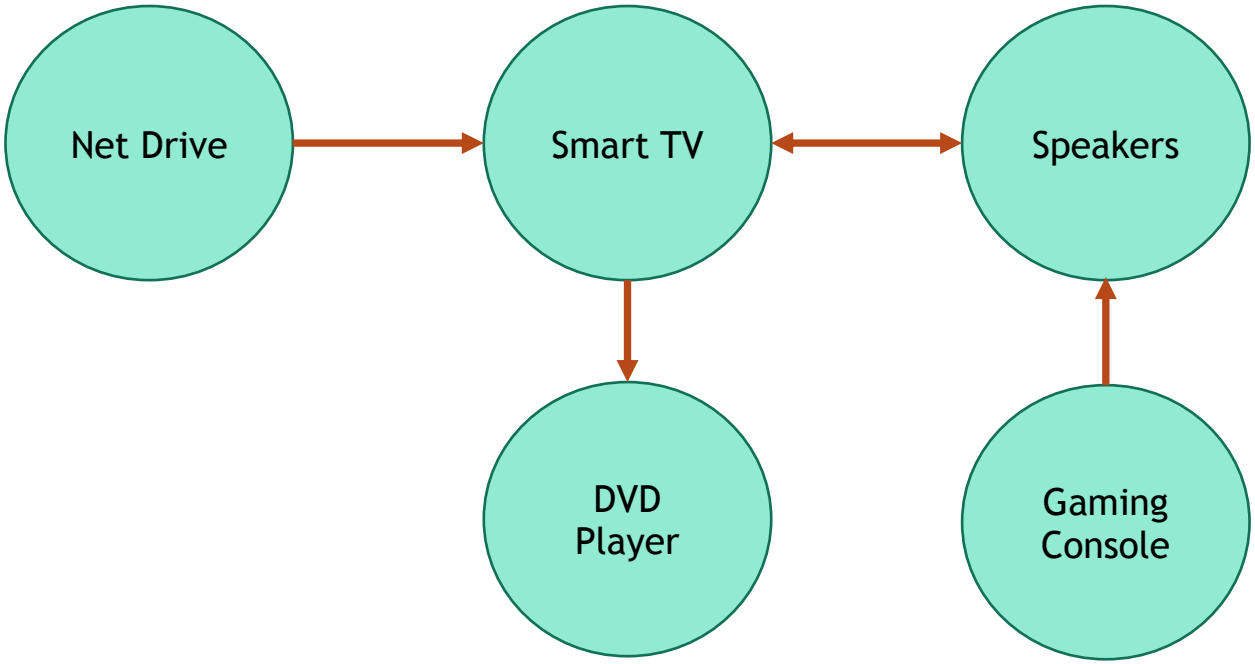
Examples of Security Functions Deployment

Device	Confidentiality	Data Integrity	Authentication	Availability	Privacy
Smart TV	End	End	End	Edge	Edge
Smart Bulb	Edge	Edge	Edge	Edge	Edge
Smart Lock	Edge	Edge	Edge	Edge	Edge
Camera	End	End	End	Edge	Edge
Thermostat	End	End	End	Edge	Edge

University of Houston Clear Lake

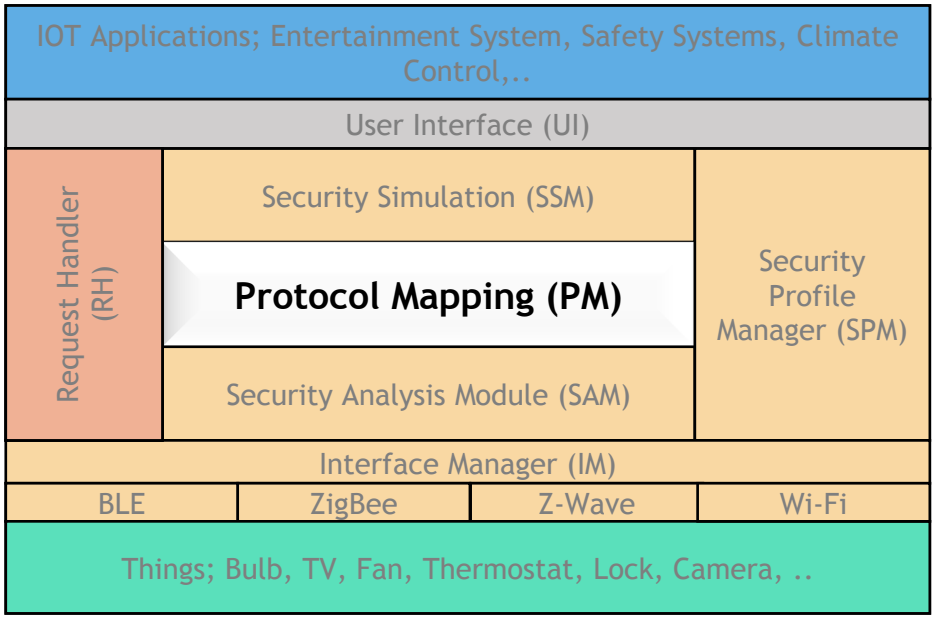
Examples of Security Dependency Analysis

Directed graph is used to model security dependency



Protocol Mapping (PM)

- Chooses candidate protocols based on available resources and security profiles
- Selects appropriate protocols from protocol library



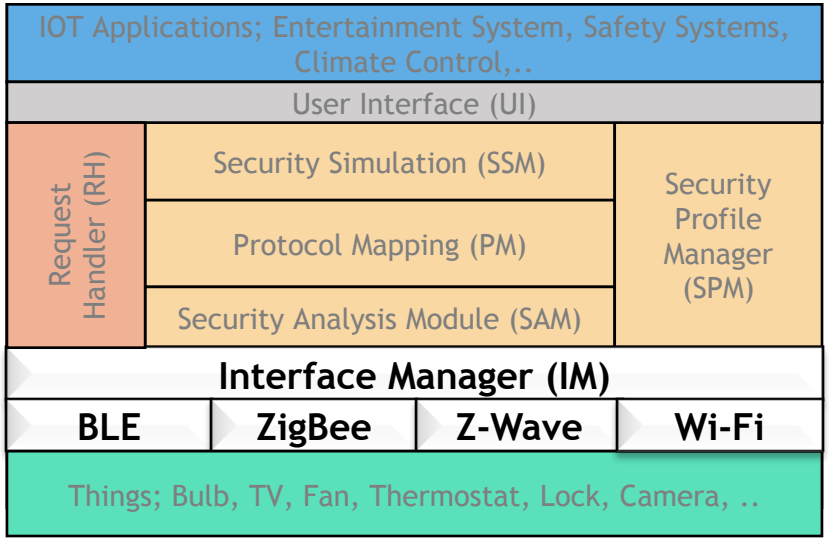
Examples of Protocol Mapping (PM)

Devices	Confidentiality	DI	AA	Avail.	Privacy
Smart TV	TLS	TLS	TLS	Firewall and IDS	K-anonymization
Smart Bulb	TLS	TLS	TLS	Firewall and IDS	K-anonymization
Smart Lock	TLS- for cloud to Edge segment; [22] – for Edge to End segment	TLS- for cloud to Edge segment; [22]- for Edge to End segment	TLS- for cloud to Edge segment; [22]- for Edge to End segment	Firewall and IDS	K-anonymization
Smart Camera	TLS	TLS	TLS	Firewall and IDS	K-anonymization
Thermostat	TLS- for cloud to Edge segment; Not supported – for Edge to End segment	TLS- for cloud to Edge segment; Not supported – for Edge to End segment	TLS- for cloud to Edge segment; Not supported – for Edge to End segment	Firewall and IDS	K-anonymization

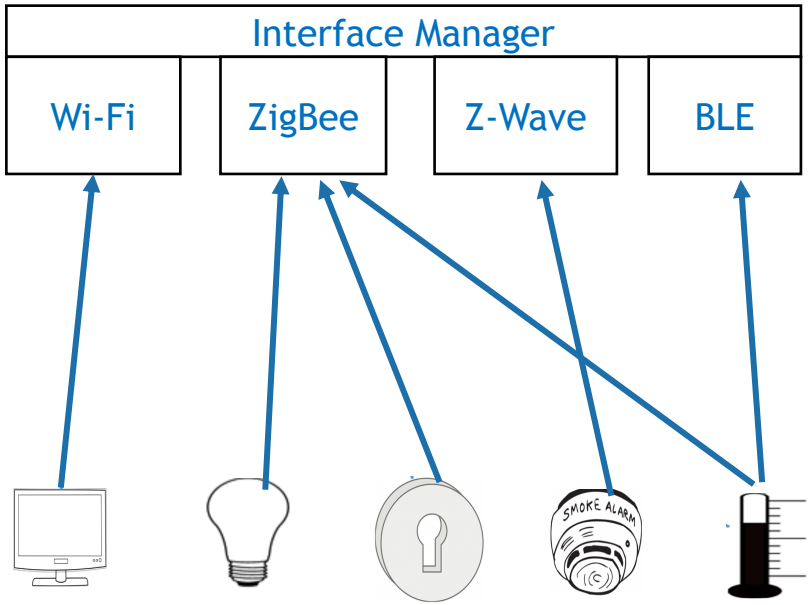
University of Houston Clear Lake

Interface Manager (IM)

- Mask heterogeneous communication channels
- Detects the type of devices and forwards message accordingly

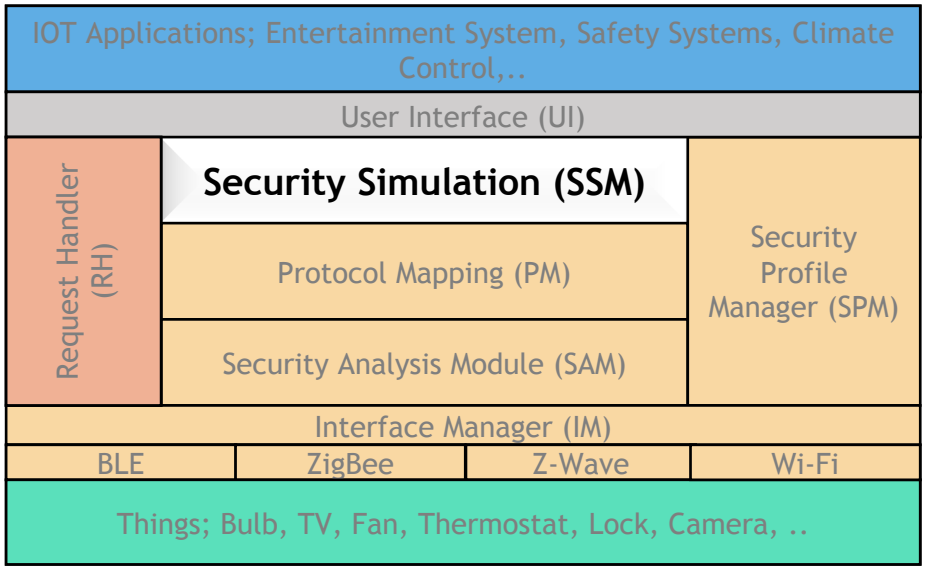


Examples of How IM Working



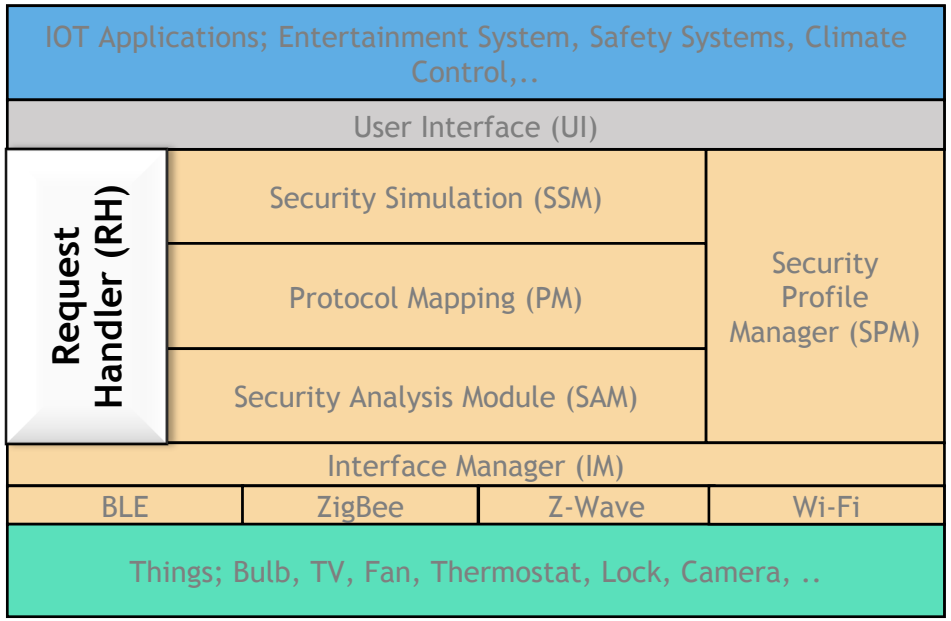
Security Simulation Module (SSM)

- Tight coupling with the physical world
- Simulates critical instructions before actually executing them on end devices



Request Handler (RH)

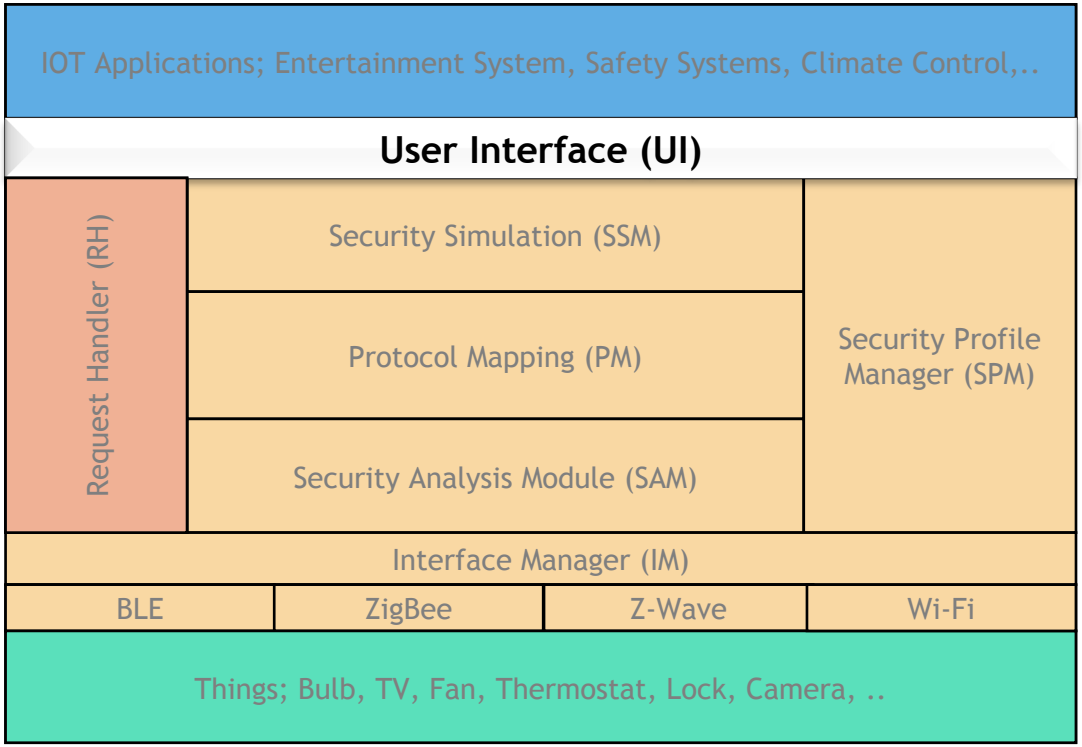
- Coordinates multiple components in EdgeSec
- Handles requests from peers within or outside of the network



User Interface (UI)

Interface for -

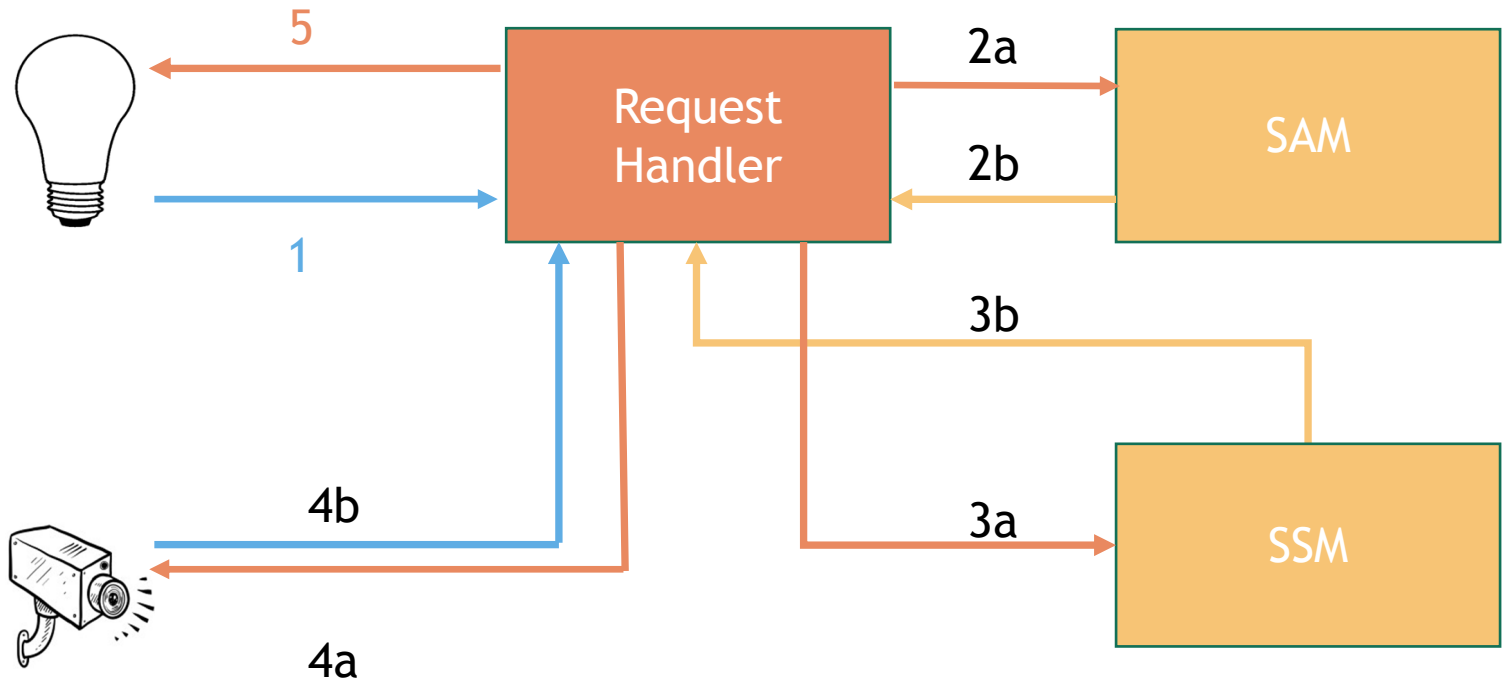
- Administrators
- SSM users
- PM libraries
- Etc..



Smart Home Case Study

Handling a local request

A smart bulb requests to access smart cameras that monitors room occupancy



Cyber Security Institute
University of Houston-Clear Lake

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Case Study II: Securely Reading Smart Device

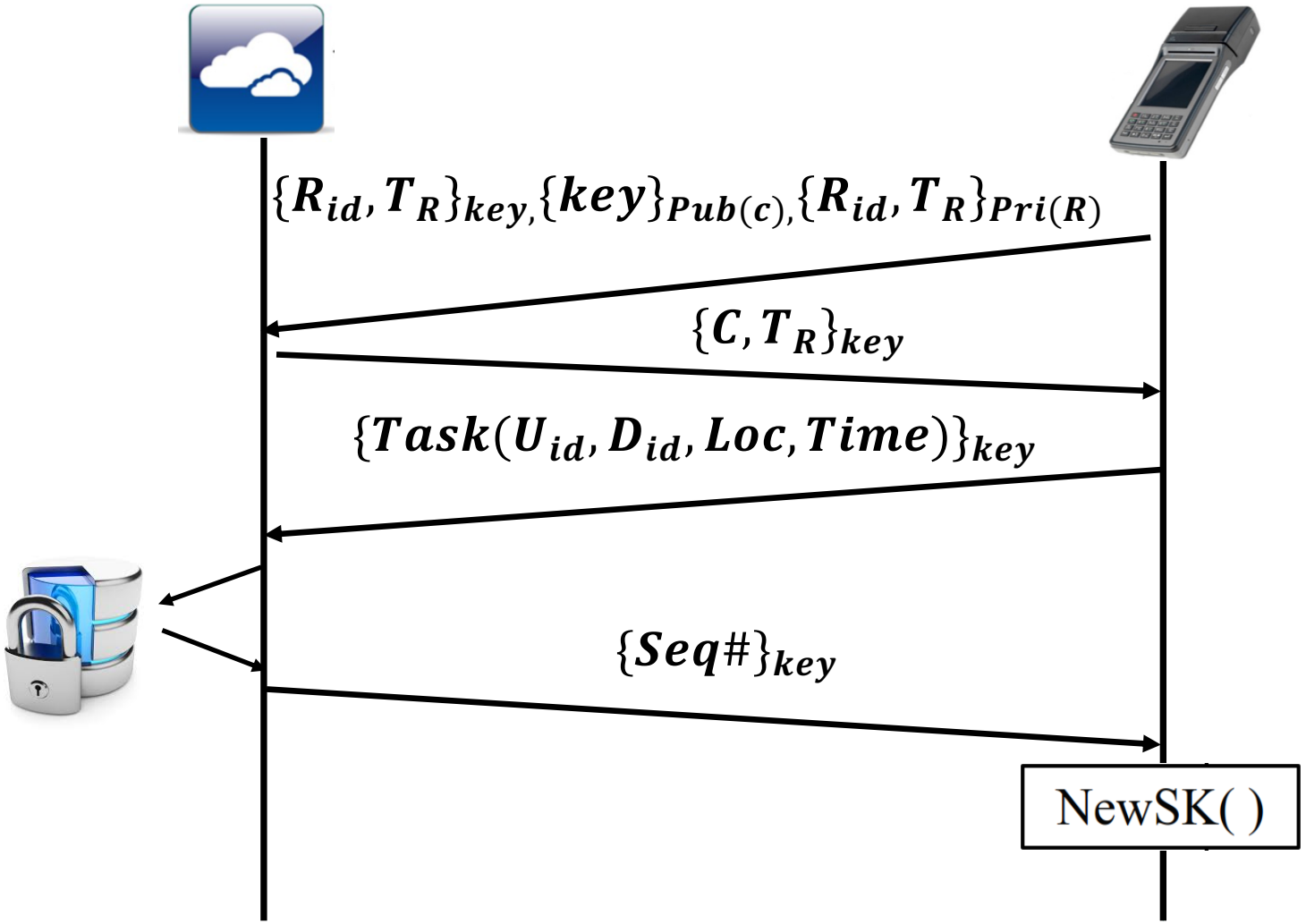
- Problem definition
  - Cloud needs to read data from smart meter (Things)
  - Security is needed to protect the sensitive data
- Challenges
  - Smart meter cannot support asymmetric encryption
  - It is hard to design scalable key distribution mechanism
  - Smart meter has limited resource to secure itself
  - Many types of attacks need to be considered

University of Houston Clear Lake

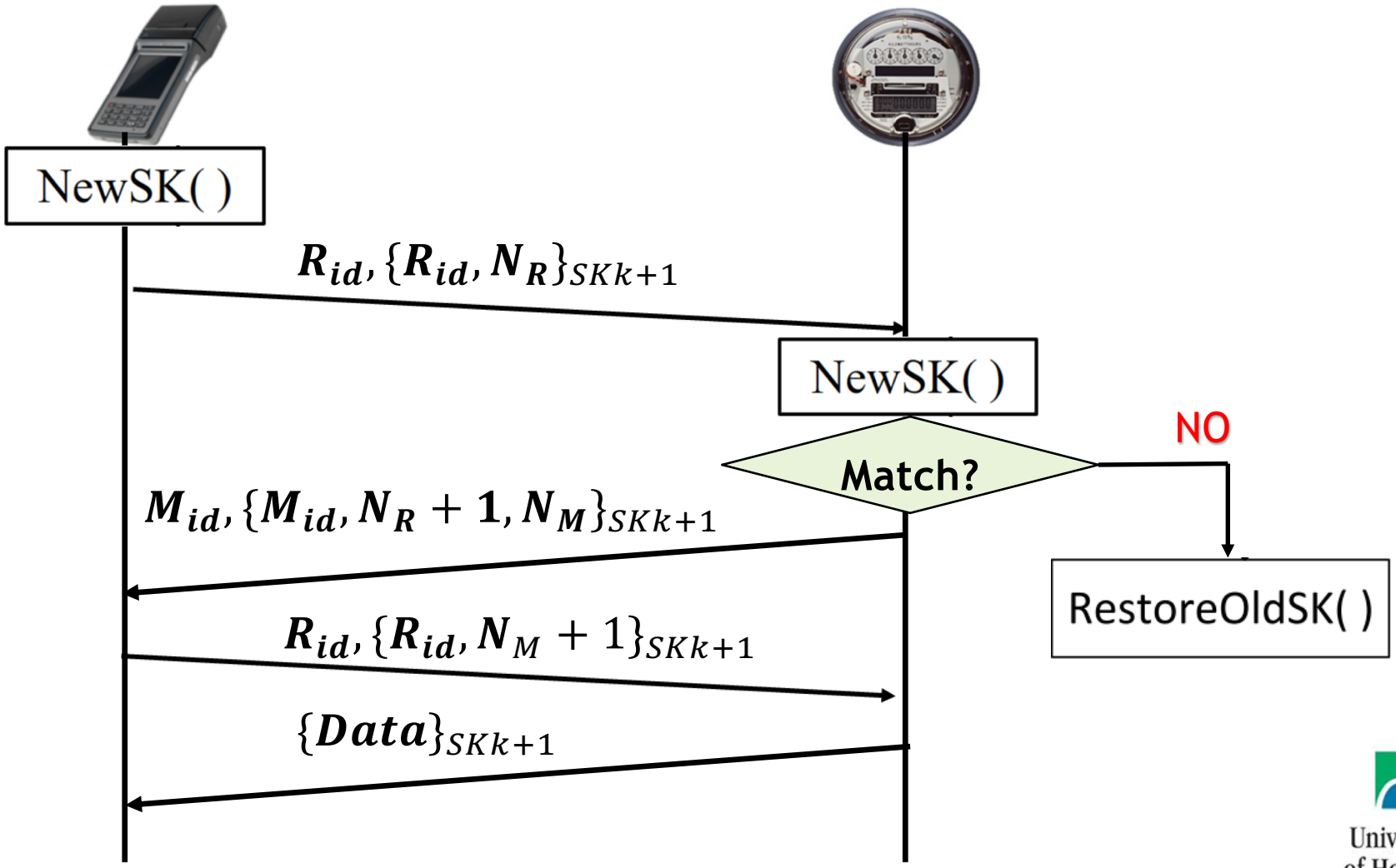
Overview of Edge Supported Authentication

- An edge supported two-phase authentication protocol
  - Smart reader is the edge device

Reader-Cloud Authentication



Reader-Device Authentication



One-time Key Generation

- NewSK()
  - NewSK = Hash(Zipcode, Timestamp, Seq#, OldSK)
    - Key_0, Key_1, Key_2,…, Key_k, Key_{k+1},…
  - Seq# = (Seq# + 1) mod MaxSeq
  - MaxSeq should be big enough
  - Key0 is from the smart grid cloud directly
  - Sequence number is initialized randomly

Cyber Security Institute
University of Houston-Clear Lake

Design Analysis

- A lightweight design
  - Light operation of Hash
  - Efficient symmetric key scheme
- Easier symmetric key distribution
  - One-time key generation
  - Unlinkability between the new and old keys
  - Wired connection based key renovation

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Security Analysis I

- Eavesdropping
  - All communications encrypted
- Brute force attack
  - Big enough MaxSeq number
  - Limited times of tries
  - Random initial sequence number
  - Location information
- Man-in-the-Middle attack
  - Asymmetric key for cloud-reader authentication
  - One-time symmetric key for read-meter authentication

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Security Analysis II

- Device attack
  - Faked reader failed to be authenticated
  - Faked reader failed to generate the one-time symmetric key
- Internal attack
  - Lost legitimate reader and malicious attack
    - Location information in authentication
    - Job verification
    - Very limited reading window
  - Legitimate reader and utility worker not assigned for the job
    - Job verification

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Security Analysis III

- Reply attack
  - One-time symmetric key
  - Timestamps and nonce
- Forward secrecy
  - One-time symmetric key as session key
  - Compromising of previous keys not compromising future keys
  - Only store the last previous key
- DoS attack
  - Mostly blocked by authentication

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Open Research Problems

- New-layer, new security risks
  - Edge device security, interface security
- Models for security states
  - Security simulation, security evaluation
- Management of secure Edge layer
  - Secure Edge node joining/leaving
- Isolation among IoT applications at Edge
- Light-weight security protocols
- Lightweight secure OS for Edge Computing
  - SeL4?

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Conclusion

- Security design is more challenging in IoT than that in traditional networks
- Edge layer provides new opportunities in security solution designs
  - EdgeSec, an Edge layer security solution for IoT security
  - An edge supported two-phase authentication protocol
- More research are needed to secure the edge layer & design edge-based security services

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Thank you!

University
of Houston
Clear Lake