Internet of Things Security

Lecture 7: Threat Modeling in IoT

Mehmoona Jabeen

Mehmoona.jabeen@au.edu.pk

Department of Cyber Security, Air University

Lecture Outlines

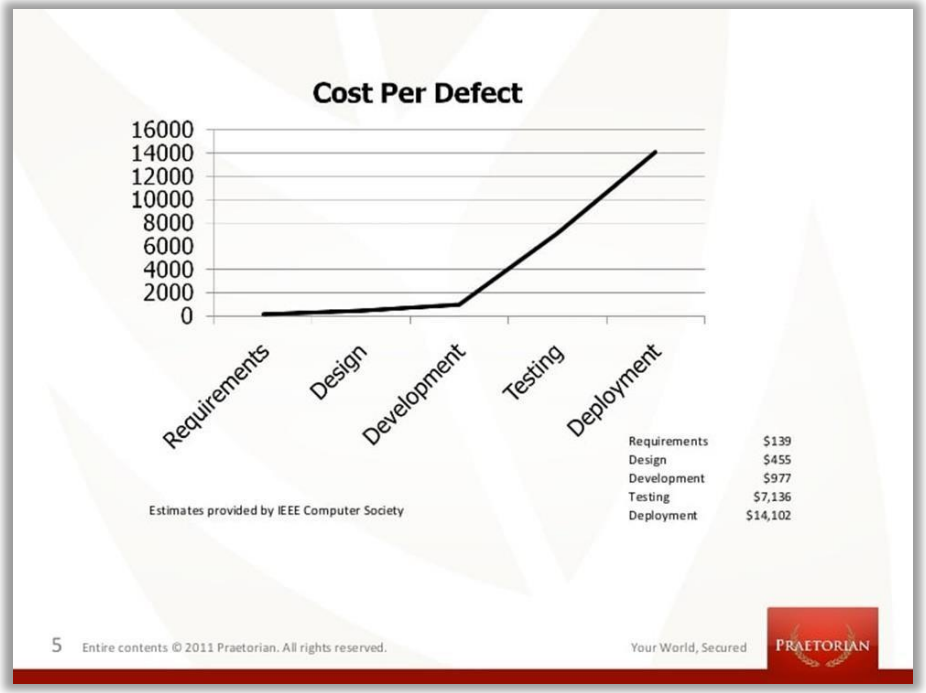
- Introduction to Threat Modeling
- How to Model Threats
- STRIDE Modeling
- Modeling Use Cases

What is Threat Modeling?

- An effective technique to help secure your systems, applications, networks, and services during the design process.
- Helps you identify potential threats and risk reduction strategies earlier in the development lifecycle.
- It is cheaper to identify vulnerabilities on the whiteboard than to fix them at the keyboard
- Uses a data-flow diagram that graphically shows how the system works.
- Applies a security framework to help you find and fix security issues.
- STRIDE-spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege
- VAST-Visual agile and simple threat modeling
- PASTA-process for attack simulation and threat analysis
- Attack Trees

Why Do We Need?

- Detect problems early in the software development life cycle (SDLC)—even before coding begins.
- Evaluate new forms of attack that you might not otherwise consider.
- Maximize testing budgets by helping target testing and code review.
- Identify security requirements (Confidentiality, Integrity, Authentication).
- Remediate problems before software release and prevent costly recoding post-deployment.
- Highlight assets, threat agents, and controls to deduce components that attackers will target.



Benefits

Improve Security

- Champions threat analysis
- Uncovers logical and architectural vulnerabilities
- Reduces risk and minimizes impact

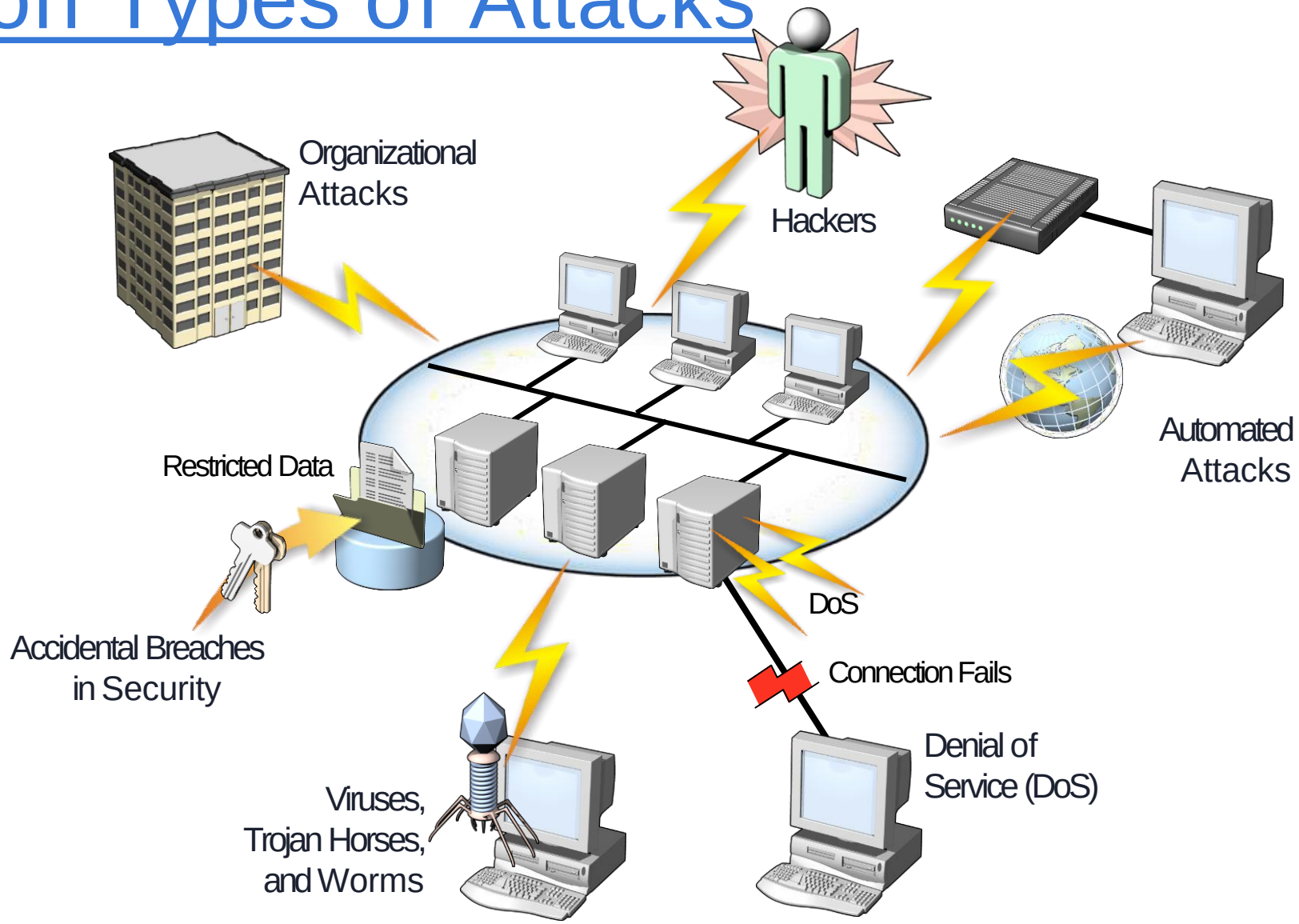
Drives Testing

- Validates design meet security requirements
- Serve as a guide for verification testing

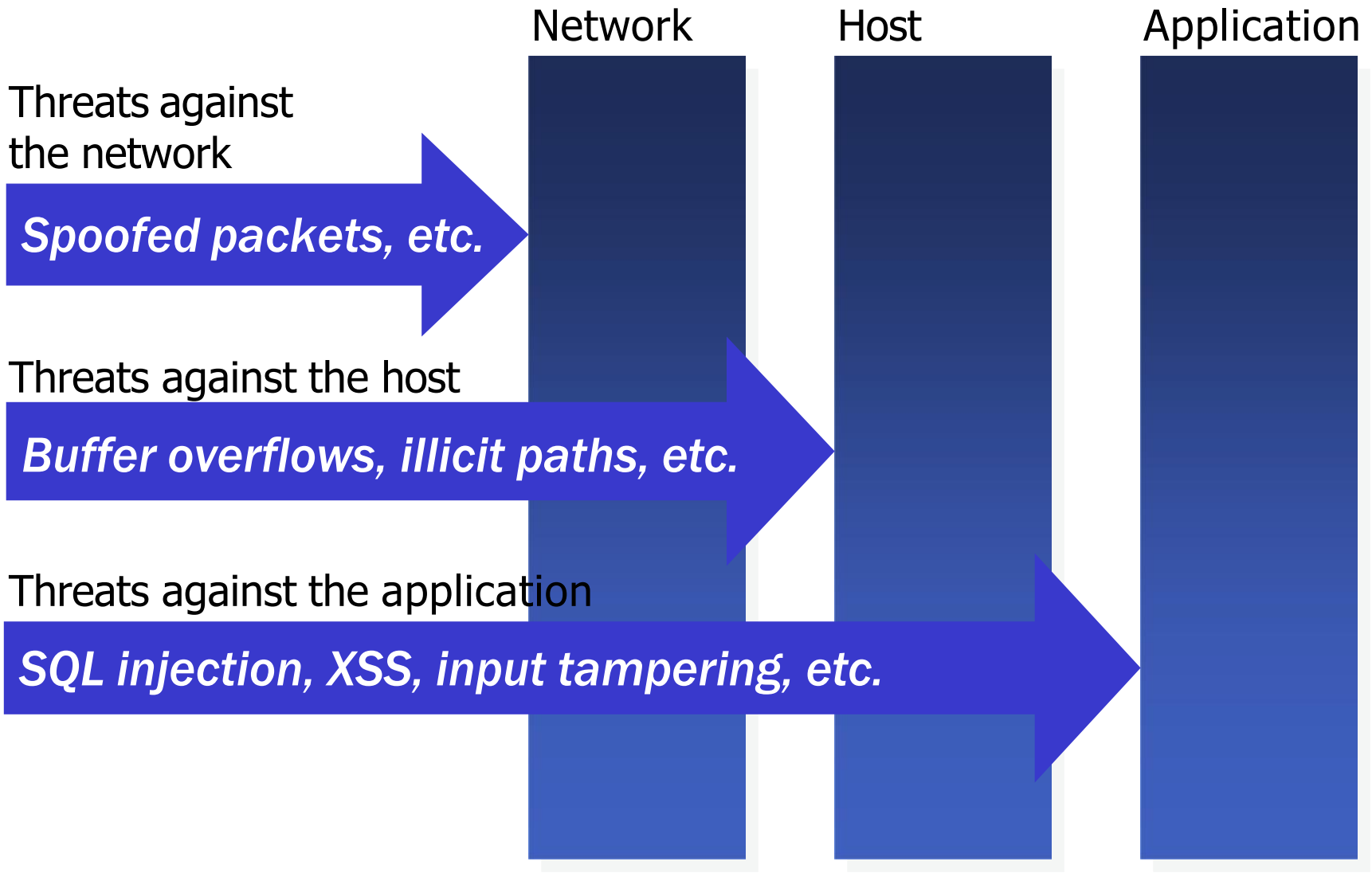
Reduces Cost

- Identifies expensive mistakes early on
- Improve understanding and structure of application
- Decrease new hire ramp up time

Common Types of Attacks



Types of Threats



Threats Against the Network

Threat	Examples
Information gathering	Port scanning
	Using trace routing to detect network topologies
	Using broadcast requests to enumerate subnet hosts
Eavesdropping	Using packet sniffers to steal passwords
Denial of service (DoS)	SYN floods
	ICMP echo request floods
	Malformed packets
Spoofing	Packets with spoofed source addresses

http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh15.asp?frame=true#c15618429_004

Threats Against the IoT Devices

Threat	Examples
Information gathering	Port scanning and trace route
	Vendor default passwords and configuration of IoT Devices
	Firmware Analysis
Eavesdropping	Using packet sniffers to steal passwords
Information Disclosure	Unencrypted Data
	No authentication
Spoofing	Packets with spoofed source addresses or device cloning

http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh15.asp?frame=true#c15618429_004

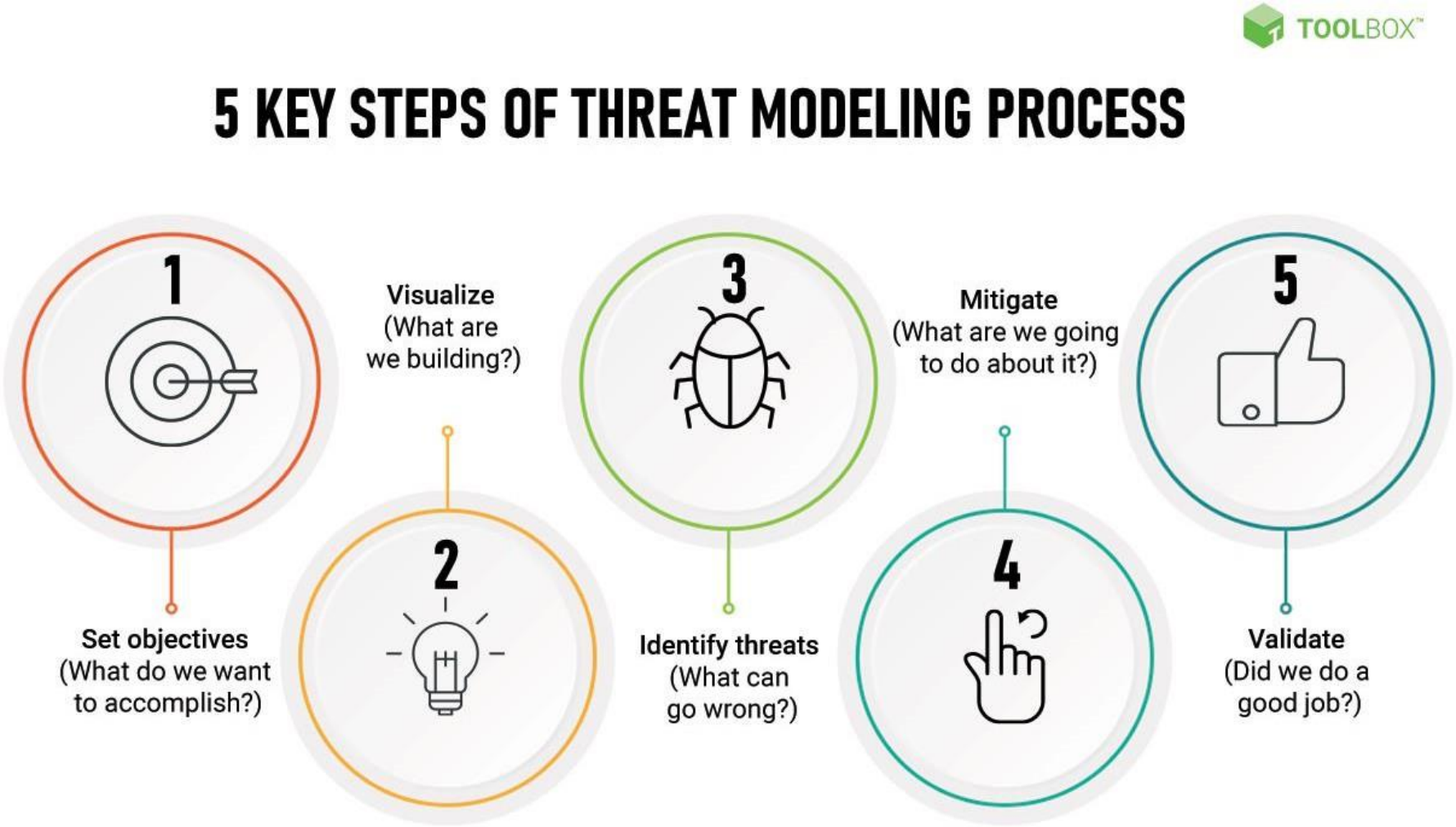
Threats Against the Hosts

Threat	Examples
Arbitrary code execution	Buffer overflows in ISAPI DLLs (e.g., MS01-033)
	Directory traversal attacks (MS00-078)
File disclosure	Malformed HTR requests (MS01-031)
	Virtualized UNC share vulnerability (MS00-019)
Denial of service (DoS)	Malformed SMTP requests (MS02-012)
	Malformed WebDAV requests (MS01-016)
	Malformed URLs (MS01-012)
	Brute-force file uploads
Unauthorized access	Resources with insufficiently restrictive ACLs
	Spoofing with stolen login credentials
Exploitation of open ports and protocols	Using NetBIOS and SMB to enumerate hosts
	Connecting remotely to SQL Server

Threats Against the Application

Threat	Examples
SQL injection	Including a DROP TABLE command in text typed into an input field
Cross-site scripting	Using malicious client-side script to steal cookies
Hidden-field tampering	Maliciously changing the value of a hidden field
Eavesdropping	Using a packet sniffer to steal passwords and cookies from traffic on unencrypted connections
Session hijacking	Using a stolen session ID cookie to access someone else's session state
Identity spoofing	Using a stolen forms authentication cookie to pose as another user
Information disclosure	Allowing client to see a stack trace when an unhandled exception occurs

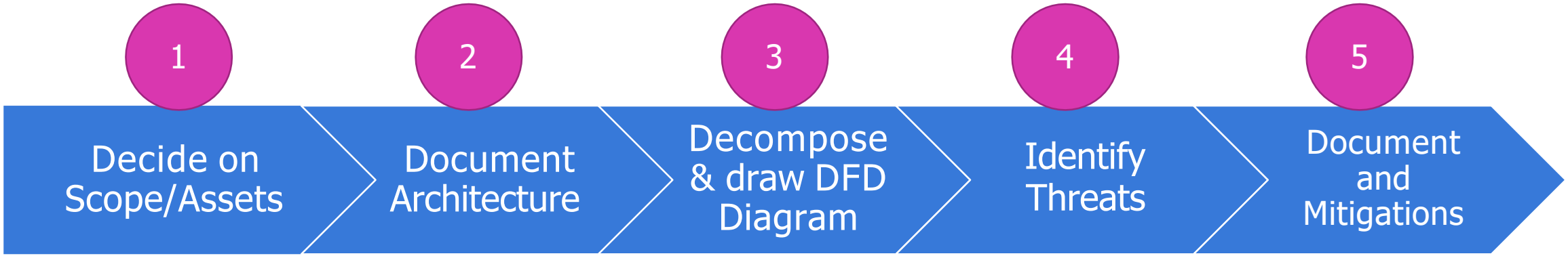
Threat Modeling Process



Modeling Approaches

- Attack Centric
  - Evaluates from the point of view of an attacker
- Defense Centric
  - Evaluates weakness in security controls
- Asset Centric
  - Evaluates from asset classification and value
- Hybrid
  - Evaluates application design using combination of methodologies to meet security objectives

High Level Threat Modeling Process



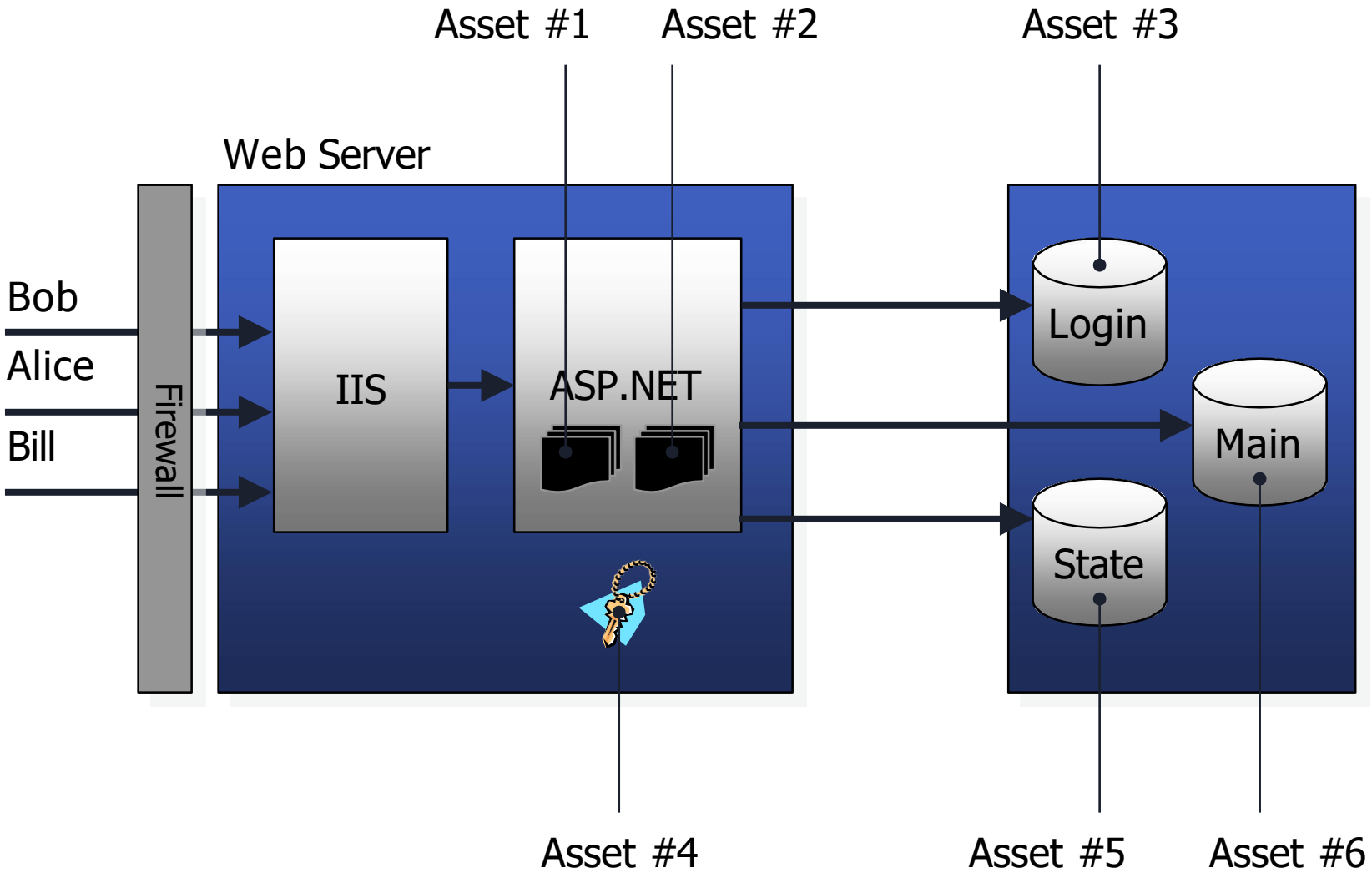
1. Identify Assets

- What is it that you want to protect?
  - Private data (e.g., customer list)
  - Proprietary data (e.g., intellectual property)
  - Potentially injurious data (e.g., credit card numbers, decryption keys)
- These also count as "assets"
  - Integrity of back-end databases
  - Integrity of the Web pages (no defacement)
  - Integrity of other machines on the network
  - Availability of the application

2. Document Architecture

- Define what the app does and how it's used
  - Users view pages with catalog items
  - Users perform searches for catalog items
  - Users add items to shopping carts
  - Users check out
- Diagram the application
  - Show subsystems
  - Show data flow
  - List assets

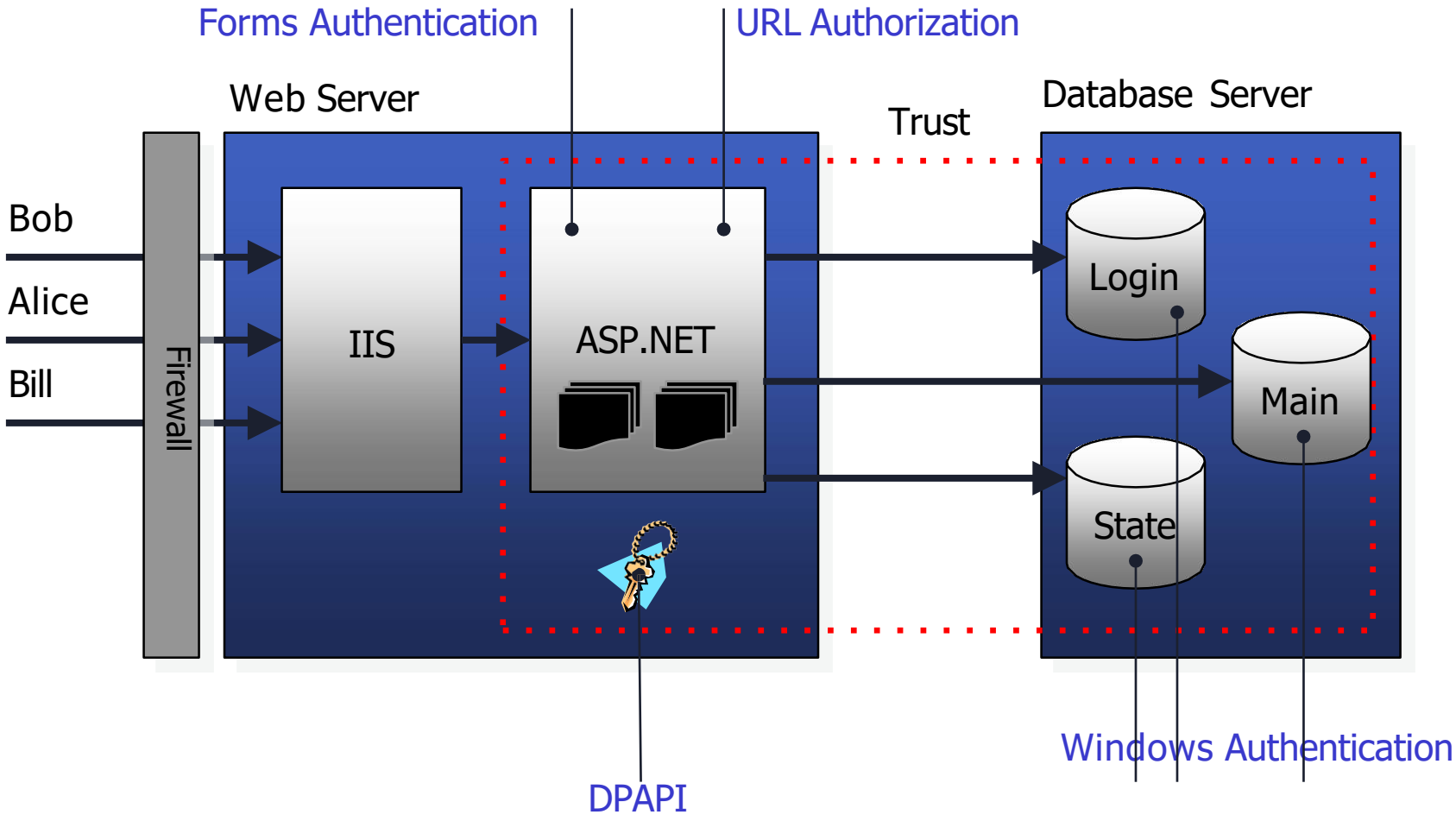
Example Assets



3. Decompose and Draw DFD

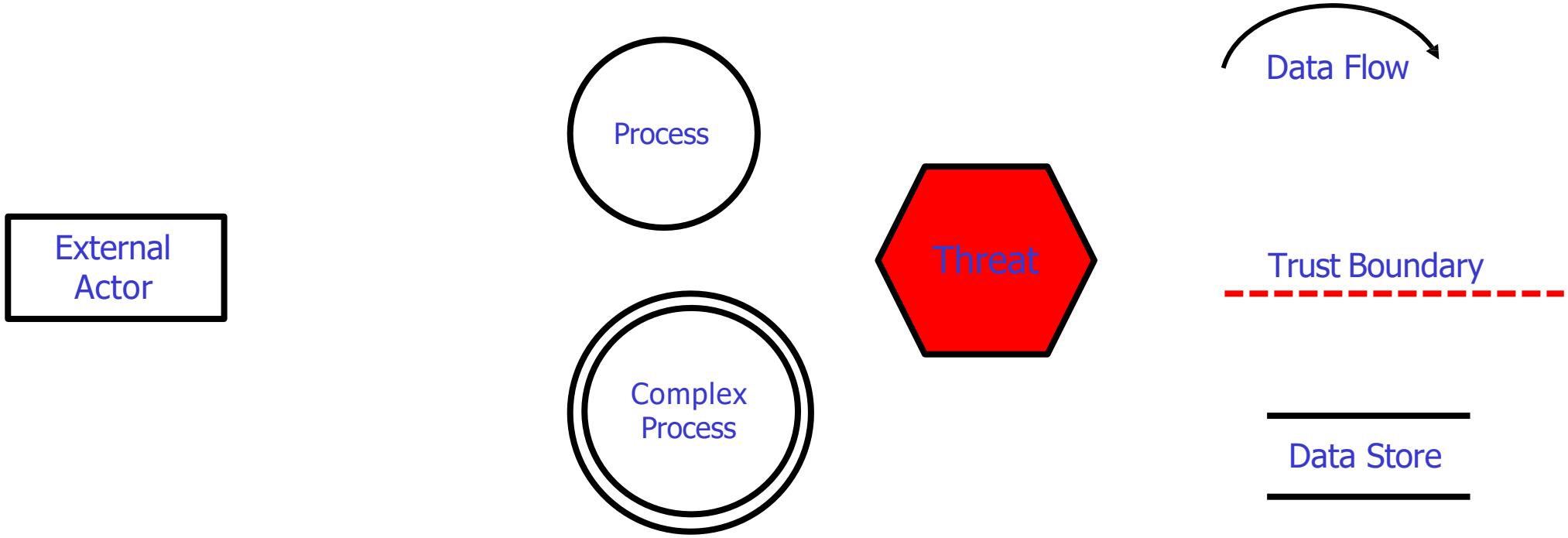
- Refine the architecture diagram
  - Show authentication mechanisms
  - Show authorization mechanisms
  - Show technologies (e.g., DPAPI)
  - Diagram trust boundaries
  - Identify entry points
- Begin to think like an attacker
  - Where are my vulnerabilities?
  - What am I going to do about them?

Example

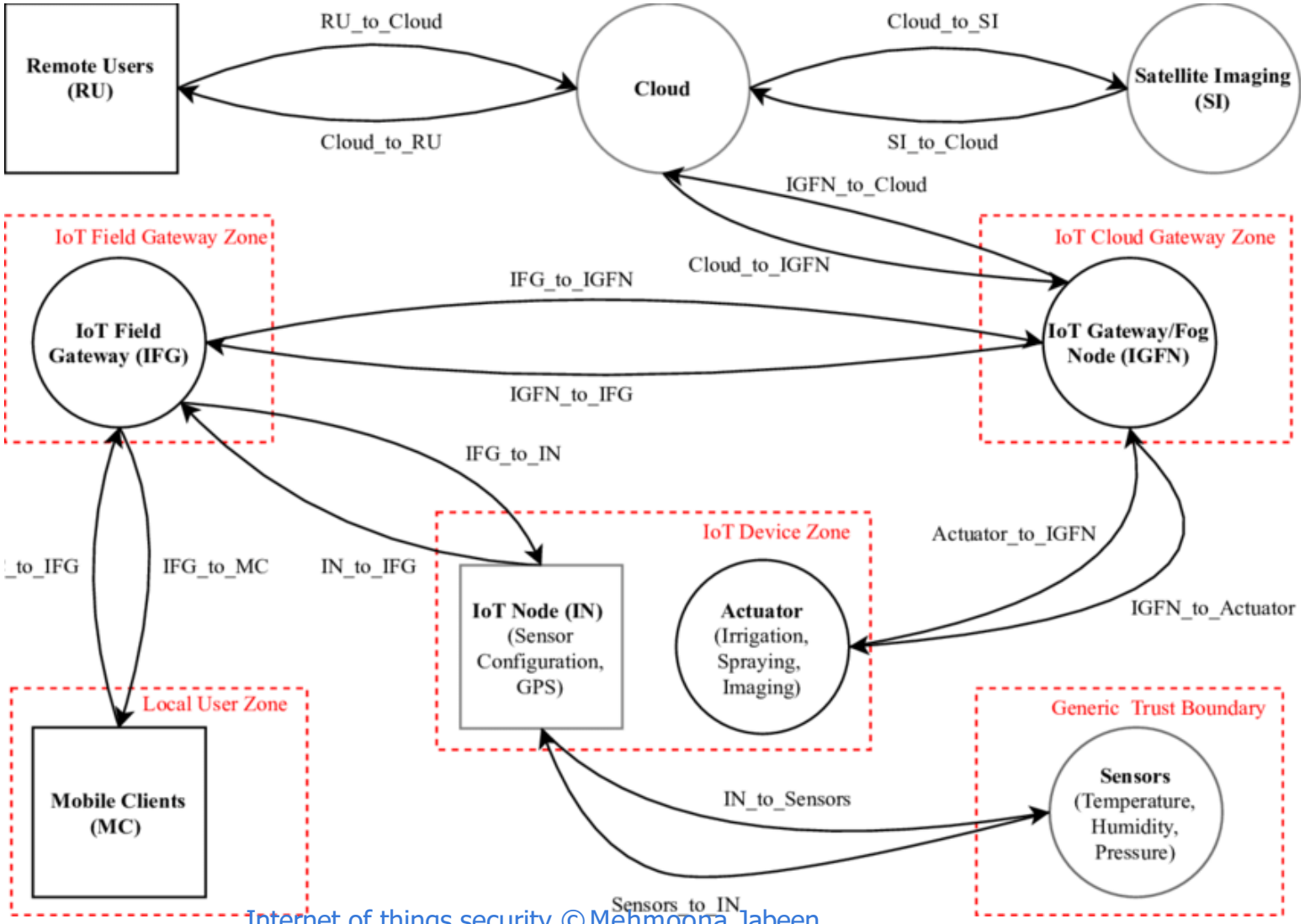

Forms Authentication
URL Authorization
Web Server
Trust
Database Server
Bob
Alice
Bill
Firewall
IIS
ASP.NET
Login
Main
State
DPAPI
Windows Authentication

Creating DFDs

- Decompose the system into a series of processes and data flows
- Explicitly identify trust boundaries



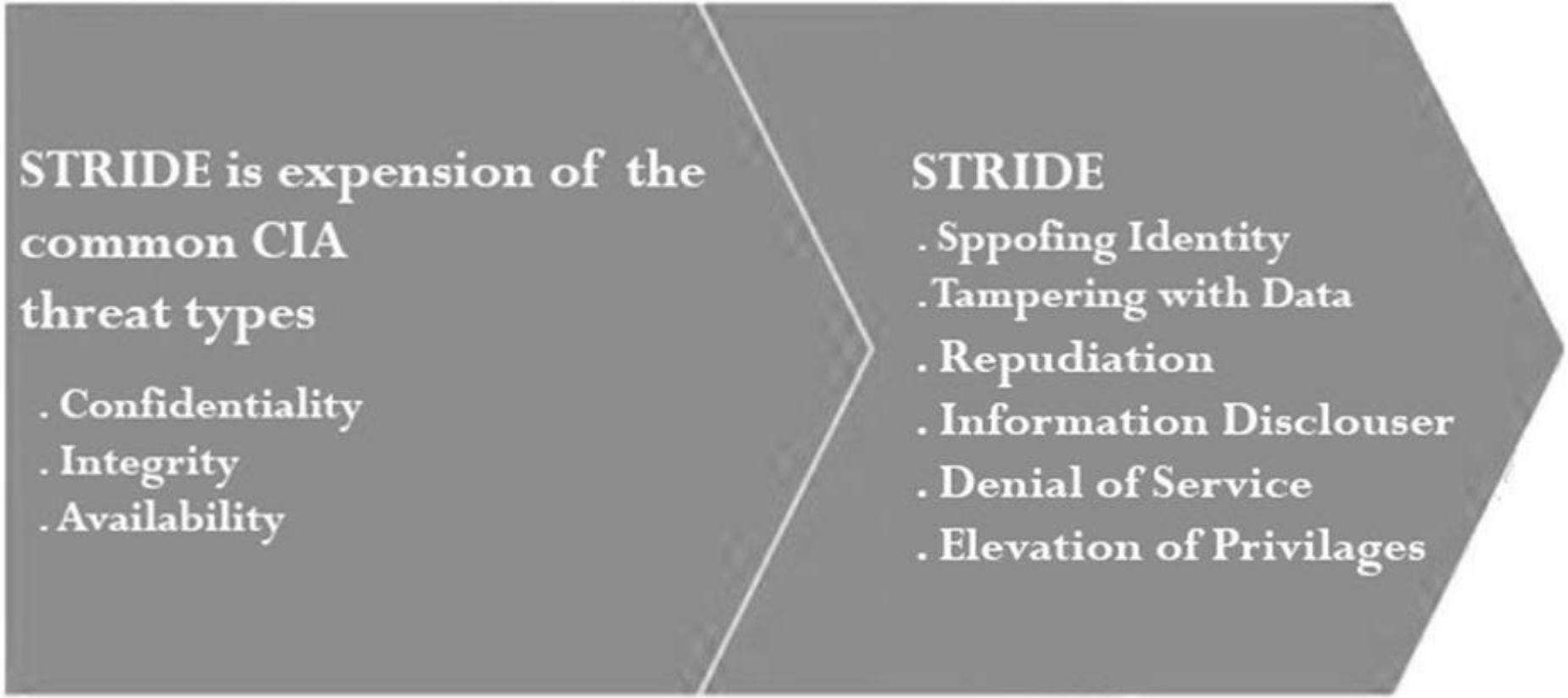
Example DFD


Remote Users (RU)
RU_to_Cloud
Cloud_to_RU
Cloud
Cloud_to_SI
SI_to_Cloud
Satellite Imaging (SI)
IGFN_to_Cloud
Cloud_to_IGFN
IoT Field Gateway Zone
IoT Field Gateway (IFG)
IFG_to_IGFN
IGFN_to_IFG
IoT Cloud Gateway Zone
IoT Gateway/Fog Node (IGFN)
IFG_to_IN
_to_IFG
IFG_to_MC
IN_to_IFG
IoT Device Zone
IoT Node (IN) (Sensor Configuration, GPS)
Actuator (Irrigation, Spraying, Imaging)
Actuator_to_IGFN
IGFN_to_Actuator
Local User Zone
Mobile Clients (MC)
Generic Trust Boundary
Sensors (Temperature, Humidity, Pressure)
IN_to_Sensors
Sensors_to_IN

4. Identify Threats

- Method #1: Threat lists
  - Start with laundry list of possible threats
  - Identify the threats that apply to your app
- Method #2: STRIDE
  - Categorized list of threat types
  - Identify threats by type/category
- Optionally draw threat trees
  - Root nodes represent attacker's goals
  - Trees help identify threat conditions

Identifying Threats from DFDs



Microsoft STRIDE Categorization

STRIDE is a model for identifying security threats, developed by Praerit Garg and Loren Kohnfelder at Microsoft.

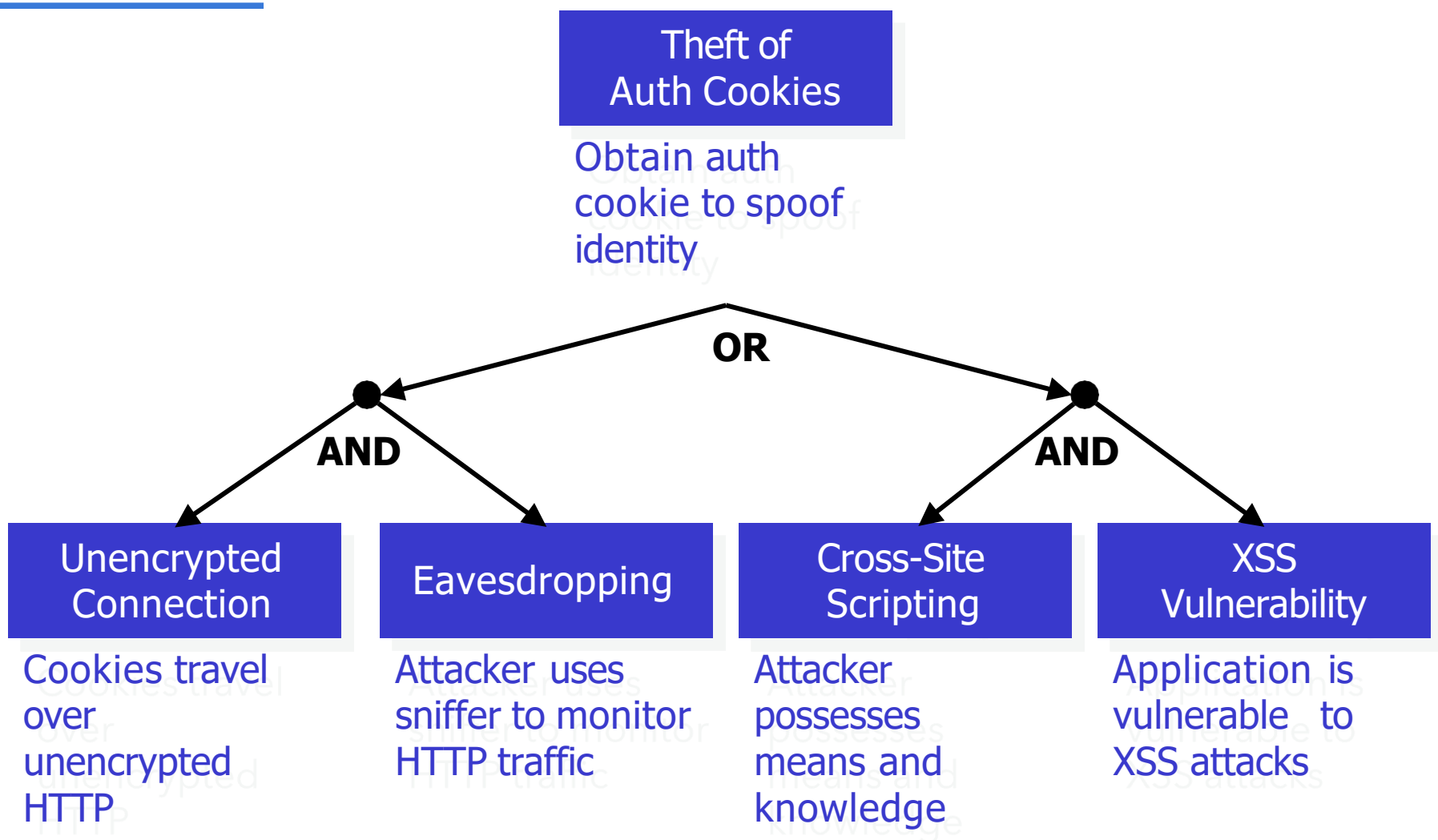
Help answer the question "what can go wrong in this system we're working on?"

Threat	Desired property	Attack Definition
Spoofing	Authenticity	Attackers pretend to be the legitimate user to gain access. E.g. Faking email address or phishing
Tampering	Integrity	Attackers pretend to be a real user to alter the data. E.g. SQL injection
Repudiation	Non-repudiability	Attacker deny any involvement in malicious activity. E.g. change logs to prevent audit process.
Information disclosure	Confidentiality	Attackers gain unauthorized access to confidential data. Verbose error message reveal DB schema
Denial of service	Availability	Attackers overload or disrupt the normal functioning of the system
Elevation of privilege	Authorization	Attackers gain access to unauthorized accounts. E.g. attacker is able to gain admin access.

DREAD Threat Assessment

- DREAD is part of a system for risk-assessing computer security threats.
- The categories are:
  - **D**amage – how bad would an attack be?
  - **R**eproducibility – how easy is it to reproduce the attack?
  - **E**xploitability – how much work is it to launch the attack?
  - **A**ffected users – how many people will be impacted?
  - **D**iscoverability – how easy is it to discover the threat?
- Each category is given rating from 1 to 10.
- It was abandoned when discovered that the ratings are not very consistent and are subject to debate and discontinued at Microsoft by 2008

Threat Trees



Microsoft Threat Modeling Tool

- MTM uses STRIDE by default
- Draws the system in the form of Data Flow Diagram (DFD)
- You can design a new system template
- Design an MTM template
- Define Threats
- Define Threat Mitigations
- Draw data flow diagram
- Generate threat report

Countermeasures

- Do nothing
- Remove the feature
- Turn off the feature
- Warn the user
- Counter the threat with operations
- Accountability
- Separation of duties
- Counter the threats with technology
- Change in design
- Change in implementation

Threat Models to Scope Assessment

- IoT systems have many different parts and kinds of parts
- Web applications, web services, custom hardware, esoteric protocols
- Creating a test plan can be challenging –you will never have the resources to be exhaustive
- Threat modeling can help drive decision about trade-offs
- Should we fuzz-test the device Zig by stack or run SAST on the web services
- Safety Concerns
  - Confidentiality, Integrity, and Availability
  - Everywhere else: Confidentiality breaches of regulated information
  - IoT (especially industrial): Integrity or availability breaches impacting the kinetic environment

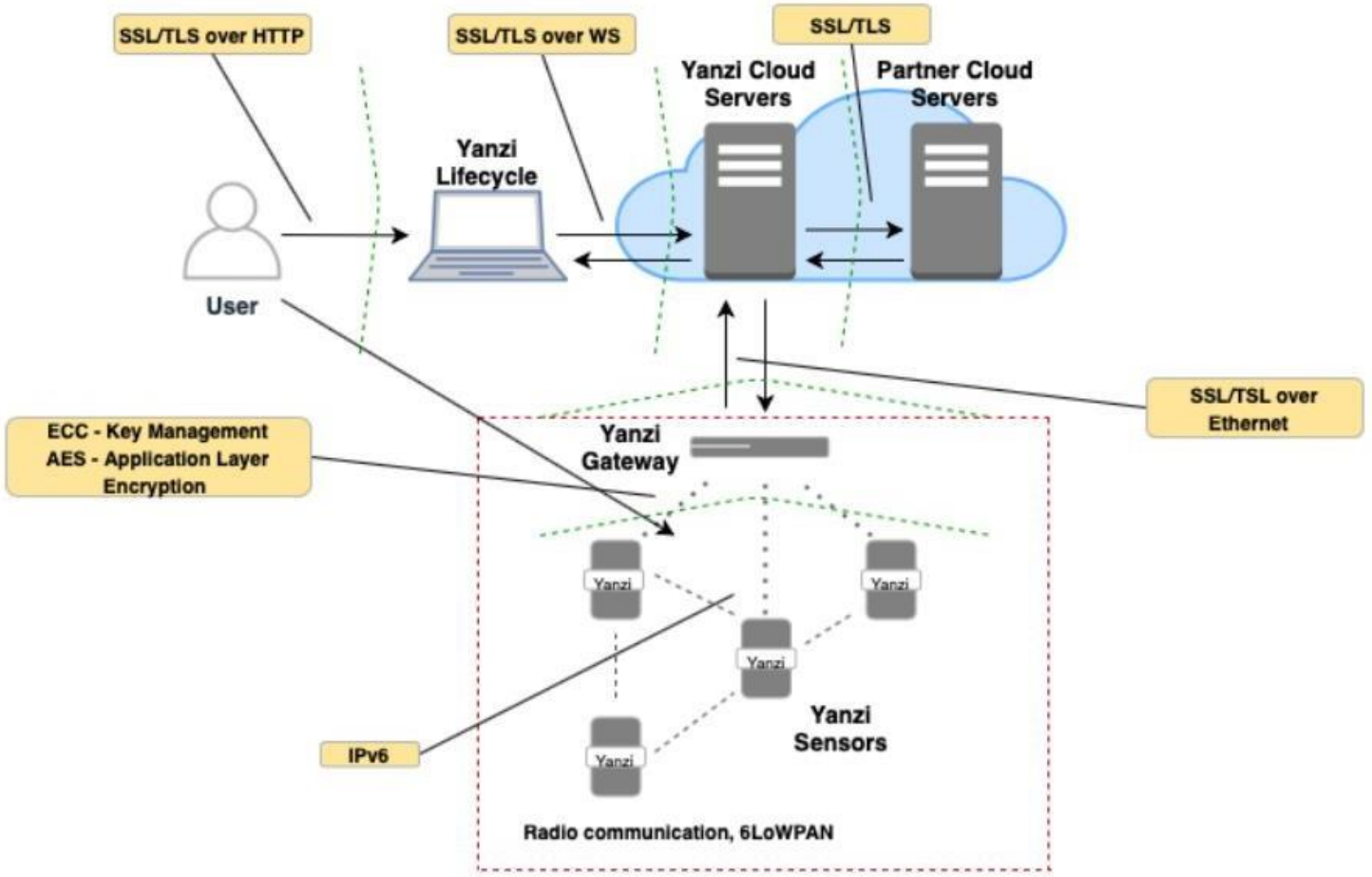
Threat Modeling for Yanzi IoT System

- The IoT platform delivered by Yanzi Networks is a fast, all IP and end-to-end solution, consisting of gateways, sensors and a cloud platform named Cirrus1 .
- The application functions as a management tool for gateways/access points and sensors in smart buildings, and is provided to real estate owners and facility management companies who wish to enter the smart building industry.

Components

- It consists the following components:
  - Yanzi Cirrus Software as a Service
  - Gateways
  - Sensors
  - Access Points
  - ECC Key Management
  - AES Application-layer Encryption
  - SSL Client/ Server Certificates
  - Yanzi Lifecycle (Cirrus is bundled into a SaaS solution)
  - Yanzi Cloud Servers
  - Partner Cloud Servers
  - Networks (WAN, LAN), IPS (IPV4, IPV6)

Architecture Overview of Yanzi



1. Information Gathering

- Before any threat modeling and testing was conducted, essential information such as the precise frequency used for communication and the protocol
- Used for communication needed to be identified.
- There are 16 channels available for the 802.15.4 protocol, and it was, therefore, necessary to find out which of the channels that is utilized.
- At first, the GQRX spectrum analyzer and the HackRF were used in an attempt to find a peak rising higher above the other peaks, e.g when moving a sensor closer to the HackRF.
- Frequency band and channel can be found in the Yanzi lifecycle tool, under Network topology and the 2D map section, by clicking on one of the sensors for information. ”Channel 2.1.11” is displayed, where 2.1 corresponds to the 2.4 GHz frequency band and 11 the 802.15.4 channel utilized in that band.
- Yanzi IoT states that IPv6 and IEEE 802.14.5 are used, which indicates that the 6LoWPAN protocol and an adaption layer are present.

2. Identified Assets

All assets that are considered as interesting to protect were identified in this step. It was concluded that five assets could be probable targets for an attacker, and each one is described in the following table

Asset	Description
Yanzi Gateway	The device has two Ethernet ports, whereas solely one is in use, and the device, therefore, connects to the local network through an Ethernet cable.
Yanzi Sensors	Each sensor contains several smaller sensors that measure temperature, motion etc. depending on the model of the sensor.
Web application	The Yanzi cloud SaaS platform, where live data sent by the gateway can be viewed by a user. To enable this, the user is required to have a separate username and password and to be a member of a group that has access to a location associated with sensors and gateway.
Radio communication	All traffic between sensors and gateway is transmitted over radio communication.
Firmware	Yanzi Stamp firmware that includes automatic channel selection, automatic security setup, automatic over-the-air update etc.

3. Identified Technologies

After the creation of the architecture diagram, the different technologies that are utilized were identified, examined, and documented in the table, with the purpose to further analyze and later identify possible threats.

Technology	Details
Yanzi Sensors	2.4 GHz, 5-25 m range, 50-100 m line of sight
Yanzi Gateway	Embedded Raspberry Pi, 2.4 GHz, communicates over Ethernet
Firmware: Yanzi Stamp	Firmware for sensor updates, security setup, automatic discovery etc
Communication protocol: HTTPS	Encrypted communication when user access the web application through the web browser
Communication protocol:6LoWPAN (802.15.4)	RF protocol for communication between gateway and sensors
Communication protocol: IPv6	Network protocol for data delivery between sensors and gateway
Communication protocol: WSS	Encrypted communication between web application and Yanzi cloud servers
Communication protocol: Ethernet	Encrypted communication between gateway and servers
Encryption: AES	Encryption on the application layer
Encryption: SSL/TSL	Encryption over several various protocols
Encryption: ECC	Key management between sensors and gateway

Decomposition of the IoT Devices

- With the architectural diagram in mind, a decomposition of the IoT was performed, where entry points, data flow and trust boundaries were identified.
- One of the identified entry points in the Yanzi IoT is the web application, where a user can view live data and control connected devices, which solely require login credentials.
- Another entry point is the gateway itself, since it is connected to the internet and might have ports open that can be exploited.
- The third entry point is the wireless communication between sensors and gateway, which however is protected by AES encryption, and can therefore be difficult to attack.
- The last identified entry point is the Yanzi Stomp firmware, which controls several critical aspects of the product, and can therefore be misused if it falls into the wrong hands.

4. Identified Threats

- Threats were therefore only identified based on the included entry point. Threats are identified with both the OWASP top ten list for IoTs and listed IoT weaknesses presented in PATRIoT:
- A systematic and agile IoT Pen testing Process. Identified threats for radio communication according to the STRIDE model
- Spoofing
  - Spoofing one of the sensors through the RF communication
  - Spoofing the gateway through the RF communication
- Tampering
  - Capturing and manipulating data packets in transit
  - Replaying signals that transit between sensors and gateway to alter live values in the cloud

- Information Disclosure
  - Eavesdropping/sniffing on the RF communication to uncover if data is encrypted or not. If data is sent in plain text, sensitive information can be extracted.
  - Reverse engineering (decoding) the RF protocol to uncover sensitive information
  - Open ports on the gateway that can result in an extracting of firmware and/or other sensitive information that might be stored
- Denial of Service
- Jamming or blocking of RF signals in transit

5. Documented Threats

Threat Description	Target	Attack Technique	Countermeasure
Attacker obtains keys used for authentication and used to impersonate a sensor/gateway	Traffic, sensor gateway	Attacker can sniff/eavesdrop on traffic and then analyze in wireshark	Encrypt all traffic
Attacker modifies either data payload or headers e.g. sequence number	Packets in transmission	Attacker can perform MITM attack or simply replay the altered packets	Message Digest Code or checksum
Attacker can decode signal data and obtain valuable information	Wireless Signals	Attackers can reverse engineer RF signal by use of URH to get meaningful bits and decode to find useful information	Use standard encryption algorithms on whole packet in wireless transmission

Smart Home Use Case

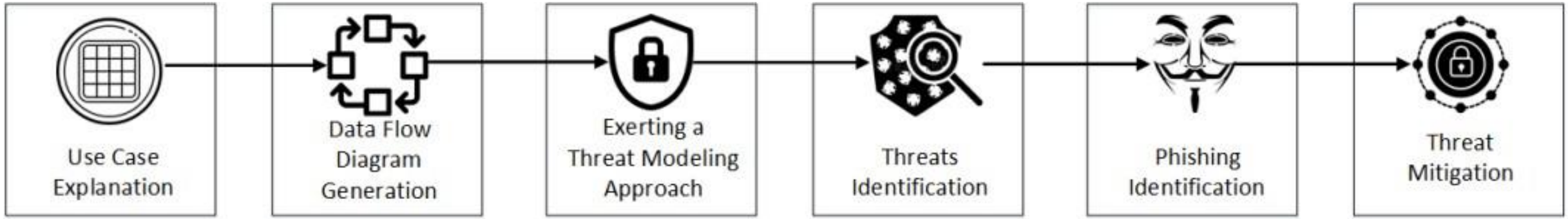
- In smart home use-case, the IoT devices are controlled via the Azure server through the IoT field gateway.
- To better understand this, we divided the smart home use-case into five zones, i.e.,
  - IoT device zone,
  - IoT field gateway zone,
  - IoT cloud gateway zone,
  - Azure zone
  - Consumer zone.
- The IoT device zone contains all the IoT sensors and actuators, which obtain different sensing values from the environment and are operated using the actuators

Use Case Zones

- IoT Device Zone
  - IoT device zone contains all the IoT sensors and actuators, which obtain different sensing values from the environment and are operated using the actuators.
- IoT Field Gateway Zone
  - IoT filed gateway zone is directly connected to the IoT end-devices, and it operates by controlling the data flow to or from the devices.
- IoT Cloud Gateway Zone
  - This zone provides a remote communication medium to the IoT devices, so that they can remotely communicate with the Azure zone through the IoT field gateway.
- Azure Zone
  - This Azure zone consists of Microsoft Azure server and Azure components such as Azure stream analytics, Azure IoT Hub, and Azure storage. Azure stream analytics is an engine that enables simulations of real-time analytics on data streams of various sources, such as the internet, sensors, actuators, and devices.
- Consumer zone
  - This is the client zone from which the user can control or analyze the IoT devices.

Threat Modeling in Smart Home

- The activity consists of six major stages, as shown in below Figure.
- These stages include use-case reconnaissance, data-flow-diagram generation, exerting a threat-modelling approach, threat identification, phishing threat identification, and threat mitigation.



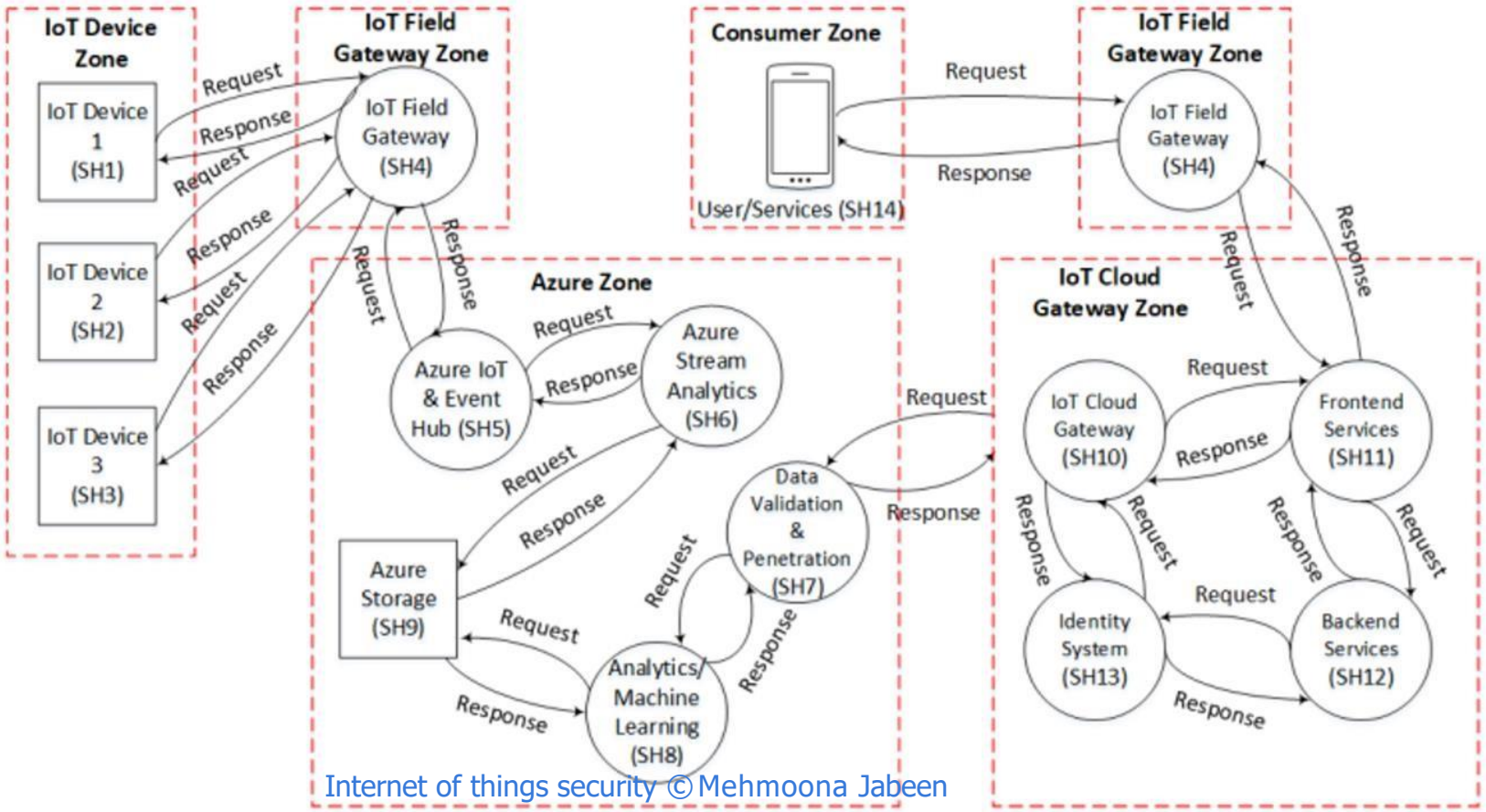
1. Information Gathering

Use-case reconnaissance is a preliminary step in the proposed threat modelling approach, in which we gather information in all different zones.

Smart Autonomous Vehicular System	
Assets	**Ids**
Sensor Zone	
OBD-II, Engine ECU, Brake ECU, Camera, Radar, LiDAR, Sensor Fusion ECU, Vehicle ECU, LKA ECU, ACC ECU	AV1, AV2, AV3, AV4, AV5, AV6, A7, AV8, AV9, AV10
Cloud Zone	
Gateway, TCU, GPS Receiver, V2X DSRC	AV11, AV12, AV13, AV14
Consumer Zone	
User/Laptop, IVI System, USB, Bluetooth	AV15, AV16, AV17, AV18
Smart Home System	
Assets	**Ids**
IoT Device Zone	
IoT Device 1, IoT Device 2, IoT Device 3	SH1, SH2, SH3
IoT Field Gateway Zone	
IoT Field Gateway	SH4
IoT Cloud Gateway Zone	
IoT Cloud Gateway, Frontend Services, Backend Services, Identity System	SH10, SH11, SH12, SH13
Azure Zone	
Azure IoT & Event Hub, Azure Stream Analytics, Data Validation & Penetration, Analytics/Machine Learning, Azure Storage	SH5, SH6, SH7, SH8, SH9
Consumer Zone	
User/Service	SH14

DFD Generation

After the use-case reconnaissance, the next step is to generate the data flow diagram (DFD) of the use-case, as illustrated in below Figure. Based on the information gathered in use-case reconnaissance.



Exerting a Threat Modelling Approach

Once the DFD of an underlying use case is designed, the next step is to exert a STRIDE threat-modelling approach on both smart use-cases. The Figure below presents a mapping of each STRIDE threat with the corresponding security measures.

STRIDE Threat	Descriptions	Security Violation
Spoofing	Misleading a user or system by illegally accessing authentication information	Authentication
Tampering	Maliciously modifying the original information by accessing it without permission	Integrity
Repudiation	Denying the user's privileged access by performing malicious actions	Non-repudiation
Information Disclosure	Exposing the sensitive information of the user without permission	Confidentiality
Denial of Service	Denying the network or services access to the valid user	Availability
Elevation of Privilege	Gaining the privileged resources without the user's permission, to compromise the system	Authorization

4. Threat Identification

As we applied the STRIDE threat-modelling technique in MTM tool, it generated a threat report of each component of a given DFD. Afterwards, we listed all the threats separately in the results Section. The listed threats show how the components can be compromised by a specific threat in the below Figure.

STRIDE	Descriptions	AV Assets	SH Assets	CIA
Spoofing	An adversary can exploit the authentication by performing malicious actions	AV1, AV2, AV3, AV4, AV5, AV6, AV7, AV8, AV9, AV10, AV11, AV13	SH1, SH2, SH3, SH4, SH5, SH6, SH7, SH8, SH9, SH10	Authentication
Tampering	An adversary can steal the stored data and change it accordingly	AV2, AV3, AV7, AV8, AV12, AV14	SH1, SH2, SH3, SH4, SH5, SH9, SH11, SH12, SH13	Integrity
Repudiation	An adversary can gain privileged access	AV11, AV16, AV17, AV18	SH1, SH2, SH3, SH4, SH5, SH6, SH9, SH14,	Non-repudiation
Information Disclosure	An adversary can disclose the sensitive information by taking control over the communication medium	AV1, AV2, AV3, AV7, AV8, AV9, AV10, AV11, AV12, AV13, AV14, AV15, AV16	SH1, SH2, SH3, SH4, SH5, SH6, SH7, SH8, SH9, SH14	Confidentiality
Denial of Service	An adversary can deny the authorized users access	AV1, AV2, AV3, AV7, AV8, AV9, AV10, AV11, AV12, AV13, AV14, AV15, AV16	SH1, SH2, SH3, SH4, SH5, SH6, SH7, SH8, SH9, SH10, SH11, SH12, SH14	Availability
Elevation of Privilege	An adversary can avail the privileged resources	AV1, AV2, AV3, AV7, AV8, AV9, AV10, AV11, AV12, AV14, AV15, AV16, AV18	SH1, SH2, SH3, SH5, SH6, SH7, SH8, SH9, SH10, SH11, SH12, SH14	Authorization

Phishing Threats in Smart Home Use Case

- We analyze all the threats in the smart home use-cases reported in the threat identification stage to figure out which of the identified threats can lead to phishing attacks.
  - Phishing in IoT Device Zone
  - Phishing in IoT Field Gateway Zone
  - Phishing in Cloud and Azure Zone
  - Phishing in Consumer Zone

5. Threat Mitigation

- Threat Mitigation for Smart Home Use Case
- The devices should be authenticated with transport layer security (TLS)
- Tampering and repudiation in IoT devices, such as exploitation of the vulnerabilities in unpatched devices, can be mitigated by enabling the proper device firmware updates.
- DoS threats can be mitigated by limiting access to unused services and open ports.

Readings

1. Md. Rashid Al Asif et. al., STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems, 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2021
2. Microsoft Threat Modeling Tool, https://www.microsoft.com/en-us/download/details.aspx?id=49168