

Lesson 3

Security Requirements and Threat Analysis Tools

A set of three architectural views

- functional view (FV), information view, and deployment and operational view.
- F. Carrez and co-workers functional view
- Security, a functional group (FG) of the FV.
- FG for security consists of security functions between the application and device.

Security FG Five Sets Of Functional Components (FCs)

- Required for FCs ensuring security and privacy

1. Identity management (IdM)

2. Authentications

3. Authorisation

4. Key exchange and management

5. Trust and reputation

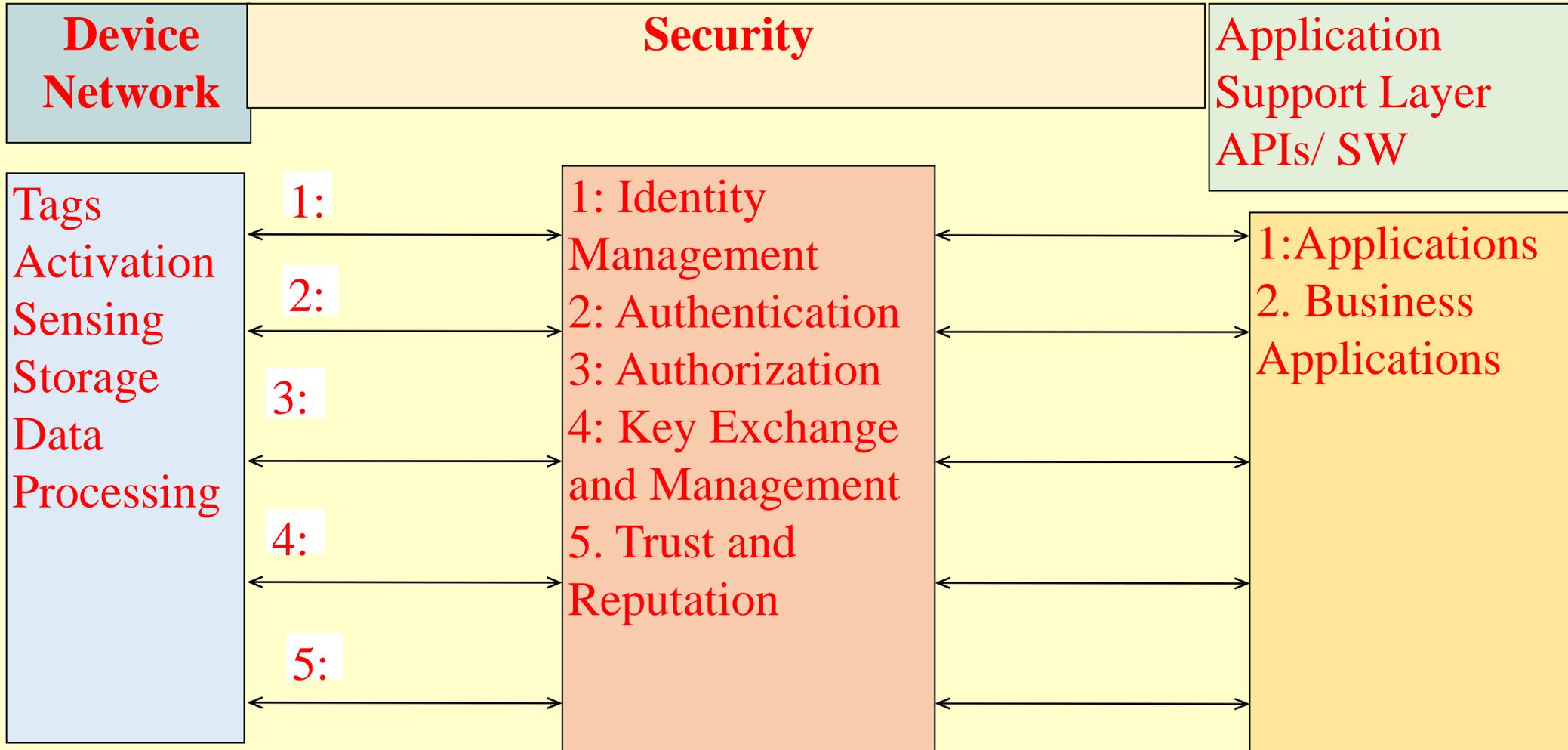


Fig. 10.1 Security Function Group Components in IoT reference architecture

Threat Analysis

- Threat analysis means uncovering the security design flaws after specifying the *stride* category, data flow diagram, elements between that the interactions occur during the stride, processes which are activated for analysis.

Stride

- Means a regular or steady course, pace
- Means, passing over or across in one long step
- Set of statements when considering a threat to a software component

Threat Analysis Tool

- First generates the threats and analyses a system for threat(s).
- A model is designed for the threat analysis with definitions of the strides and elements first.
- The interacting elements are processes, data store, flow, boundary or may be external specified elements in the system.

Threat Analysis Tool Three Components

1. Getting started guide
 2. Create a model,
 3. Open a model.
- ‘Create a model’ is used after ‘Getting started guide’.
 - The tool component ‘open the model’ precedes the threat analysis for each Stride.

Threat Analysis Tool

- Tool also provisions for definitions of new threats using a stride category.
- A stride category first created
- Generates list of threats which are active based on interactions between the elements.
- The list is as per the definitions in the model open for analysis.

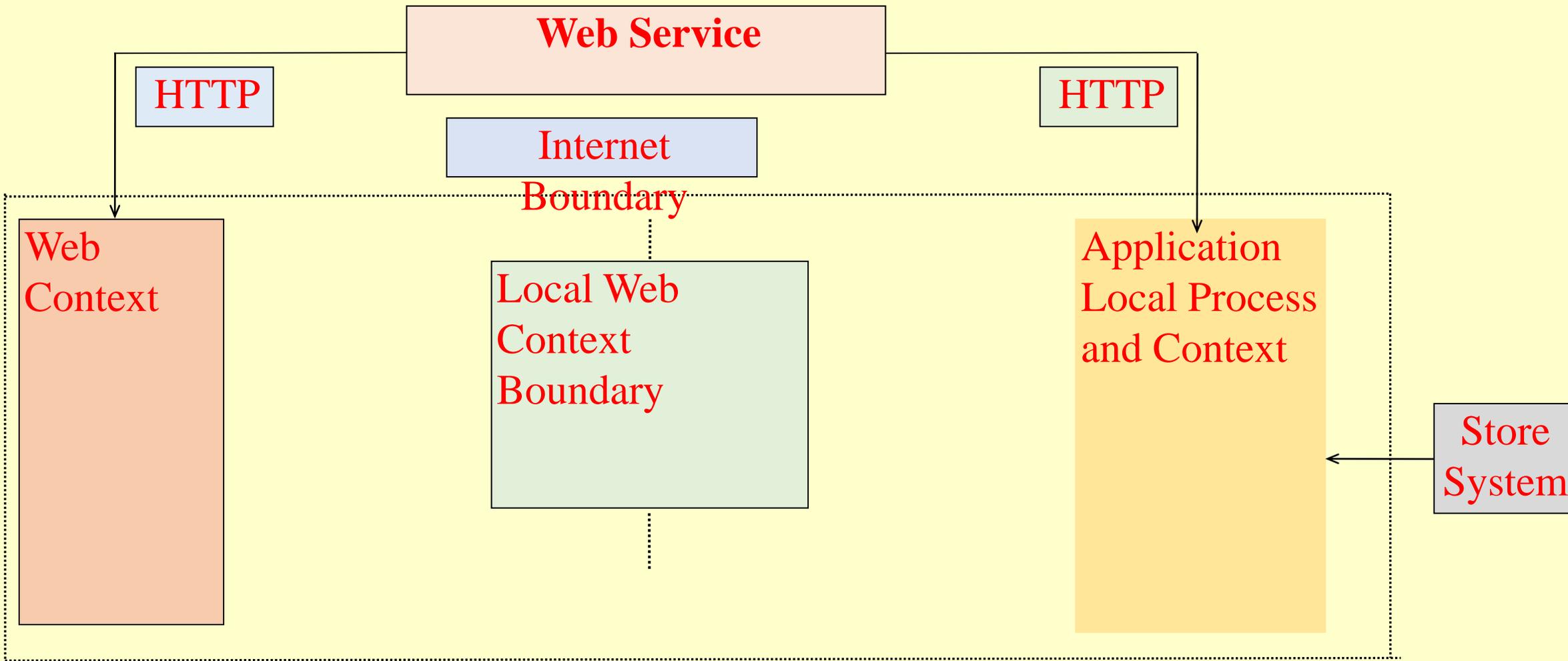


Fig. 10.2 An Application_Threat_Model in Microsoft Threat Modeling Tool display when 'Diagram' Item selected

Summary

We learnt

- Five functional components (FCs) in security functional group in-between the application/service and device
- Identity management, authentications, authorisation, key exchange and management, trust and reputation.

Summary

We learnt

- A threat analysis tool to uncovers the security design flaws after specifying the stride category
- Data flow diagram
- Elements between that the interactions occur during the stride
- Specifying the processes which are activated for analysis.

End of Lesson 3 on Security Requirements and Threat Analysis Tools