Security

Threat Modelling

Security Requirements & Misuse Cases

Security Requirements Specification

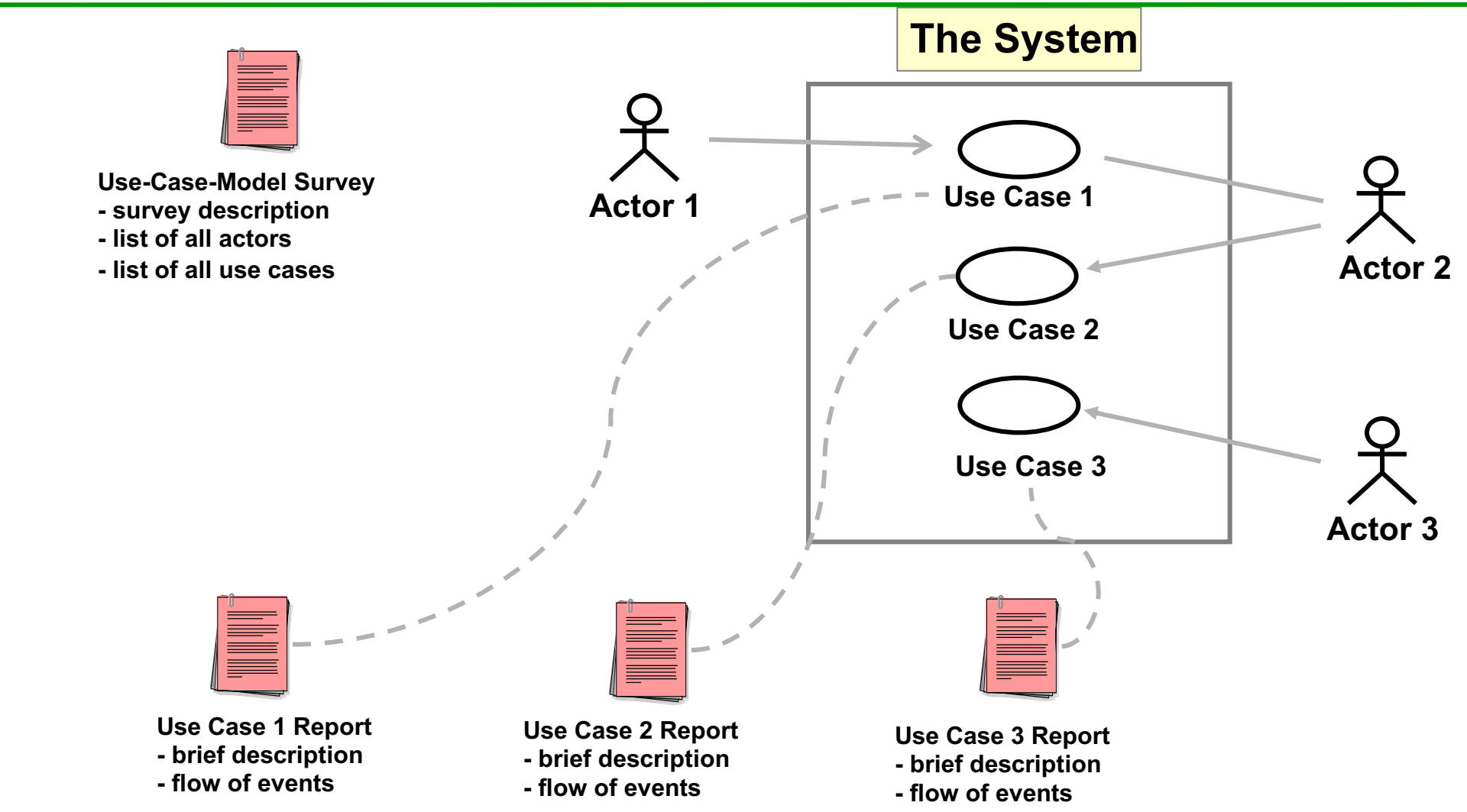
- Secure software development relies on proper specification of security requirements – to deliver confidentiality, authentication, etc
- Need to define:
  - Which controls are necessary
  - When are they necessary (applicability)
  - Why are they necessary; e.g.:
    - industry/customer expectation
    - regulatory requirement (PCI, Sarbanes-Oxley, FDA, SEC, …)
    - organisational policy,
    - common weaknesses and vulnerabilities

Use Cases in Requirements Analysis

- Use cases are a way to define interactions between a user/role and a system being designed
- Requirements analysis technique
- Defines interactions and functionality but not how it is implemented
- Formalised in UML* (Unified Modelling Language).

(*) It's probably worth noting that UML is out of out of fashion in the software industry, partly as its formal style tends to work against agile software development. The equivalent to a use case in agile development is a user story which is largely the same idea

Use Case Model



Defining a Use Case

- Two steps:
  - Write text-based case descriptions
    - What the user can do
    - How the system responds
  - Translate descriptions into diagrams

- Each use case describes one and only one function, but may have multiple paths

Syntax for Use Case Diagram (UML)

AN ACTOR:

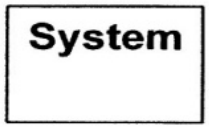
- Is a person or system that derives benefit from and is external to the system
- Is labeled with its role
- Can be associated with other actors using a specialization/superclass association, denoted by an arrow with a hollow arrowhead
- Is placed outside the system boundary

A USE CASE:

- Represents a major piece of system functionality
- Can extend another use case
- Can include another use case
- Is placed inside the system boundary
- Is labeled with a descriptive verb–noun phrase

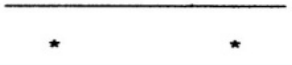
A SYSTEM BOUNDARY:

- Includes the name of the system inside or on top
- Represents the scope of the system



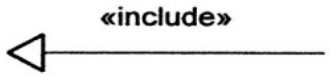
AN ASSOCIATION RELATIONSHIP:

- Links an actor with the use case(s) with which it interacts



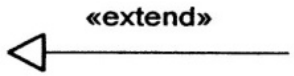
AN INCLUDE RELATIONSHIP:

- Represents the inclusion of the functionality of one use case within another
- The arrow is drawn from the base use case to the used use case



AN EXTEND RELATIONSHIP:

- Represents the extension of the use case to include optional behavior
- The arrow is drawn from the extension use case to the base use case



A GENERALIZATION RELATIONSHIP:

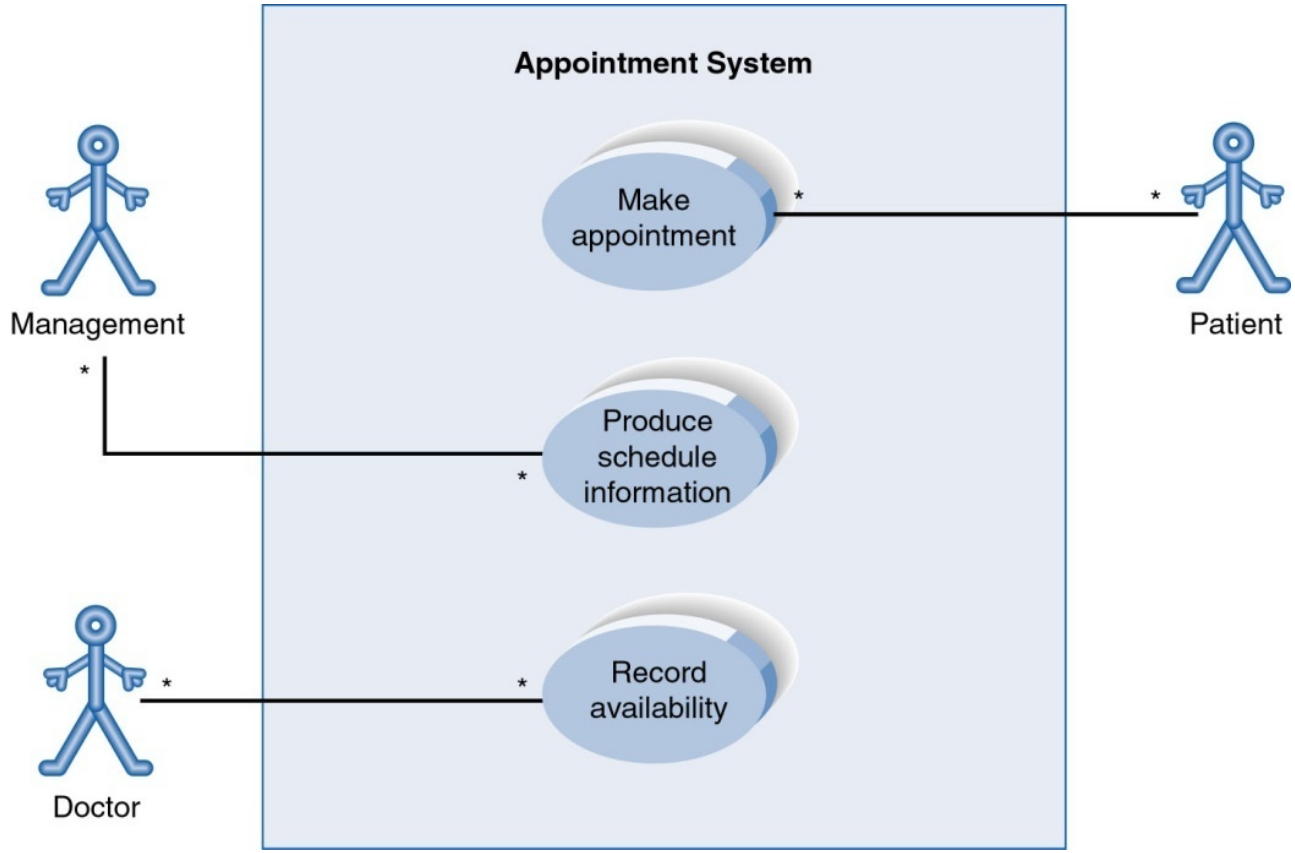
- Represents a specialized use case to a more generalized one

The arrow is drawn from the specialized use case to the base use case

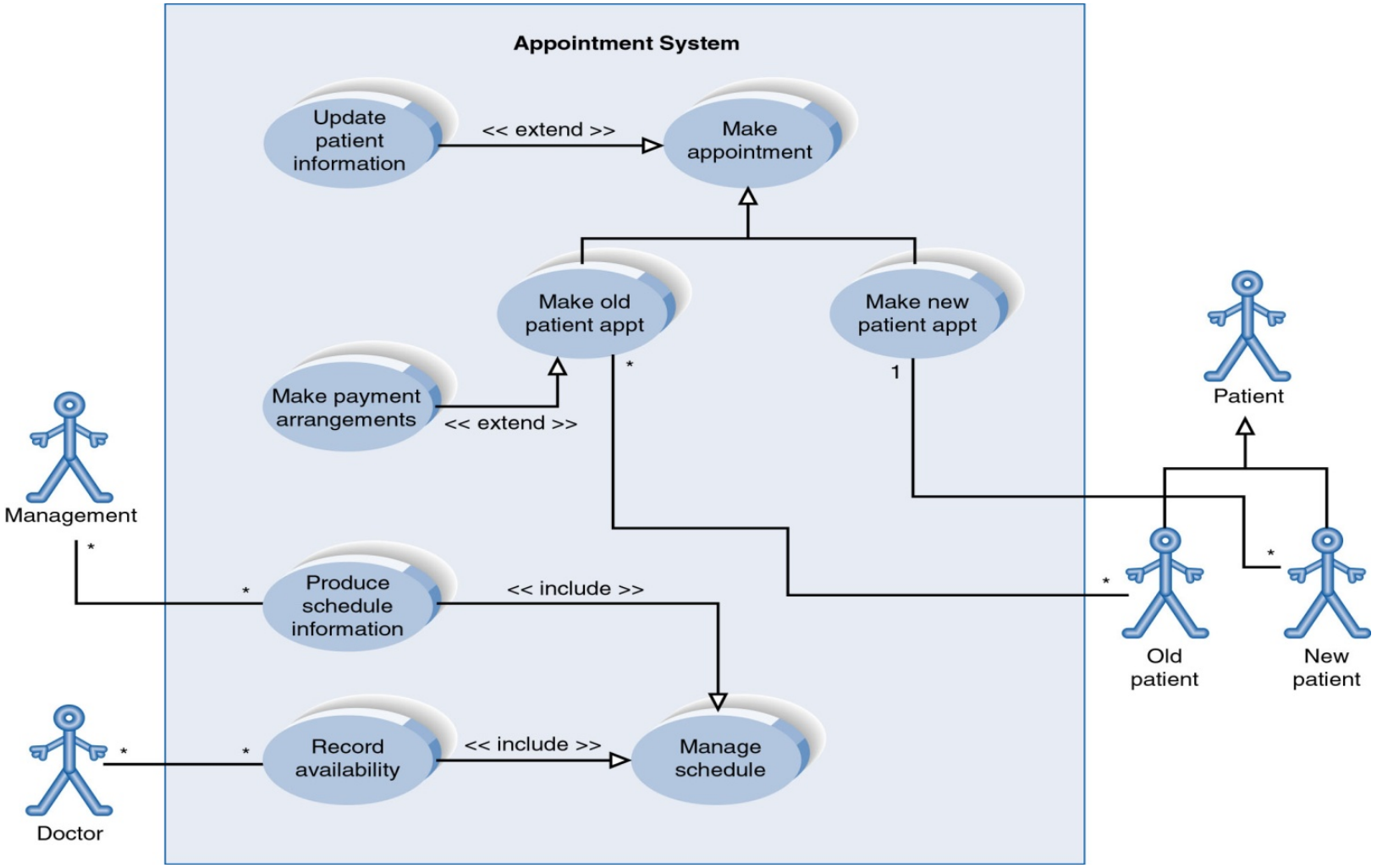
Elements of a Use Case Description

Use Case Section	Description
Name	An appropriate name for the use case
Brief Description	Description of the use case's role and purpose.
Flow of Events	Description of what the system does with regard to the use case (not how specific problems are solved by the system)
Special Requirements	Description that collects all requirements, such as non-functional requirements, on the use case.
Preconditions	Defines any constraints on the system at the time the use case may start.
Post conditions	Defines any constraints on the system at the time the use case will terminate

Use Case Diagram for Appointment System



Extend and Include Relationships



What use cases do not cover

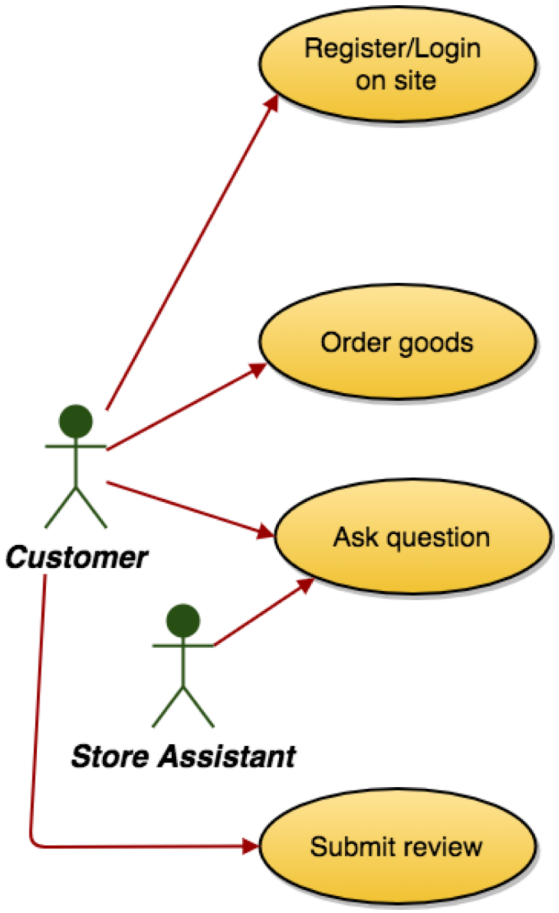
- Implementation
  - How functions are implemented
- Non-functional requirements
  - Performance
  - Scalability
  - **Security**
  - Price
  - etc
- Sequencing
- State modelling

Misuse Cases

- UML does not cater specifically for misuse/abuse cases
- Extending use cases to include **misuse cases** can be very useful for threat modelling
- A number of different styles are used for misuse cases
- New keywords introduced;
  - e.g.

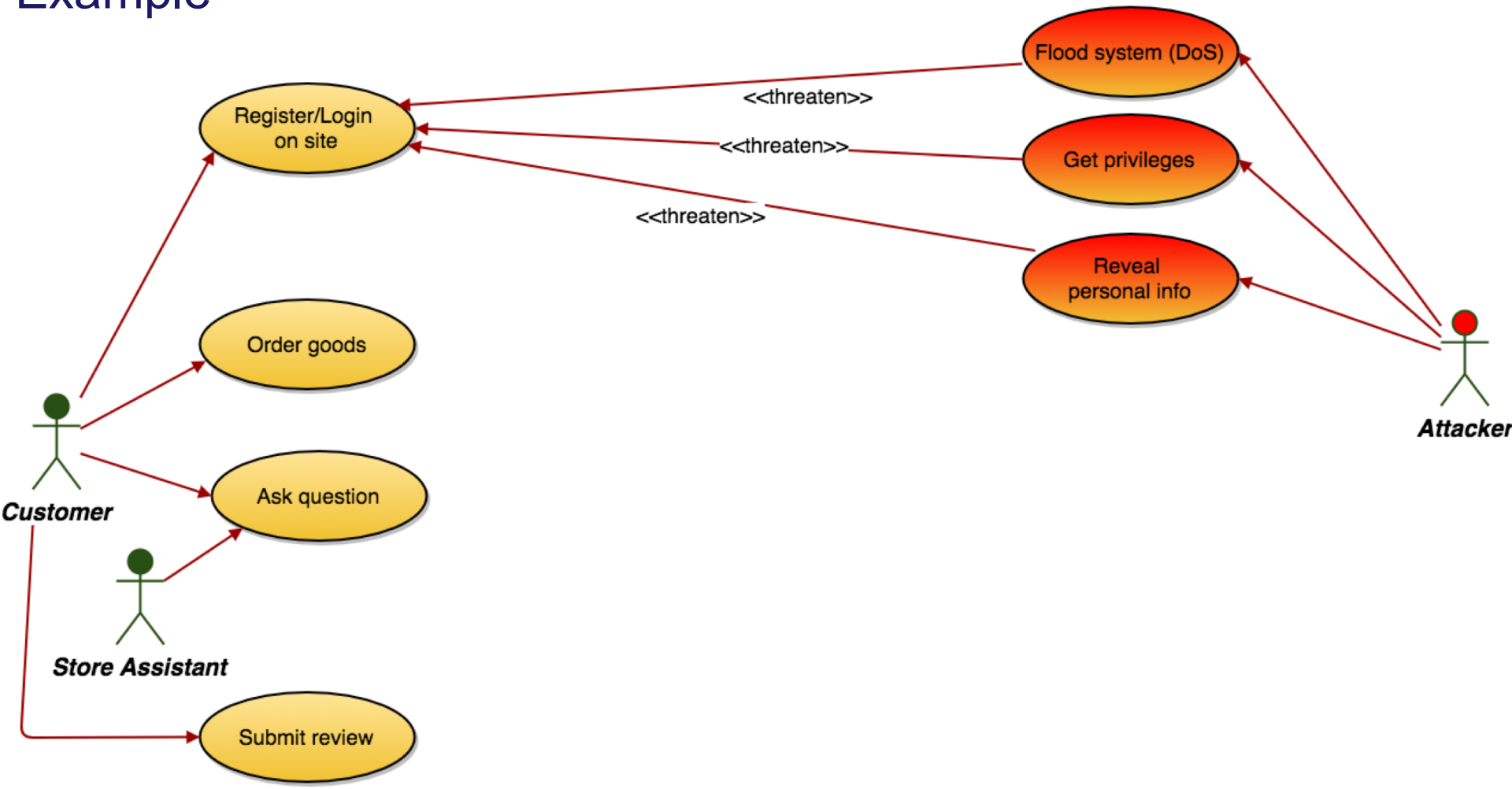
    <<threaten>> and <<mitigate>>

Misuse Cases
Example (online shop)



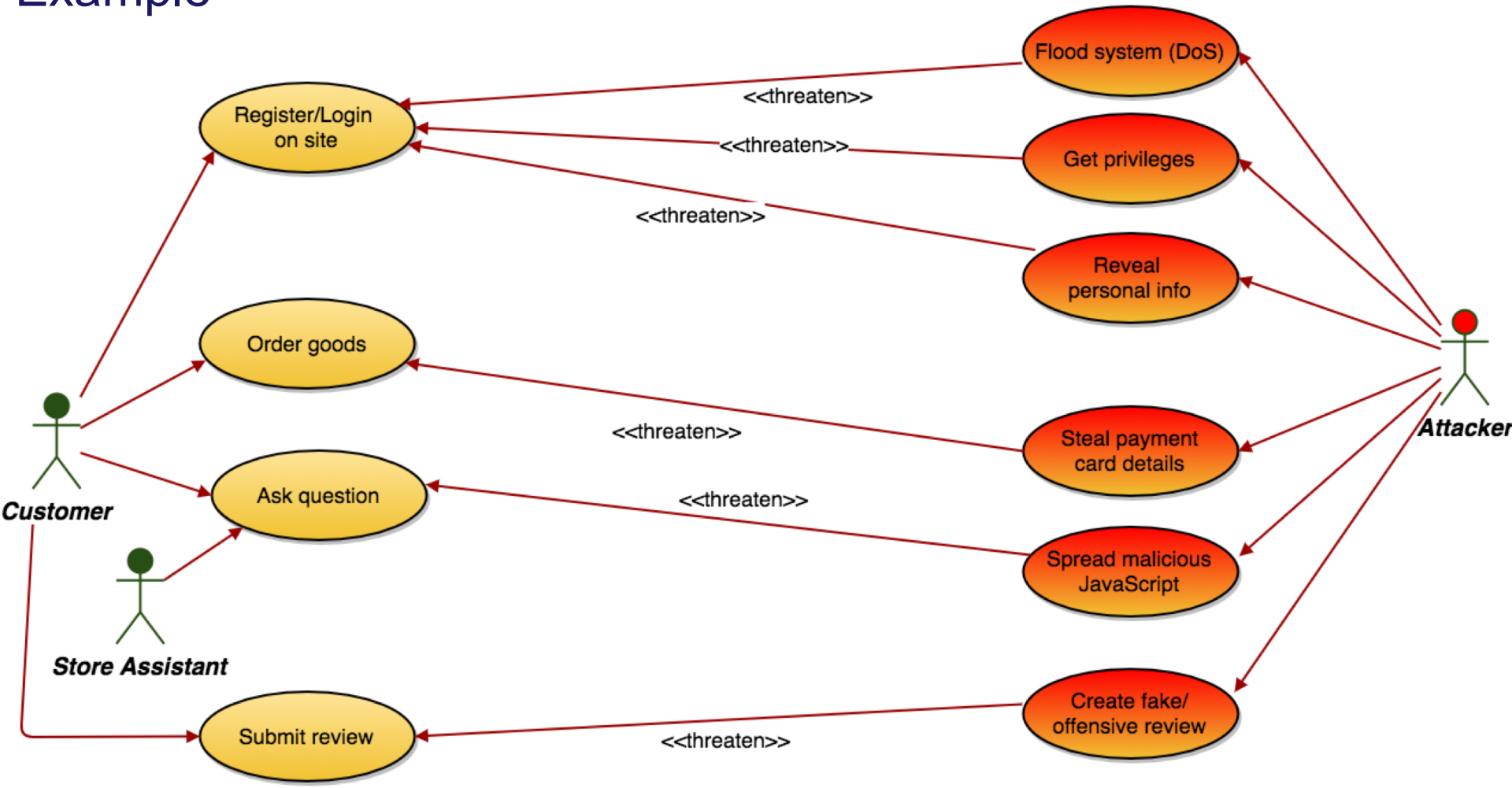
Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



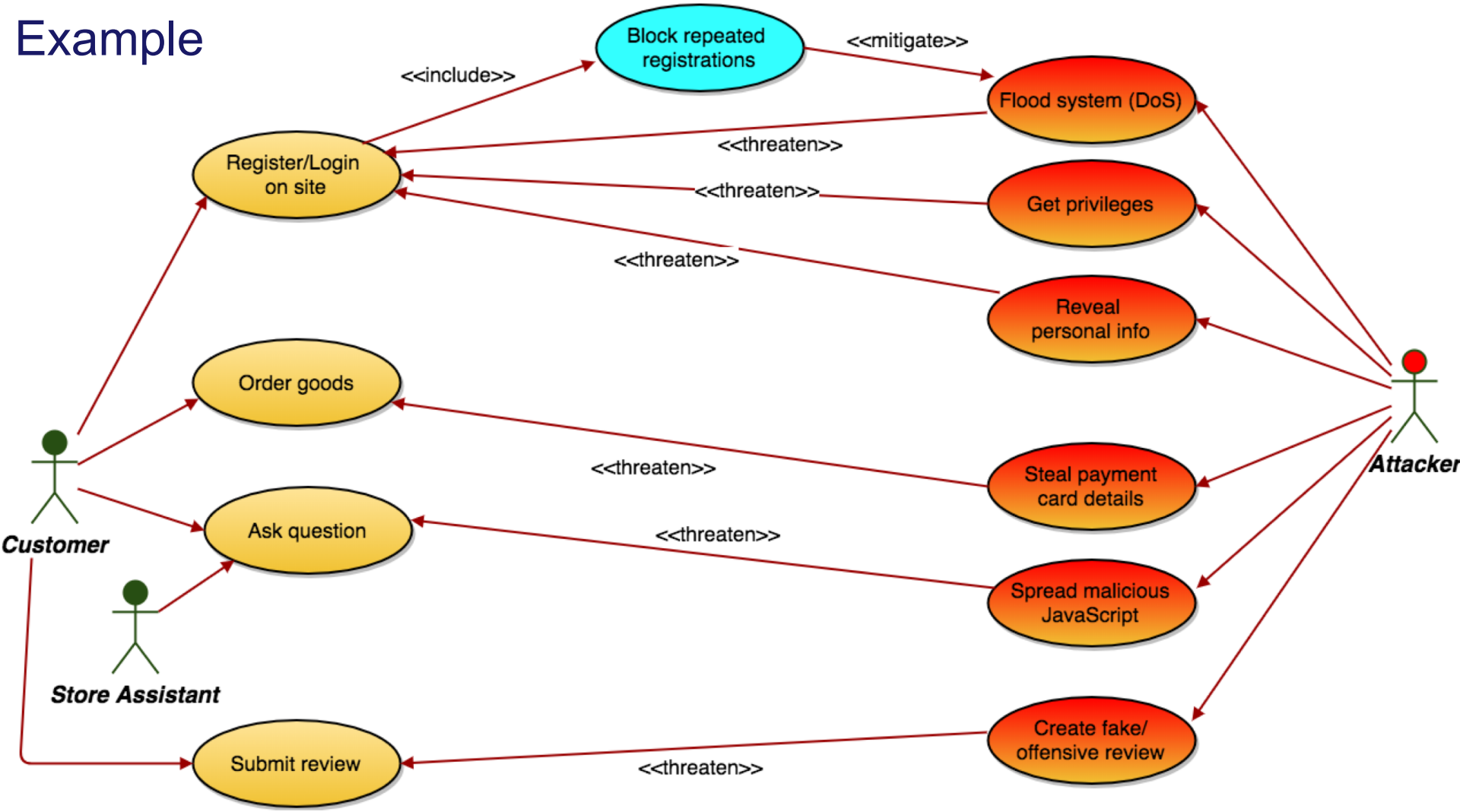
Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



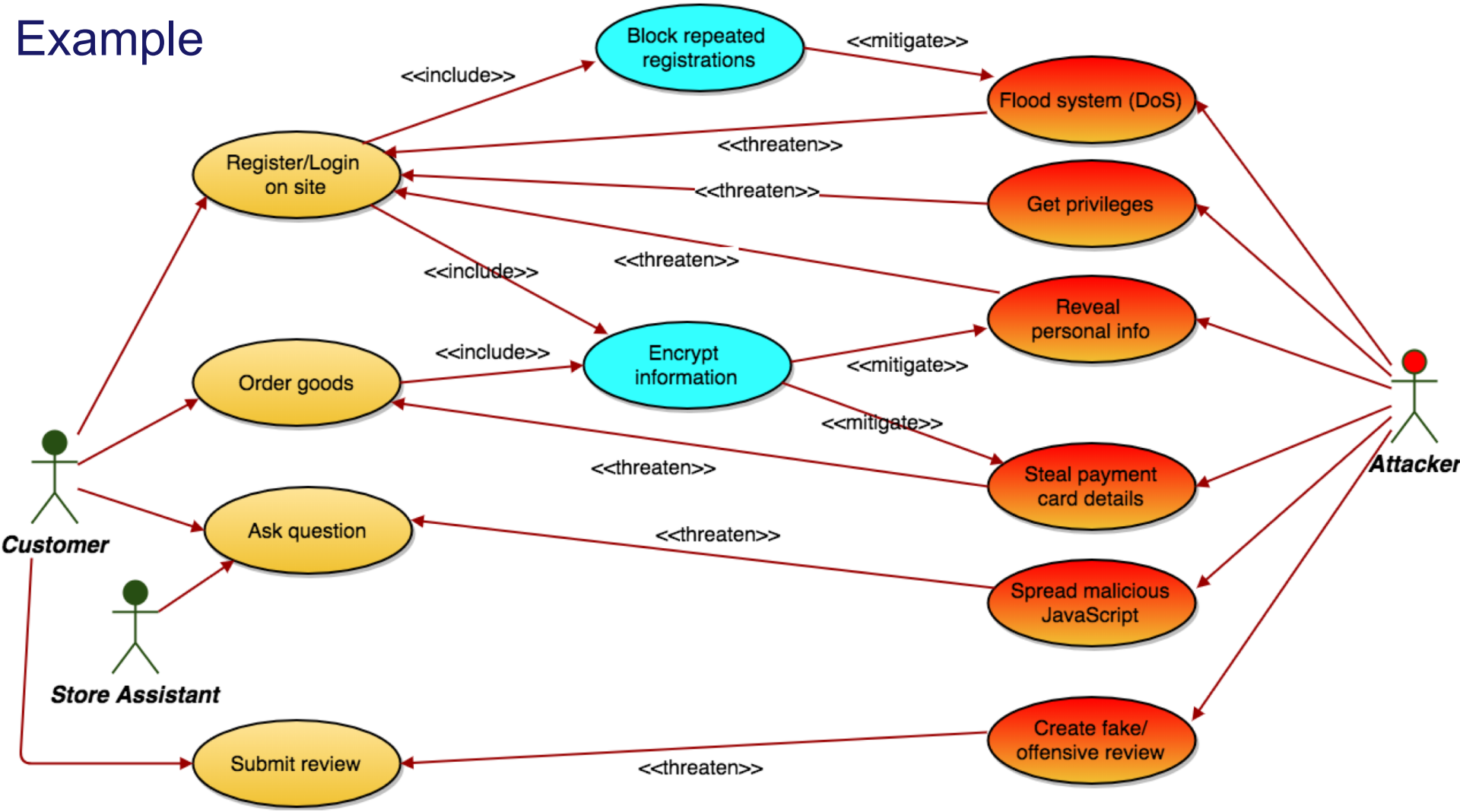
Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



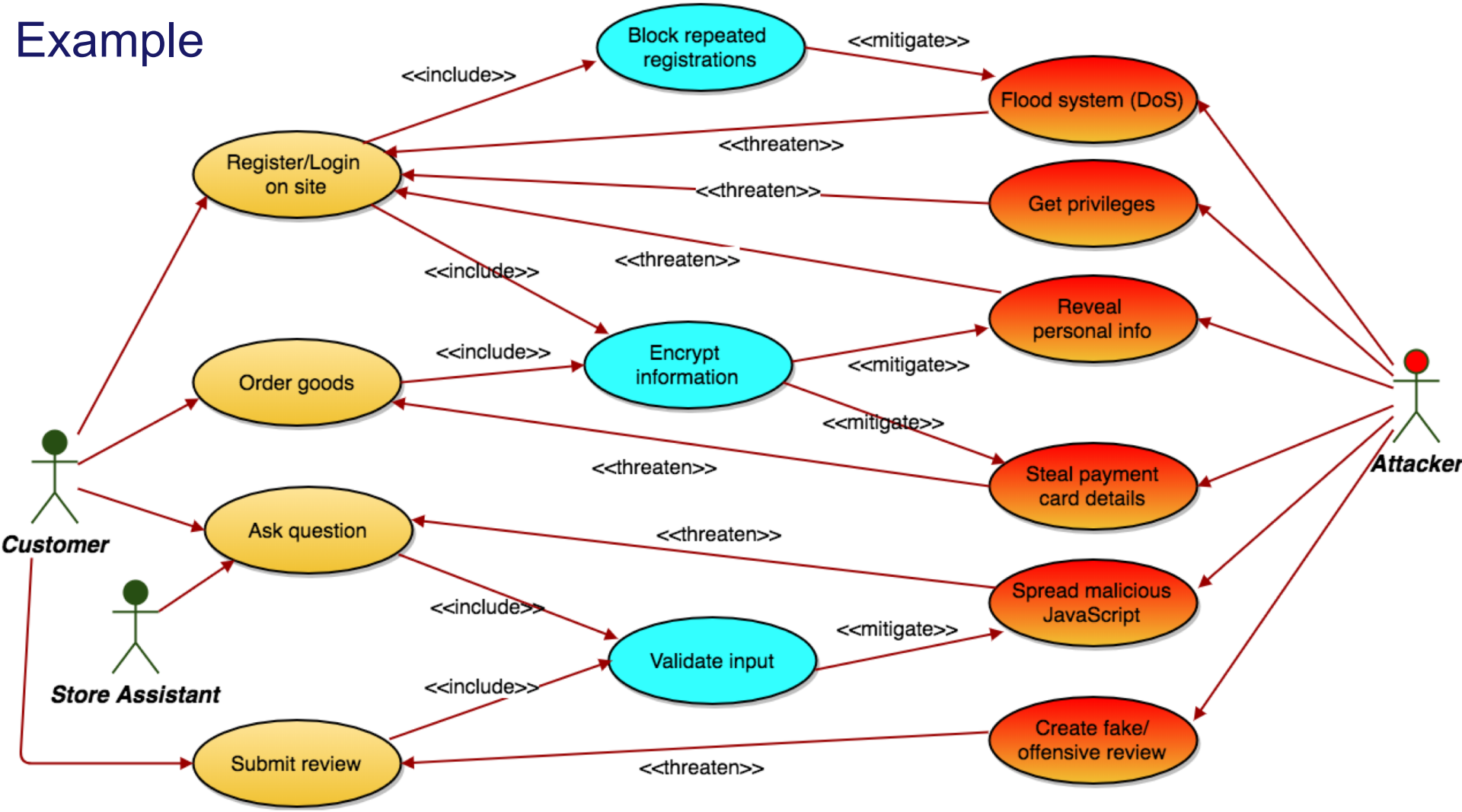
Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



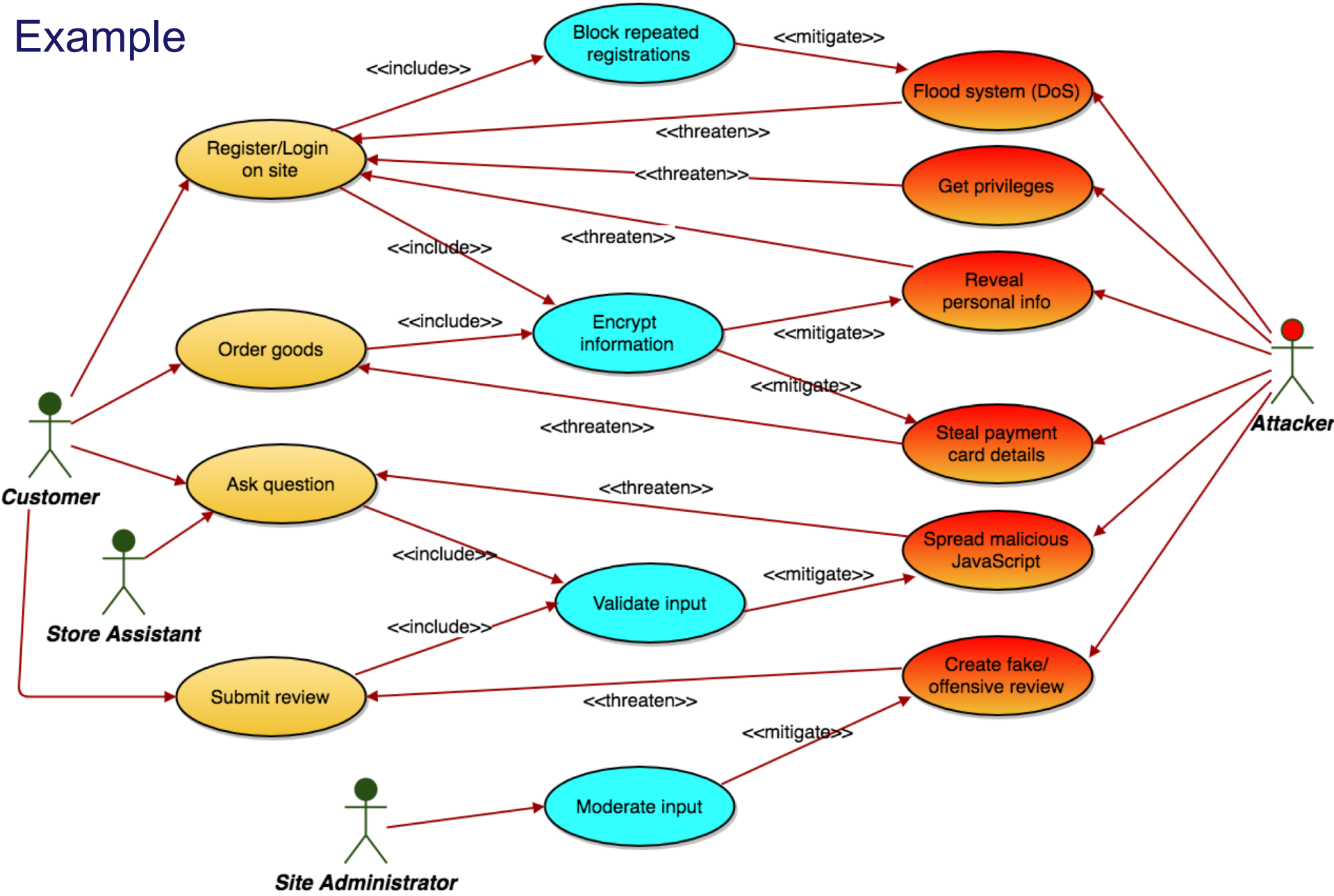
Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl

Misuse Cases Example



Adapted from: Eliciting security requirements with misuse cases, Sindre & Opdahl