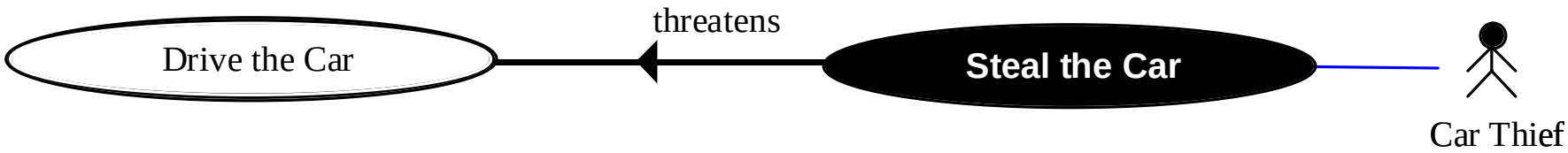
Misuse Cases

Understanding Negative Scenarios

- A Scenario is a sequence of actions leading to a Goal desired by a stakeholder

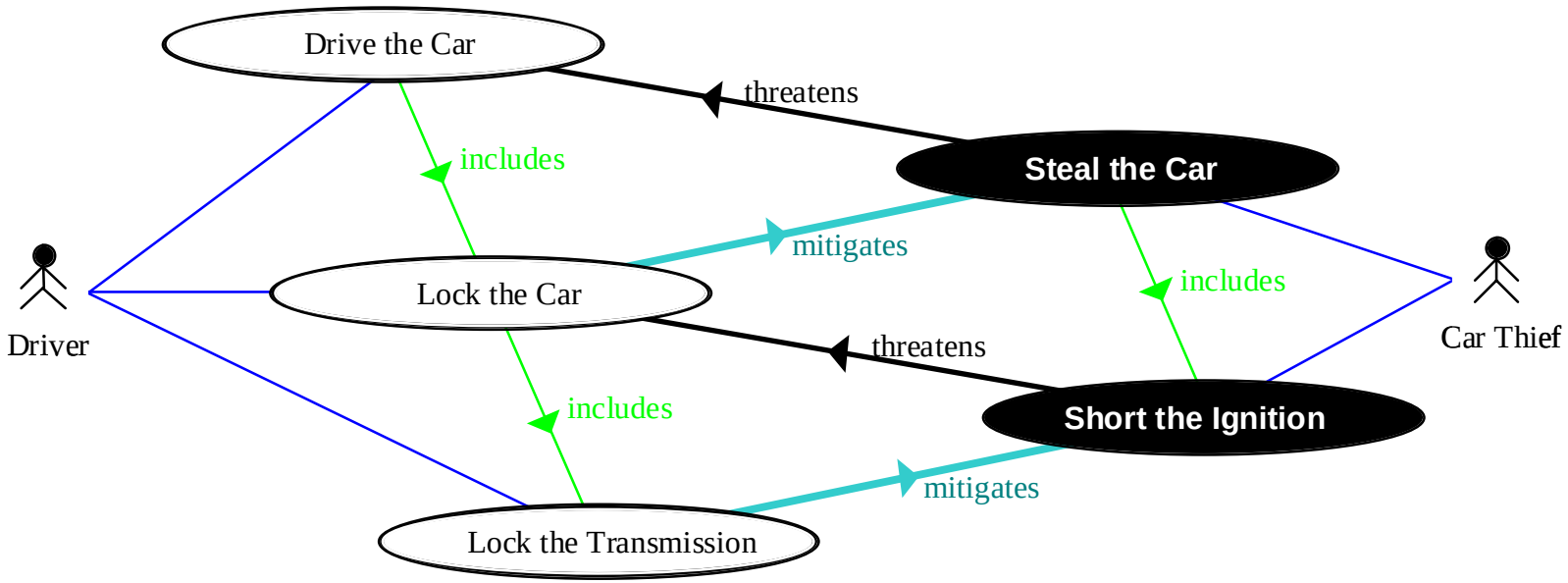
- A Negative Scenario is a scenario whose Goal is
  - desired Not to occur by the organisation in question
  - desired by a hostile agent (not necessarily human)

Misuse Cases



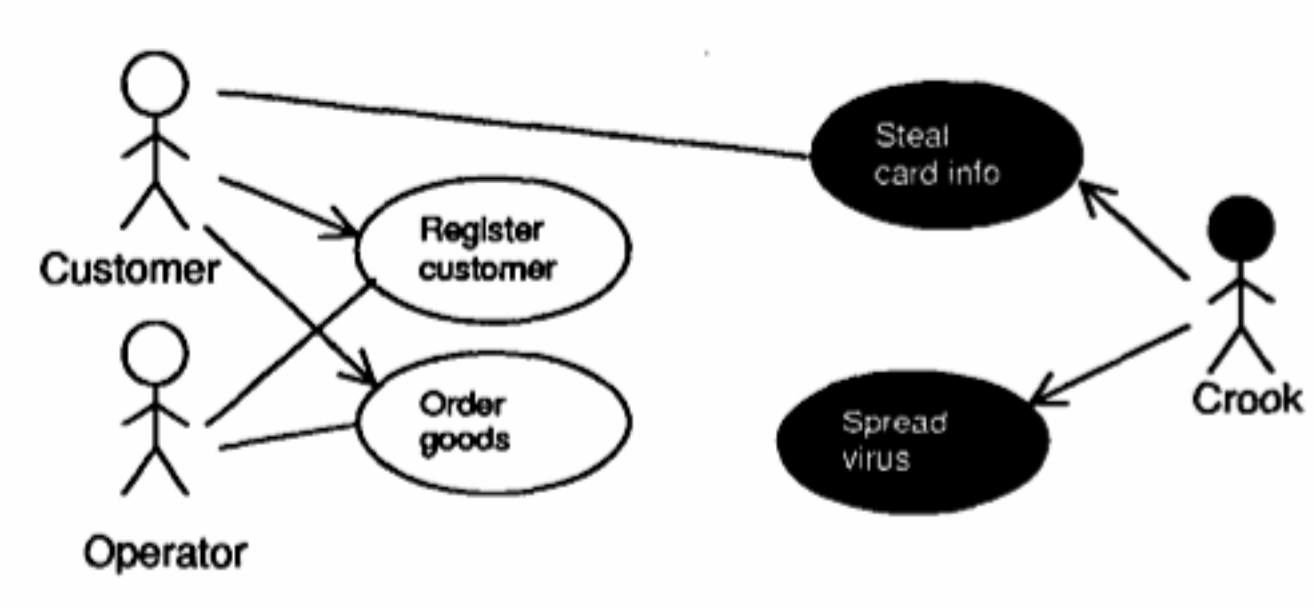
- Guttorm Sindre and Andreas Opdahl, 2000
- Actor is a Hostile Agent (Misactor)
- Bubble is drawn in inverted colours
- Goal is a Threat to Our System

A Chess Approach to Security

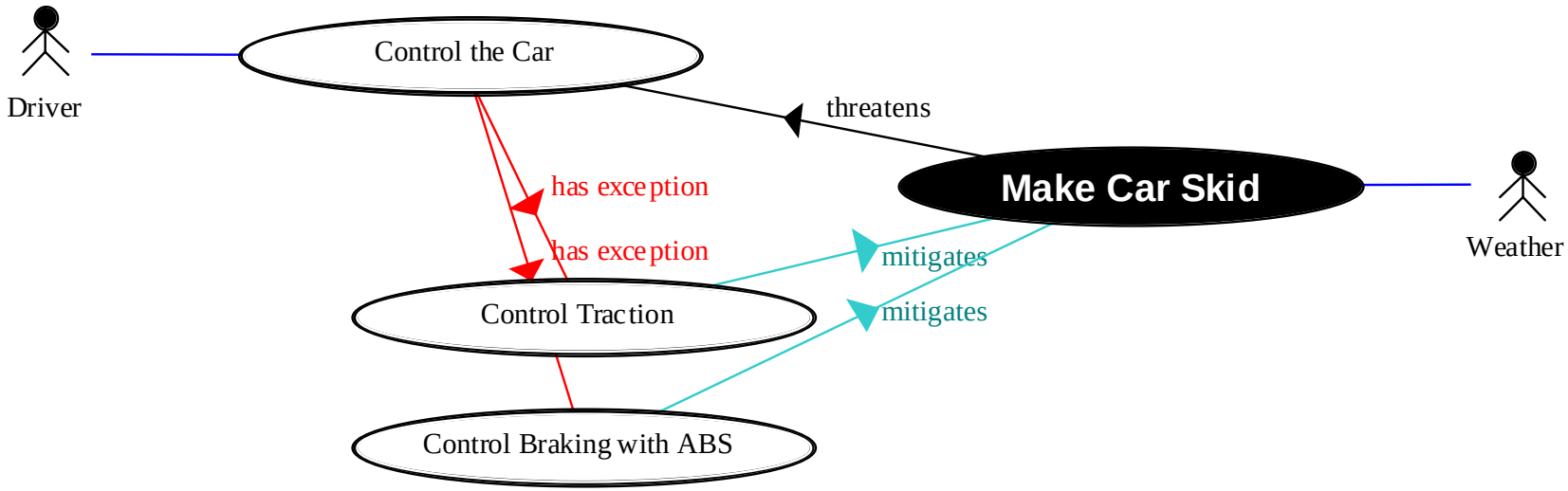


Use Cases for 'Car Security' [3]

- Actor's Best Move … is to find out Misactor's Best Move, and counter it
- Misuse Case A 'threatens' Use Case B if achieving the goal of A reduces the system's ability to achieve the goal of B
- Use Case A 'mitigates' Misuse Case B if it reduces B's effects on the Use Cases that it 'threatens'.
  - Also sometimes *prevents*: the function provided by the use case that the arrow originates from, prevents the activation of the misuse case that the arrow is directed towards, sometimes.
  - *detects*: the function provided by the use case that the arrow originates from, detects the activation of the misuse case that the arrow is directed towards, sometimes.

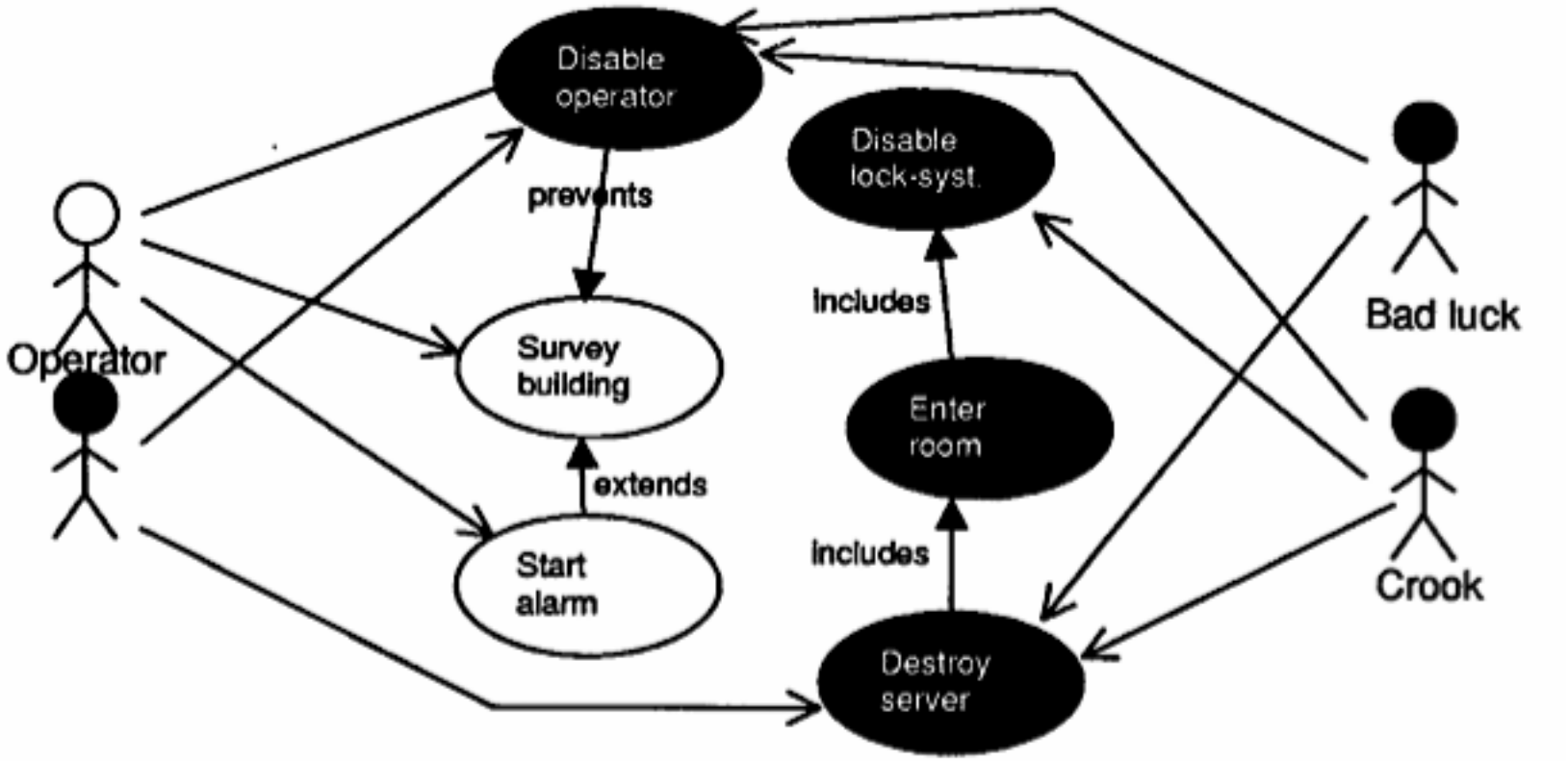

Customer
Operator
Register customer
Order goods
Steal card info
Spread virus
Crook

Anthropomorphize … for Safety

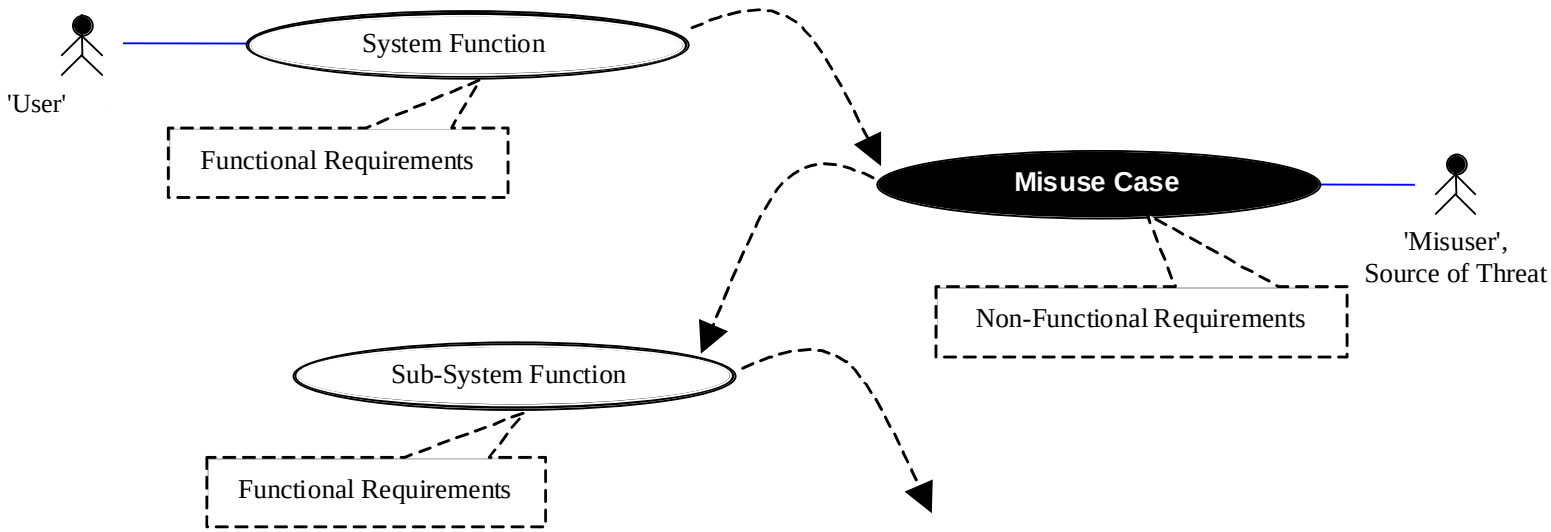


- UML's stick-man looks like 'human agent' but can be of any type (robot, system)
- Anthropomorphizing Forces of Nature is useful: it enables us to reason about threats to our systems
- Misuse Case helps to Elicit Subsystem Functions

Another example



Misuse Cases Identify NFRs



Interplay of Use & Misuse Cases with Functional & Non-Functional Requirements

- Use Cases are weak on Nonfunctional Requirements (NFR)
- Misuse Cases naturally focus on NFRs, e.g. Safety
- Response is often a SubSystem Function, possibly to handle an Exception

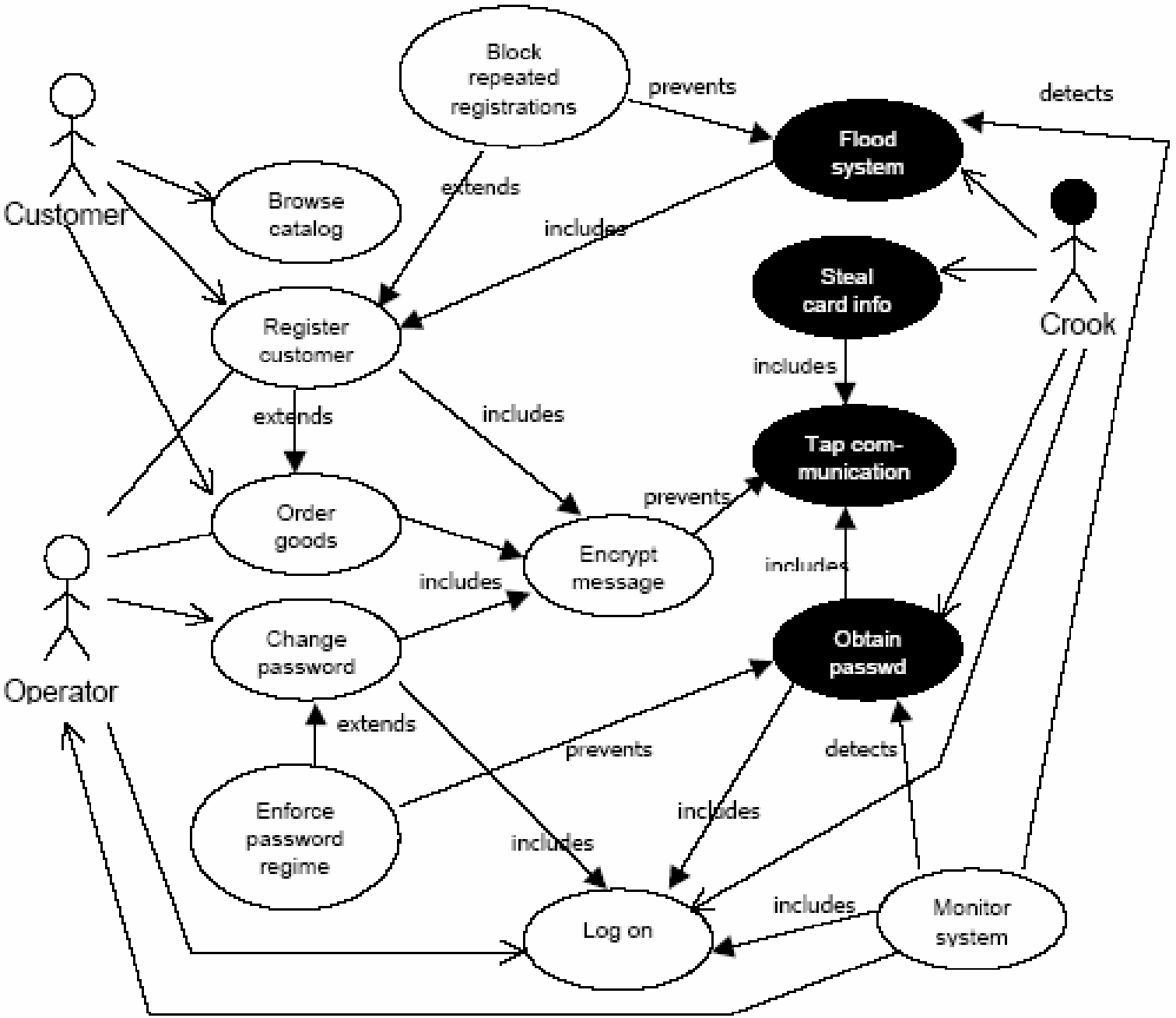
Benefits of Misuse Cases

- Open a new avenue of exploration
- Contribute to searching systematically for exceptions, directed by the structure of the scenarios
- Offer immediate justification for the search and indicate the priority of the requirements discovered
- By personifying and anthropomorphizing the threats, add the force of metaphor to requirements elicitation
- Make the reasoning behind affected requirements immediately comprehensible

Applications of Misuse Cases

- Eliciting Security Requirements
- Eliciting Safety Requirements
- Identifying Exceptions
- Identifying Test Cases
- Design Trade-offs

Misuse Case Example


Block repeated registrations
prevents
detects
Flood system
Customer
Browse catalog
extends
includes
Steal card info
Crook
Register customer
includes
extends
includes
Tap com-munication
Order goods
prevents
Encrypt message
includes
includes
Operator
Change password
Obtain passwd
extends
prevents
detects
Enforce password regime
includes
includes
Log on
includes
Monitor system

Misuse Case Example

- **Name:** Obtain Password
- **Summary:** A crook obtains and uses a password for e-shop by reading messages sent through a compromised network.
- **Author and Date**

Misuse Case Example

- **Basic Path (bp0): (aka Primary Scenario)**
  - The primary path of action taken, ending with success for the misactor and thus failure for the system and its owners.
  - **Bp0-1** A crook hacks a host and installs IP sniffer
  - **Bp0-2 (and extension point e-1):** All packets with Login, password, etc are intercepted and analyzed
  - **Bp0-3** Thus the crook collects likely username and password pairs
  - **Bp0-4** The crook uses the stolen username and password pair to login illegally

Misuse Case Example

- **Alternate Paths:**
  - Alternate paths of completion of the scenario.
    - Can highlight specific technologies or extreme data values that can be exploited.
  - **Ap1:** The crook has Superuser privileges (at Step 1)
  - **AP2:** The crook intercepts telephone messages from e-shop operator (at Step 2)
  - **AP3:** The crook intercepts e-shop operators portable device's messages (at Step 3)

Misuse Case Example

- **Capture Points**
  - Used to represent the various ways in which misuse is prevented/detected. These work against the misactor.
  - **CP1:** Password does not work – changed (bp0-4)
  - **CP2:** Password does not work – expired (bp0-4)
  - **CP3:** Password does not work – different IP address (bp0-4)
  - **CP4:** Operator login restricted to special IP (bp0-4)
  - **CP5:** Communication uninterruptible (bp0-2)

Misuse Case Example

- **Extension Points:**
  - Shows optional actions which may be taken. They cover actions that the misactor wants to perform.
  - **Ep1:** Extends misuse case *Tap Communications* (in step bp0-2)
- **Triggers: (in template - Under Preconditions)**
  - conditions that describe situations where something else than the primary actor initiates the use case (such as timing).
  - **Tr1:** always true
- **Preconditions:**
  - conditions which can be ensured by the system itself
  - **Pc1:** Operator has special authority
  - **Pc2:** Operator allowed to login over the Internet

Misuse Case Example

- **Assumptions: (in template under Preconditions)**
  - conditions which must be true but which cannot be guaranteed by the system itself
  - **As1:** operator uses the network to login (for all paths)
  - **As2:** operator uses home phone to login (for ap2)
  - **As3:** operator uses home phone to login (for ap3)
- **Worse case threat:** (post condition)
  - Describes the outcome if the misuse succeeds. If alt paths, this condition will describe variations in the outcome.
  - **Wc1:** The crook gains operator access
- **Prevention guarantee:** (post condition)
  - Describes the guaranteed outcome whatever prevention path is followed.
  - **Cg1:** The crook never gets operator access

Misuse Case Example

- **Potential Misactor Profile:**
  - Highly skilled, possibly a network admin with criminal intent
- **Stakeholders and Threats:**
  - e-shop:
    - Reduce turnover
    - Lost consumer confidence
  - Customer:
    - Privacy violation
    - Potential economic loss
- **Scope:** Entire business environment

Methods for Building Misuse Cases

1. First build Use Cases with actors
2. Introduce major Misuse Cases
3. Identify potential relationships between Use Cases and Misuse Cases

References

1. Slides by Professor Stephanie Ludi RIT SE Department Winter Quarter 2006
2. Templates for Misuse Case Descriptions by Gottorm Sindre and Andreas L. Opdahl available at www.ifi.uib.no/conf/refsq2001/papers/p25.pdf
3. Capturing security requirements through Misuse Cases by Gottorm Sindre and Andreas L. Opdahl available at www.nik.no/2001/21-sindre.pdf
4. Initial Industrial Experience of Misuse Cases in Trade-Off Analysis by Ian Alexander, available at http://easyweb.easynet.co.uk/~iany/consultancy/misuse_cases/misuse_cases_in_tradeoffs.htm
5. From Misuse cases to Colboration Diagrams by Zaid Dwaikat and Francesco Parisi-Presicce available at www.software.org/pub/externalpapers/papers/dwaikat-2004-1.pdf
6. Thanks to work from Ian Alexander