SOFTWARE SECURITY

WINTER TERM
2018/2019

SAFE AND SECURE SOFTWARE SYSTEMS
BTU COTTBUS-SENFTENBERG

Exercise Sheet 1: Security Analyses and Information Flows

Brandenburgische
Technische Universität
Cottbus - Senftenberg

[redacted]
Siddique Reza Khan
[redacted]
[redacted]
[redacted]

Network topology model: Network topology model of the system

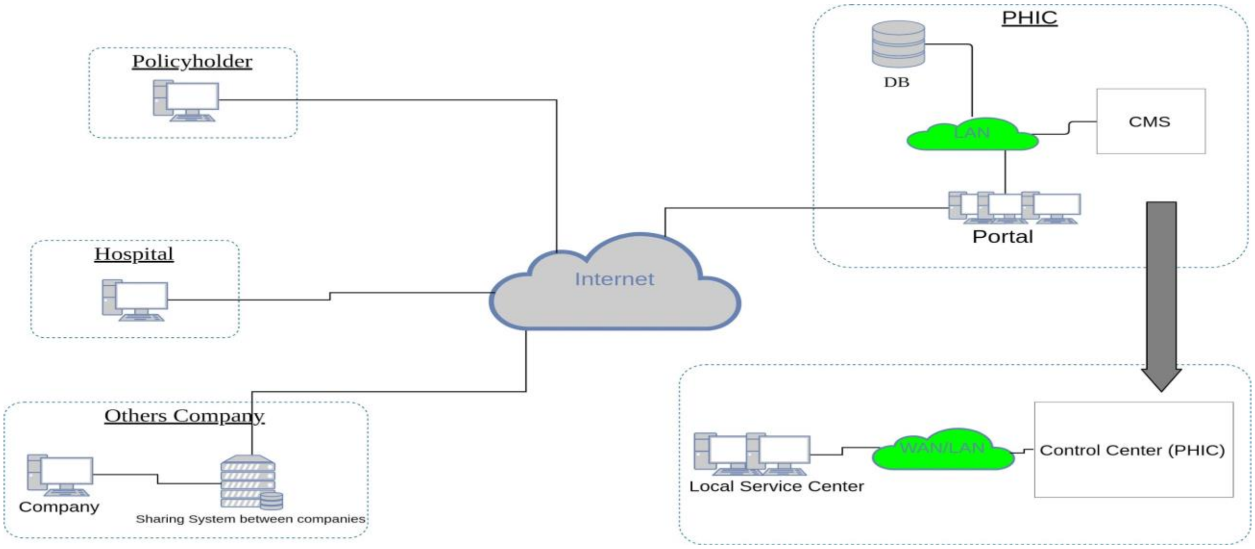

Figure 01: Network Topology

- Home Area Network: The policyholder and Hospital communicate with the PHIC via the web portal through internet.
- WAN: the Local service center and Control Center(PHIC) communicate with the central database for all policyholders and the other company are going to sharing the database of the PHIC for advertisement purpose.

Use case model: Use case model to describe actors and system functionality including protection goals for each actor

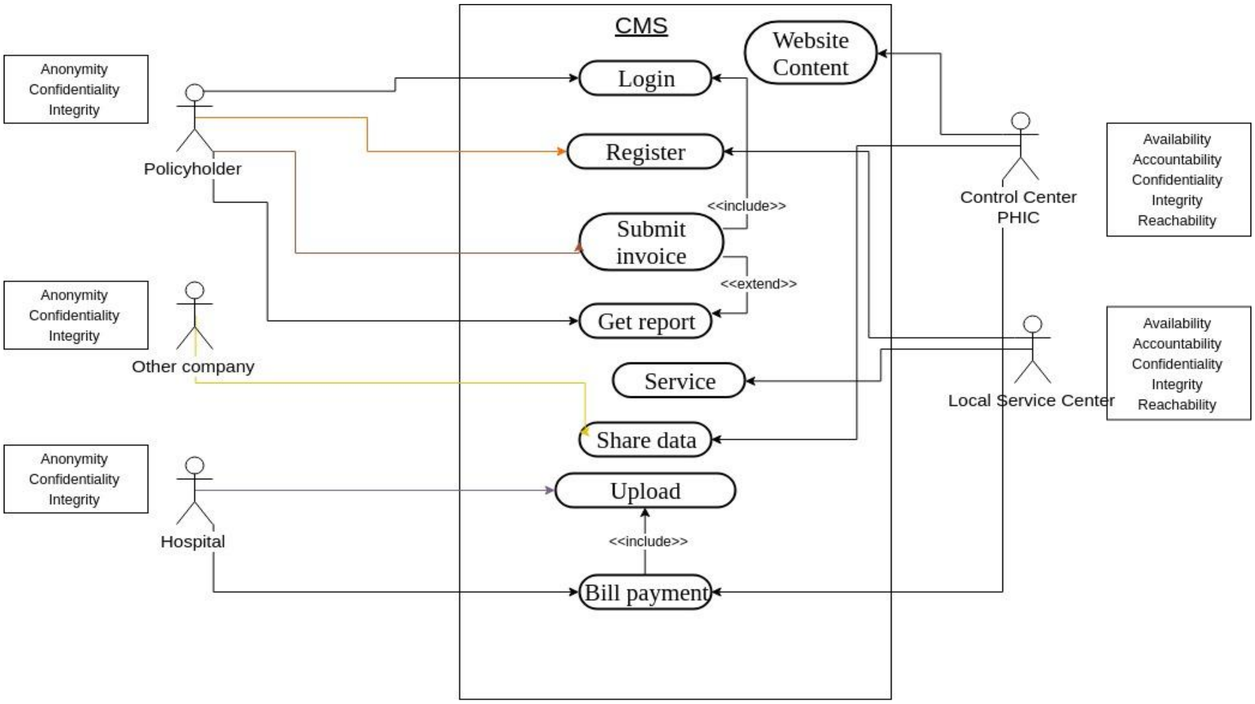

Figure 02: Use Case Model

– Which persons are involved in which roles with the system?

In our case scenario, we assume here that there are only two roles for the CMS; that is Admin and Users. Here, Control Center PHIC actor has Admin privileges and all other actors are Users such as, Policy Holder, Other Company, Hospital and Local Service Center.

– Who has what protection goals?

Protection Goal/Actor	**Accountability**	**Availability**	**Confidentiality**	**Integrity**	**Reachability**	**Anonymity**
Control Center PHIC	X	X	X	X	X	
Policy Holder			X	X		X
Other Company			X	X		X
Hospital			X	X		X
Local Service Centre	X	X	X	X	X	

Damage Scenarios:

Two damage scenarios including an evaluation resulting in the required level of protection

1) It is an attack on database, which can be compromise policyholder's data information.
2) It is an attack on website, which may create a bad reputation for the insurance company.

Protection Level	**Damage impact**
Very high	Data privacy loss.
High	Insurance company's website could not be accessed due to lots of traffic from non-legitimate user thereby causing denial of service attack, but it may be considerable.

Misuse Cases:

At least one misuse case diagram and one attack tree to refine an attacker goal.

– Who can act as an attacker against the protection goals of which parties?

In our misuse case, we consider the attacker attacks on the protection goal named Integrity, and Confidentiality for Actor and Policy Holder. Whereas, the attacker attacks on the protection goal named accountability, availability and reachability for the Actor, Control Center PHIC.

– What is the interest of these attackers?

First, the attacker’s intent might be to get service from the Insurance Company without paying the monthly premium. Again, he can make changes to the database payment entity (as Payment status would reflect the true position of your payment history. Attacker can change its status to “paid”). Moreover he is thinking to get any kinds of extra facilities from the Insurance Company by generating and submitting a fake bill to the Insurance Company.

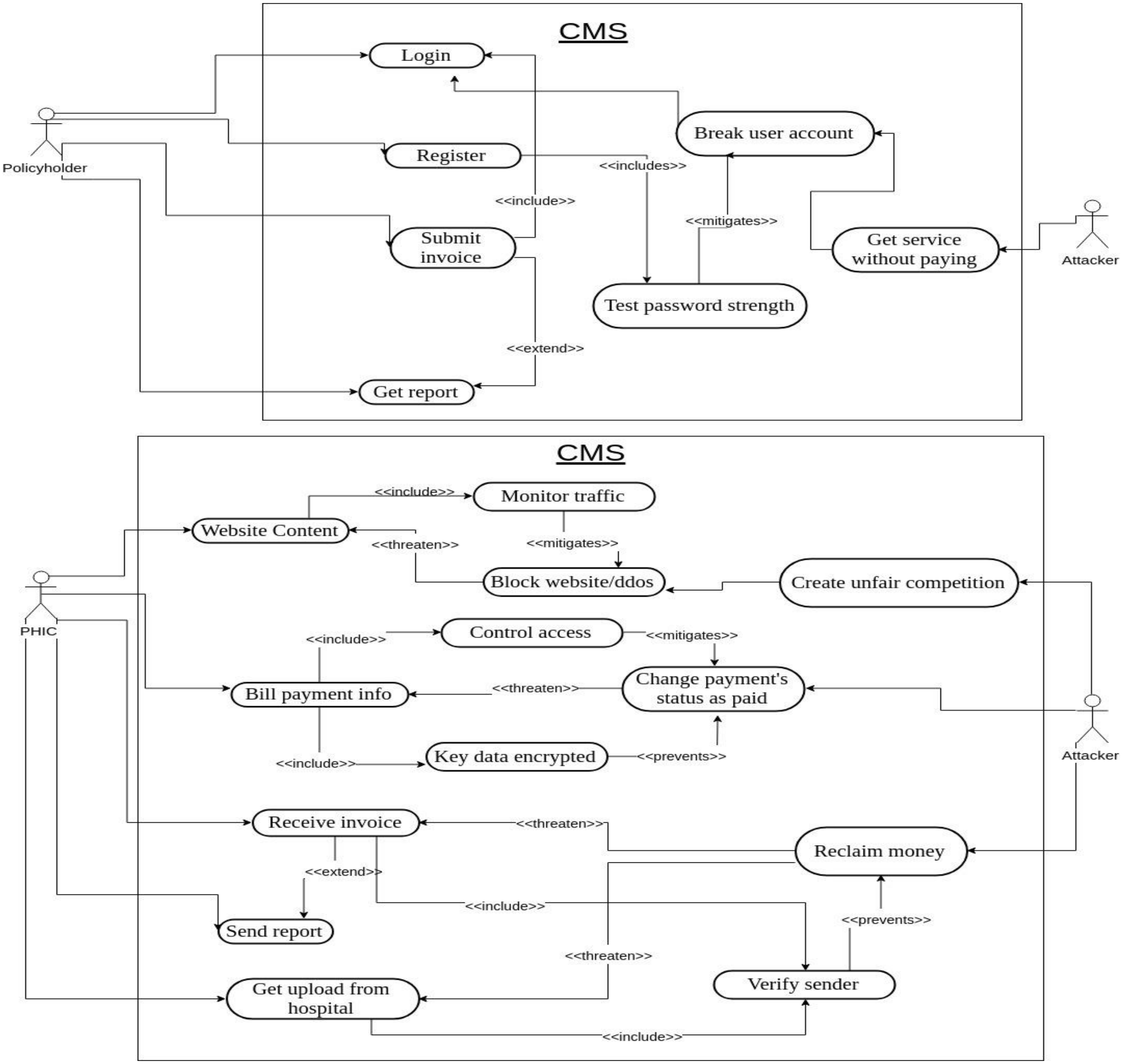

Figure 03: Misuse Case Model

Secondly, the attacker thinks to create a bad reputation for the Insurance Company by trying to benefit from the others competitor by posting unnecessary pop-up advertisement/information, or block the regular service of the website by sending lots of unwanted traffic to the website thereby also causing denial of service attack.

Attack Trees: An extended version of the attack tree, tagged by fictive costs and probabilities.

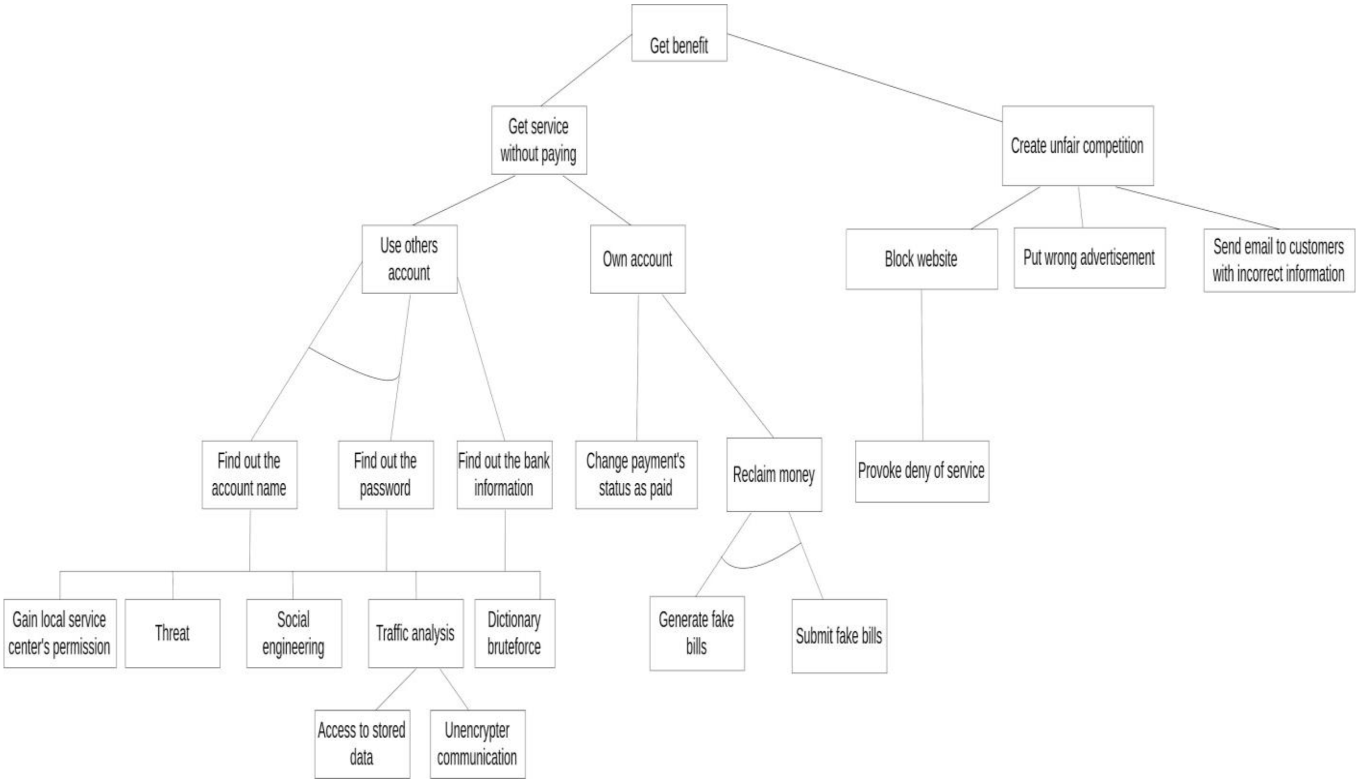

Figure 04: Attack Tree

– What power, what capabilities do these attackers have?

In our general attack tree, the main attack goal is to get monetary benefit using the other policy holder’s account as well as own account. For this purpose, the attacker needs an unauthorized access and privileges to the Database whole entity. Also, with the assumption that the Attacker is a tech savvy black hat hacker with a high skill-set and bad intent. The extent of damage that can be caused by this attacker are limitless, one of attacks is the monetary gain which can be done by running an ‘Update’ script to alter entries on the database. By so doing, the attacker has the power to change the status of his payment from ‘Unpaid’ to ‘Paid’. In addition to this, the attacker can generate fake bills in order to get some additional benefit from the insurance company.

Left side of our attack tree the attacker is hired by some of our competitor with the goal of putting some unnecessary pop-up advertisement and generating some unwanted traffic to block the website for doing its regular functioning. In this case scenario, we have to assume that the attacker has a vast experience on to develop a web application with PHP, ASP.Net, Javascript, etc and Web server that is Apache, IIS, etc. The attacker may send some spam e-mail to the policyholders with the fake link of advertisement so that they can be redirected to another fictitious website. Last but not the least, the attacker will create a huge traffic to attack on the web server like DOS, DDOS attack, so that the policyholder may not access the website for their regular day to day activities.

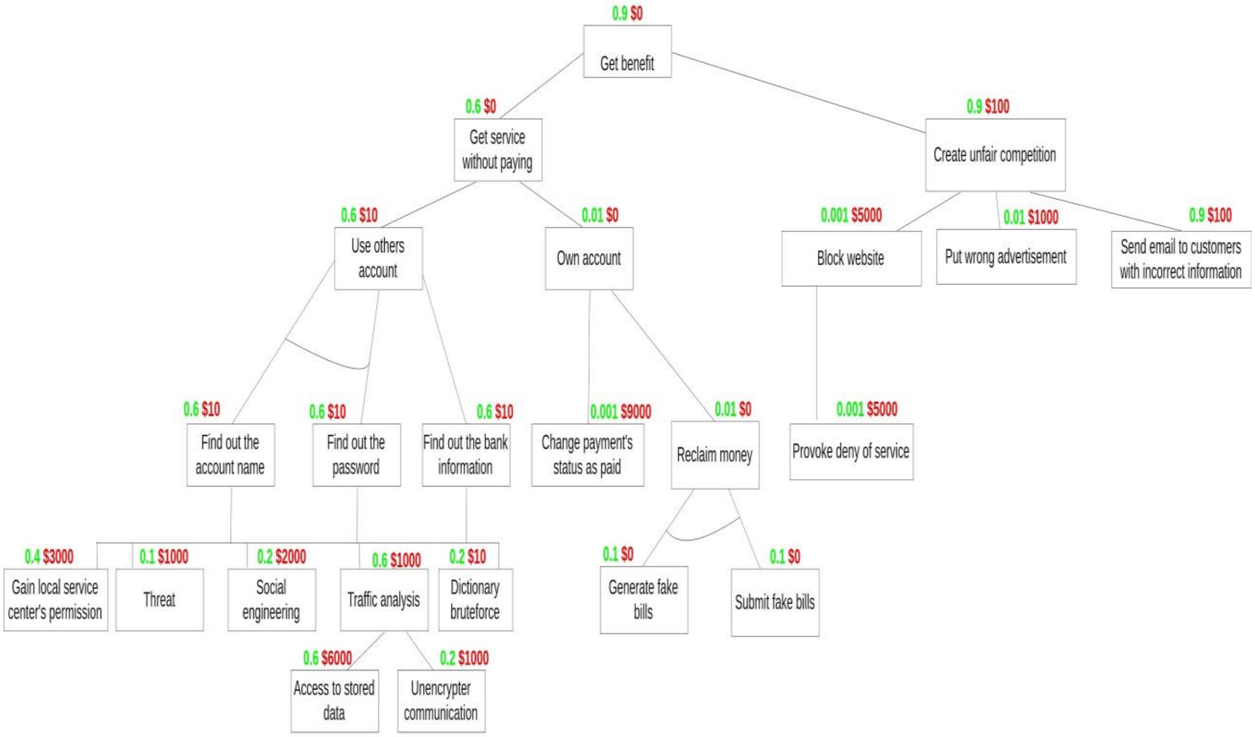

Figure 05: Extended Attack Tree

In this case of the extended version of the attack tree, we have tagged few fictive costs and probabilities by using following rules.

1. For the fictive the costs of a parent node are:
    - the sum of the costs of all sub-nodes for an AND relationship or
    - the costs of the most cost-effective sub-node for an OR relationship
2. For the probability of a parent node is:
    - the product of the probabilities of all sub-nodes for an AND relationship or
    - the maximum of the probabilities of all sub-nodes for an OR relationship.