**MIS607 – CYBERSECURITY**

**ASSESSMENT TITLE – THREAT MODEL REPORT**

**STUDENT NAME: MOHAMMED ZHOEB**

**STUDENT NUMBER – 00287693T**

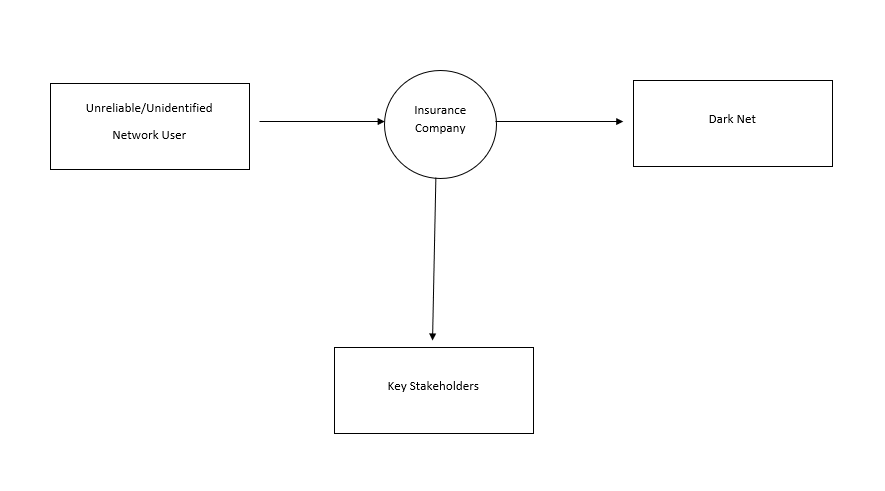
**LECTURER: 1. DR.SHAHRZAD SAREMI**

**2. DR.AZAM SHIRRAFIARDEKANI**

**TRIMESTER 3(2020)**

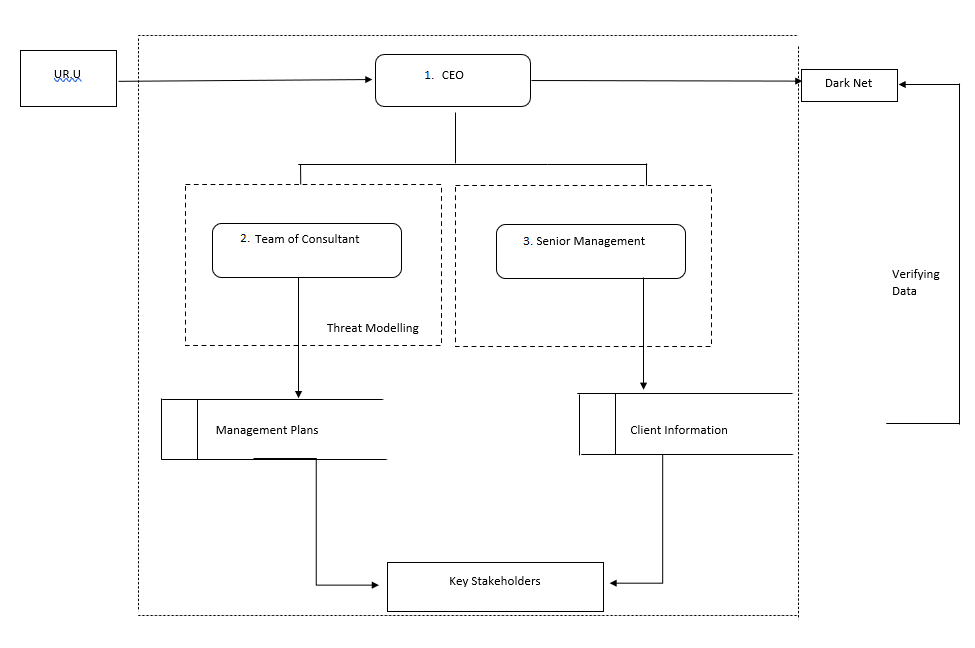
**Introduction:**  The below report describes about the data flow diagrams of the B&C insurance company along with its description. The report also illustrates about the various types of threats and also about the concept of threat modelling. A brief illustration of the STRIDE method of threat modelling has also been described in the report along with the tables for better understanding.

**Context diagram:** Context diagram is an important tool of modelling of various functions. It allows an individual to represent the highest level of model of the system that already exist,defining the interest of the system which is present at the centre along with its boundaries and interactions with the various elements present within the environment. It does not describe the function present within the system but only the interactions with the elements present externally (Burge, 2011). Tuma et al was the first to identify the flow of information analysis about DFDs labeling the flow of data along with assets and measures of security (Faily & Scandariato, 2020).

The above context diagram represents the unreliable/unidentified network user, key stakeholders and dark net as an external entity, whereas insurance company is the highest level within the system. The flow of data is been represented by the arrows within the context diagram.

**Data flow diagram (Level – 0):**

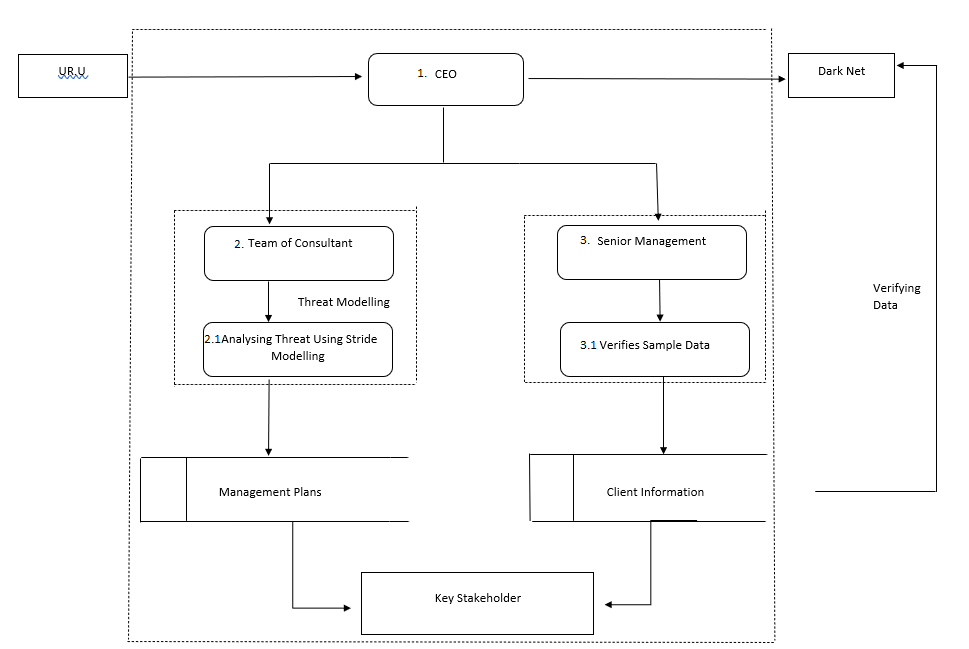
The level-0 data flow diagram depicts the highest level of the process present in the system at the primary level. It represents the information flow from one process to another process and also represents the data store within the diagram (Franchitti, n.d.).



The above context diagram represents the decomposition of insurance company into the CEO which act as main process, whereas the team consultant and senior management act as a source. The flow of data takes place from CEO to the senior management who verifies the client information from the data source along with the dark net. The flow of data also occurs towards team consultant acting as a source who does threat modelling and the plans are store in the data store. Both the data flow occurs towards the key stakeholders acting as an external entity. Their also exist a trust boundary as depicted in the diagram.

**Data flow diagram (Level – 1):**

The level-1 data flow diagram depicts the entire processes that have been shown within the level-0 diagram. It represents the process of higher level in more details. The flow of information is also shown between each process. Level-0 diagram might not be needed to construct level-1 diagram (Jr, n.d.).



The above data flow diagram is further in-depth of level-0 diagram. In which the sources team consultant (2) is decomposed in detail level consisting of analysing threats using stride modelling (2.1) and the process senior management (3) is decomposed into further sub process called verifies sample data (3.1). The flow of information is shown with respective data stores followed by the external entity (key stakeholders).

**Threat:**

Threat is been defined as a malicious event of an agent which might have adverse effect on the system or asset. Every threat has three main attributes: what kind of act, its probability and its impact.

Threat has been defined as two types:

**Internal threat:**

Internal threat might be present within the internal environment of the organization like employees, vendors, contractors etc. These individual might have motive or opportunity to cause the malicious event in the system.

**External threat:**

External threat might be present outside the environment of the organization. The hackers usually use some of the methods like phishing, DDos attack, malware, ransom ware are the methods and virus used by an agent causing effect on the system gaining the access to it (Moschovitis, n.d.).

**Threat modelling:**

Threat modelling is a method to identify the potential threats which consist of vulnerabilities, failure in defence mechanism and building a well-structured security plans to mitigate the risk.

**STRIDE:**

In (1999) Loren Kohnfelder and Praerit Garg developed a methodology called Stride to detect the threats and vulnerabilities (Shostack, 2014).

Stride consists of the following:

* Spoofing
* Tampering
* Repudiation
* Information disclosure
* Denial of service
* Elevation of privilege

Spoofing: Spoofing is a method of presenting themselves in someone’s identity which they are not authorized to

IP spoofing: It is a method of creating packets with false IP address source making the legitimate network thinking of trusted source (Lavanya & Sahoo, 2016).

Tampering: Tampering is a method of changing the information which might be present on the network; memory or it can be present on a disk.

Repudiation: Repudiation is meant as false claiming or denying of being accused of crime.

Information disclosure: It is a threat allowing people to gain access to the information that they are not allowed or authorized to.

Denial of service: It is a threat which makes the legitimate users unable to access the information that they are allowed by exhausting their resources.

Elevation of privilege: It is a threat which makes an unintended user to have access to the information that they are not authorized to (Shostack, 2014).

Threat modelling using **STRIDE** for B&C insurance company:

**Spoofing:**

Process spoofing:

* Creating a software application to save the passwords for any single login attempt of the user.

Filename spoofing:

* Creates a code which will save the user credentials in a file directory which will be stored in a local machine.

Machine spoofing:

* The attacker scan the IP address of the main server and local user server and can make a miss connect between each other confusing both the server and generating the IP address of the attacker as authorized server gaining all the communication in between (pretending both the sides of network channel).
* The attacker can send the IP packets to the main server of company in a disguise of the genuine client which sends back the require information to the client (IP spoofing).

Individual spoofing:

* The attacker can send the local clients email in a disguise of a regional manager or division person.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLES** |
| Process spoofing: | Software application to save passwords | Password saving app |
| Machine spoofing: | ARP spoofing  Internet protocol spoofing | Both the sides network channel  Requesting information in client disguise |
| Filename spoofing: | Saving credentials in file directory | Saving the client information in directory |
| Individual spoofing: | Company employee disguise | Fake emails to access information. |

**Tampering:**

* File tampering can be done in which real file of existing clients can be changed making the file unavailable.
* As the system of the B&C is hacked and information is been stolen they can modify the code making the code hard to defend.
* The process of API ticket to enter the server can also be modified changing the trust boundary.
* Packet tampering can be done in the network flow to the servers making interception in it.
* The flow of data can also be redirected to the attackers to get in the details of the clients.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLE** |
| TAMPERING | File name change (name.exe to name.temp)  Code modification in database  Modification in API gateway  Making interceptions using packets.  Directing the data flow | File unavailability  Unavailable to retrieve code  Loss of security mechanism  Obstructing data flow  Gaining the details |

**Repudiation:**

* Adding the data to the log system to avoid the doubts of the any customer complaints or issues by the company employees.
* Pretending to be the false client claiming to forgot password to gain the credentials.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLE** |
| REPUDIATION | Adding data in logs  Client disguise | Distracting the employees from being noticed  Gaining credentials (forgot the details) |

**Information Disclosure:**

* The attacker can create Sql bugs so that it can gain the access to read the data from the data tables
* The attacker can grab the most information from the logs as each log is been created for every process within the system.
* The B&C operates in multiple countries and flow of the data might also be more, the attacker can analyse data flow to learn secrets
* The attacker can used the method of DNS spoofing to look over the customer chats.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLE** |
| INFORMATION DISCLOSURE | SQL bugs for DB tables  Accessing the logs  Analysing the data flow  DNS spoofing | Accessing DB tables by creating fake queries  Gaining the client information from log directory  Grabbing details from the news about the company and its more concentration in country to analyse the traffic flow of data  To read out the customer chats |

**Denial of service:**

* Making a multiple login of the same user can create more temp files making the process slow.
* The attacker can create multiple fake accounts which can slow down the server making the genuine users unable to access.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLE** |
| DENIAL OF SERVICE | Generating more temp files  More fake accounts | System failure  Slowdown of server |

**Elevation of privilege:**

Against a process:

* As the attacker gain the access can send the packets of code in the server making the server imbalance.
* The attacker can make changes in the code so that he can read and edit any information related to the customer

Tampering the data:

* Data tampering can also be done in the trust boundary allowing the other attacker to get in, defecting the system.

|  |  |  |
| --- | --- | --- |
| **THREAT** | **ATTACKER INTENTION** | **EXAMPLE** |
| ELEVATION OF PRIVILIGE:  Against process | Sending modified codes to server  Altering the code to gain information | Server failure  Gaining client information |
| Tampering data | Allowing more attackers within the gateway | Defecting the system |

**Conclusion:**

The above report describes about the various levels of DFD giving brief description of data flow within the B&C insurance company The report also illustrates about the various threats that the company can face in future perspective helping the key stakeholders to get educated with the types of threats.

**REFERENCES:**

Burge, S. (2011). The Systems EngineeringTool Box. Retrieved from <http://www.burgehugheswalsh.co.uk/Uploaded/1/Documents/CD-Tool-Box-V1.0.pdf>

Faily, S., & Scandariato, R. (2020). Contextualisation of Data Flow Diagrams for security analysis.

Franchitti, J. Session 5 - Main Theme Software Analysis and Design. Retrieved from <http://www.nyu.edu/classes/jcf/g22.2440-001_sp06/slides/session5/g22_2440_001_c51.pdf>

Jr, L. Understanding Data Flow Diagrams.

Lavanya, M., & Sahoo, P. (2016). IP spoofing and its Detection Technique. Retrieved from https://www.researchgate.net/publication/332726965\_IP\_spoofing\_and\_its\_Detection\_Technique

Moschovitis, C. *Cybersecurity Program Development for Business : The Essential Planning Guide*.

Shostack, A. (2014). *Threat Modeling: Designing for Security*.

**LIST OF RECOMMEDATIONS:**

Valacich, J., George, J., & Hoffer, J. (2015). *Essentials of Systems Analysis and Design, Global Edition* (6th ed.). Essex, England: Pearson Education Limited.

Xin, T., & Xiaofand, B. (2014). Online Banking Security Analysis based on STRIDE Threat Model.