Detection and Termination Technology
Use-case representation

By: Hassan Nasser Eldeen.

Signature:

Date of submission: 7/4/2022

Instructor: Dr. Mohamad Elhaj

Signature:

Date of approval:

Note:

Contents

Glossary:

- DTT: “Detection and Termination Technology” a security system aimed at offering protection from attacks in the home network
- DTT Server: the main part of DTT, a computer program that preforms the functions of DTT in the home network
- DTT RCI: “DTT Remote Control Interface” a mobile application offering control and monitoring of DTT Server remotely
- Use-case: a usage scenario for a piece of software
- Use-Case Diagram: a graphical depiction pf a user’s possible interactions with a system
- Use-Case Narrative: a text-based description of a use-case

Introduction:

System introduction:

Advancements in computing has enabled the manufacture more efficient and capable machines, which gave the ability of more integration of imbedded systems in regular everyday items. IOT is taking the world by a storm, and smart devices are inarguably the way of the future, making humans lives more productive, efficient, and easy. IOT devices demand internet connectivity in order to reach their full potential, unfortunately that opens the door for malicious actors and unwanted intruders to access the home network. Due to the low processing capabilities of IOT devices, not many resources are allocated for intruder detection, and threat termination.

"Detection and Termination Technology" is an information system targeted towards solving security problems weaknesses and vulnerabilities in IOT technology, and home networks. DTT aims to offer protection to internet-connected devices; by having command over traffic, flowing through the home network, permitting and denying certain entities from entering the home network, logging network traffic, and representing it in simple and user friendly way to the client.

Detection and Termination technology (DTT) has two main components. DTT server which is the central and pivotal section of the product, and is the part that is present in the client's home network and offers protection from threats. DTT RCI(Remote Control Interface) is a mobile application, that allows the user to be notified of the network activity recorded by DTT server remotely, and it allows the client to configure DTT server remotely.

Purpose:

This paper aims to put the use-cases of the system in more non-expert friendly terms, where it makes understanding the functionality and usability of the system easier. To help none experts more easily visualize the system in operation by the visual cues given to them by the use-case diagrams, and easily understand the flow of operations through narrative use-case representation.

Overview:

This paper is a representation of the DTT (Detection and Termination Technology) network security system, in two ways, a visualizing technique by using use-case diagrams, and a workflow explanation using narrative use-case representation.

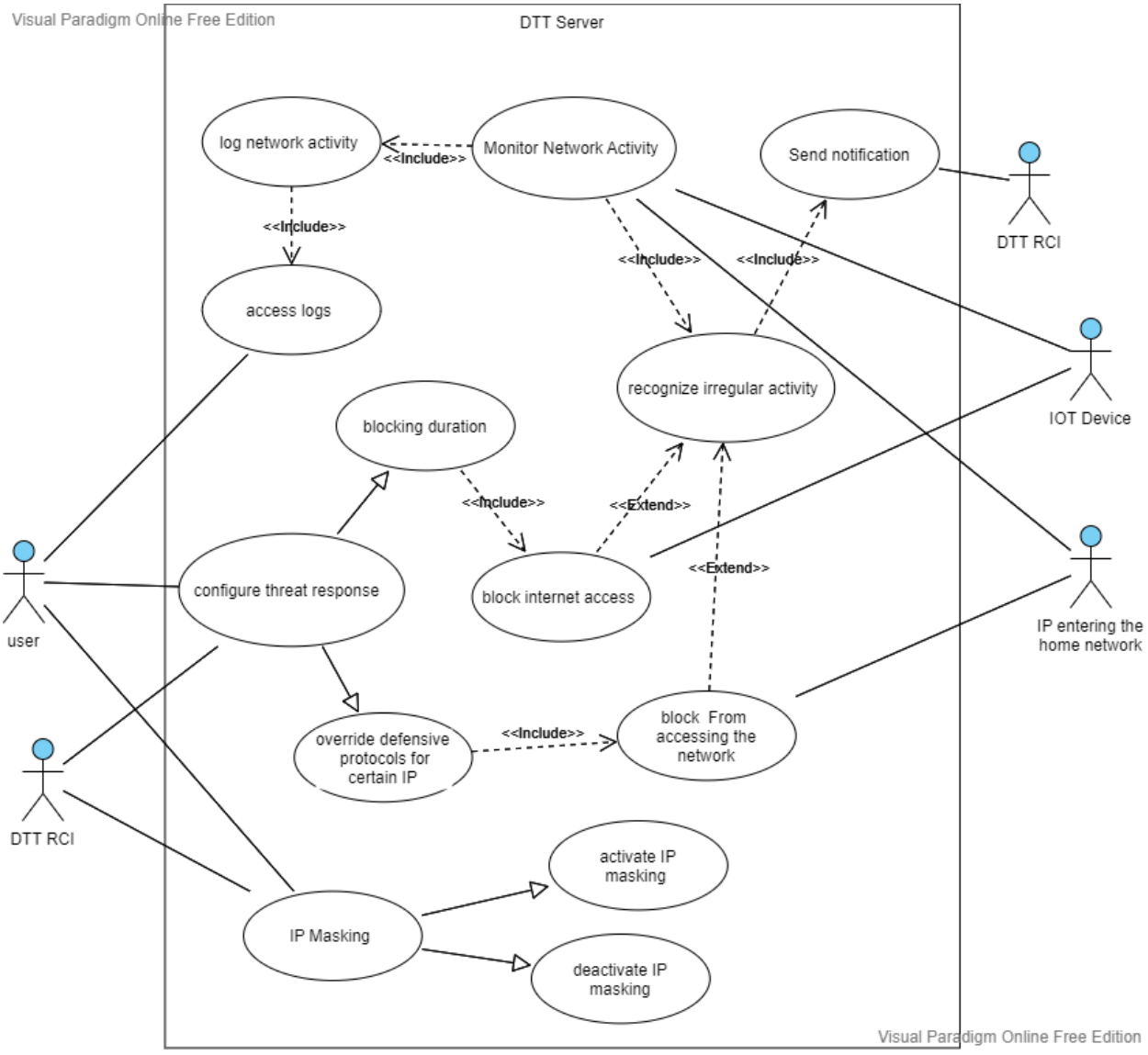
Since DTT has two main components, this paper is sectioned into two parts, one for use-case representation of DTT server, the other is for the use-case representation of DTT RCI.

Each section has use-case diagram, followed by the narrative use-case representation.

Use-case Representation:

DTT Server:

Use-case Diagram:



Narrative Use-case Representation:

Blocking a device from internet access:

Actors:

Main Actor:

- External party

Secondary Actor:

- IOT device

Preconditions:

- DTT server is installed on a machine, and connected to the home network
- DTT server is allowed by the administrator control of network traffic
- Device is connected to the internet
- DTT server configured by the administrator to block internet access of the device in case of a security breach

Event Flow:

- Device is going through regular cycles of network activity
- An external actor starts a connection with the device
- DTT sever checks past logs for recurrences of the external actor
- DTT detects that the external actor is connecting to the home network for the first time
- DTT parses threw the contents of the packets exchanged between the external actor and the device
- DTT discovers unexpected data being transmitted between the two parties of the session
- DTT blocks the Device from Internet access
- DTT keeps a log of all that has occurred including the steps taken by it

Alternative event flow:

- Device is going through regular cycles of network activity
- An external actor starts a connection with the device
- DTT sever checks past logs for recurrences of the external actor
- DTT detects that the external actor has connected to the device multiple times before
- DTT parses threw the contents of the packets exchanged between the external actor and the device
- DTT discovers no unexpected data transmitted between the two parties of the session
- DTT takes no action
- DTT keeps a log of all that has occurred including the steps taken by it

Blocking an IP address from accessing the network:

Actors:

Main Actor:

- External party

Secondary Actor:

- IOT device

Preconditions:

- DTT server is installed on a machine, and connected to the home network
- DTT server is allowed by the administrator control of network traffic
- Device is connected to the internet
- DTT server configured by the administrator to block IP addresses from accessing the network in case of a breach

Event Flow:

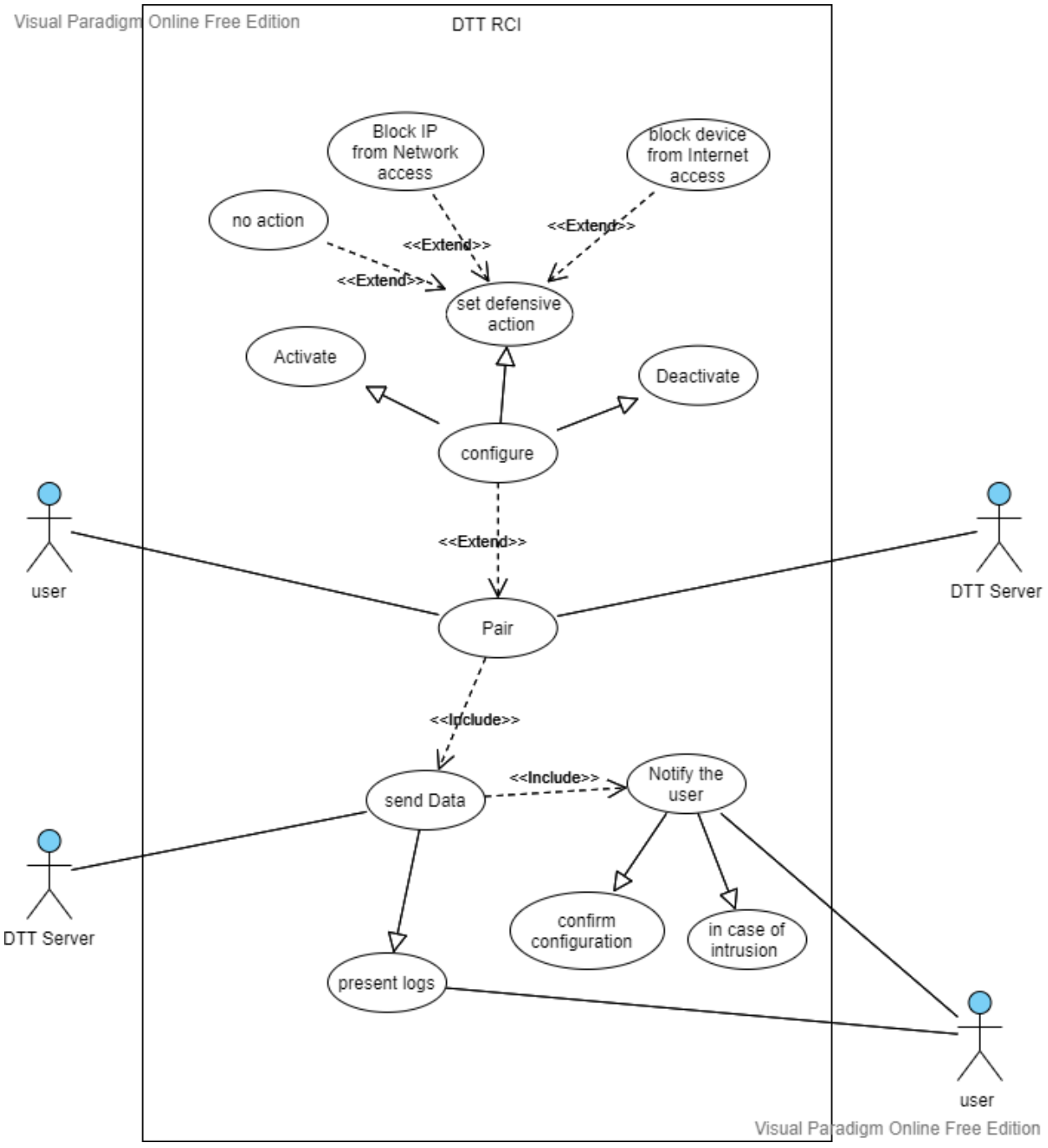
- Device is going through regular cycles of network activity
- An external actor starts a connection with the device
- DTT sever checks past logs for recurrences of the external actor
- DTT detects that the external actor is connecting to the home network for the first time
- DTT parses threw the contents of the packets exchanged between the external actor and the device
- DTT discovers unexpected data being transmitted between the two parties of the session
- DTT blocks the external actor's IP address from entering the network
- DTT keeps a log of all that has occurred including the steps taken by it

Alternative event flow:

- Device is going through regular cycles of network activity
- An external actor starts a connection with the device
- DTT sever checks past logs for recurrences of the external actor
- DTT detects that the external actor has connected to the device multiple times before
- DTT parses threw the contents of the packets exchanged between the external actor and the device
- DTT discovers no unexpected data transmitted between the two parties of the session
- DTT takes no action
- DTT keeps a log of all that has occurred including the steps taken by it

DTT RCI:

Use-case Diagram:



Narrative Use-case Representation:

Pair DTT Server with RCI:

Actors:

Main Actor:

- User

Secondary Actor:

- DTT Server

Preconditions:

- DTT server is installed on a machine, and connected to the home network
- DTT Remote Control Interface should be installed on user's mobile device
- Both DTT Server and DTT RCI should be connected to the same network
- DTT Server should be configured to accept pairing

Event Flow:

- The user presses the pair button in the RCI graphical user interface
- RCI starts roaming the network for DTT server
- A connection gets established between DTT server and DTT RCI
- DTT server prompts to user the user to confirm that they are trying to connect using the remote control interface
- User confirms identity
- Paring process between DTT server and RCI is completed

Alternative event flow:

- The user presses the pair button in the RCI graphical user interface
- RCI starts roaming the network for DTT server
- A connection gets established between DTT server and DTT RCI
- DTT server prompts to user the user to confirm that they are trying to connect using the remote control interface
- User does not confirm identity
- DTT server closes the connection with DTT RCI

Configure DTT Server remotely:

Actors:

Main Actor:

- User

Secondary Actor:

- DTT Server

Preconditions:

- DTT server is installed on a machine, and connected to the home network
- DTT Remote Control Interface should be installed on user's mobile device
- Both DTT Server and DTT RCI should have an internet connection
- DTT Server should be paired with RCI

Event Flow:

- The user enters the configuration menu in DTT RCI
- The user choses between default presets or choses to make a custom preset
- the user choses custom preset
    - User can choose blocking device from internet access
    - User can choose blocking malisons actor from accessing the network
    - User can choose to get notifications when actions are taken
    - User can change profile settings of DTT Server
- After the user finishes the preset choosing process the information is encrypted and sent to DTT server
- DTT Server changes its settings according to what has been sent by DTT RCI
- DTT Server keeps a record of the actions that have been taken

Alternative event flow:

- The user enters the configuration menu in DTT RCI
- The user chooses between default presets or choses to make a custom preset
- The user chooses one of the default presets
- After the user finishes the preset choosing process the information is encrypted and sent to DTT server
- DTT Server changes its settings according to what has been sent by DTT RCI
- DTT Server keeps a record of the actions that have been taken

Conclusion:

The use-cases of DTT might not be vast, its functionality might not be overarching, but it accomplishes its aim of protecting the home network from unwanted external actors and intruders. DTT with its targeted functionality on threat detection and termination provides the user with what they need without a lot of unnecessary bloat that could make the user experience complicated. The use-cases of DTT and the way its two part interact are simple, clear, and easy for uninitiated user to understand, expanding to user base to those who need it the most.