

Bachelor Thesis

DESIGN AND IMPLEMENTATION OF CCEAP USER INTERFACE

Bachelor Thesis Submitted as Partial Fulfilment of the
Requirements for the Degree of B.Sc. in Applied computer
science at the University of applied sciences (Hochschule Worms)

Feugang Kemegni Fabrice

Submitted Summer, 2017
supervised by Prof. Dr. Stephen Wendzel

Applied Computer Science
Software construction

Declaration of Authenticity

I hereby declare that all material presented in this document is my own work. I fully and specifically acknowledge wherever adapted from other sources.

I understand that if at any time it is shown or proven that I have intentionally misrepresented material present here, any degree or credits awarded to me on the basis of the material may be revoked.

I declare that all statements and information contained here is true, correct and accurate to the best of my knowledge and belief.

Ludwigshafen, Summer 2017.

.....

Feugang Kemegni Fabrice

Abstract

This Bachelor thesis discusses the development a graphical user interface program as an interface to a command line program called CCEAP.

CCEAP (Covert Channel Educational Analysis Protocol) is a protocol in the form of a program to help teach covert channels and hiding patterns.

The cceap program is currently executed from the command line, by starting a cceap-server program on a given port of a computer, then on another command line starting the cceap-client program with the IP address and port number of the computer where the server is running. The client is started with some other parameters that correspond to the cceap's protocol settings.

This thesis discusses the implementation of a graphical user interface to complement the command line tool so as to increase the usability of the overall cceap.

The first section of this thesis is a background discussion of what cceap is and the related concepts connected to it. Additionally brings some background information required to understand the purpose of cceap. Then discusses some limitations that lead to the need for a complementary graphical user interface.

The second section discusses the implementation of the Graphical User interface tool, the reasons that lead to the need for a GUI, the specifications and requirements of the GUI tool. Then a complete discussion on the implementation of the GUI tool

The third section discusses some problems/issues faced during the implementation of the program as well as the solutions to some of the problems.

This section is followed by a section on extensions to the GUI tool. This refers to the features that could be added to the program during future development potentially by other students that might be involved in the evolution of CCEAP.

Table of Contents

Bachelor Thesis.....	1
Declaration of Authenticity.....	2
Abstract.....	4
Introduction.....	6
What is CCEAP.....	6
Covert Channels and Hiding patterns.....	6
CCEAP.....	6
How does CCEAP function.....	7
Running CCEAP on windows.....	7
Running CCEAP on Unix.....	7
Limitations of the CCEAP Tool.....	8
What is my contribution to solve the problem.....	9
Related Work.....	10
Design and Implementation.....	11
Programming Requirements.....	11
Design decisions.....	13
Qt Creator.....	14
Problems encountered and Solutions.....	15
Solutions to encountered problems.....	17
How is the GUI implemented, descriptions.....	17
My remark about the implementation.....	17
Deploying the app to windows.....	18
Requirements.....	18
Steps (Hard Code).....	18
Extensions to the application.....	19
Features that could be added to the CCEAP-Gui tool.....	19
Conclusion.....	21
Abbreviations.....	22
Bibliography.....	23

Introduction

What is CCEAP

To simplify the understanding of CCEAP, it is best to first define some of the concepts that are related and basis for understanding the term.

Covert Channels and Hiding patterns

Also called network steganographic hiding methods are techniques used to conceal communications within network traffics. In other words covert channels involve hiding communications in plain sight by using public media(in this case the network traffic) to practice secret communication. Secret communication in the sense that the fact that the communication is even taking place is unknown. There are more than a hundred of such network steganographic methods for concealing communication however as shown in ([Wendzel et al., 2015](#)) these can be summarized into 11 so called **Hiding Patterns**.

CCEAP

With such a brief understanding of what a covert channel in the domain of networking means, we can now jump to what CCEAP stands for and why are its purposes.

CCEAP(**Covert Channel Educational Analysis Protocol**) is a command line tool(program) that emulates an application layer protocol and is designed to help in teaching/learning covert channels.

It is an application layer protocol that uses Ethernet packets payloads as covert channel(the term covert channel is explained above).

The idea behind CCEAP is to provide such a protocol that will allow learners to model/manipulate this protocol's structure with the aim of creating a covert channel.

The main features of cceap is that it is based on hiding patterns ([Wendzel et al., 2015](#)), which is summarizes more than 120 network steganographic methods to only 11. Thus it is an economic approach to learn only these 11 hiding patterns which summarize the hundred methods.

Additionally, cceap combines all methods of hiding data in network communications into a single protocol instead of using each separate protocols i.e. IP, UDP, HTTP, TCP etc. ¹

1 <https://github.com/cdpdx/CCEAP/tree/master/documentation>
<https://www.researchgate.net/project/Network-Information-Hiding-Patterns>
https://www.researchgate.net/publication/316215336_Network_Information_Hiding_and_Science_20_Can_it_be_a_Match

How does CCEAP function

Now that the term CCEAP has been explained, an explanation on how it functions should be discussed.

The CCEAP tool is a cross platform command line tool that runs on windows, Unix Linux and MAC OS.

Detailed explanations on the installation steps and other Instructions on running the CCEAP tool together with some practical exercises to demonstrate the functioning of the tool can be found on this webpage [CCEAP documentation](#). However here is a shorthand oh how to run the tool on the most widely used operating systems.

After downloading cceap from <https://github.com/cdp xe/CCEAP.git> into a folder on the computer, follow the steps below depending on the architecture.

Running CCEAP on windows

- open a command line tool cmd
- navigate to the folder where the CCEAP tools are stored i.e cd /path/to/CCEP/Folder
- start server.exe -P 1234
- start client.exe -P 1234 -D 127.0.0.1

Running CCEAP on Unix

- open shell (Terminal)
- with the terminal, navigate to folder where CCEAP program is stored
- start server ./server -P 1234
- start client ./client -p 1234 -D 127.0.0.1

In the example above, **-D** is the Port number, which must be the same for clien and server,

-D is the IP address of the computer where the server is running, if you are running the client and server on different computers, you need to replace the 127.0.0.1 with the actua address of the computer where the server is running.

Visit the CCEAP website for more details about the parameters and explanations [User CCEAP command Line tool](<https://github.com/cdp xe/CCEAP/tree/master/documentation>)

Limitations of the CCEAP Tool

After having tested the cceap tool, its relevance and support in understanding covert channels becomes obvious as it provides a practical way to visualize some of the concepts of hiding patterns and covert channels.

However, for non-computer users or even the novice ones that are not familiar or those who find the use of the command line or **cmd** or terminal uncomfortable, it becomes apparent that something could be done to increase the usability of cceap.

Below are some aspects of cceap that could reduce the motivation of learners when using cceap to learn hiding patterns and covert channels.

CCEAP is not a graphical program but instead a command line tool. For the computer novice or non-programming users, or even some computer people but who are not in love with working with the command line, it becomes a drawback to work with cceap.

Another point is the fact that it becomes difficult to follow the flow of the program from begin till end and to interpret the program's output from the command line.

Even advanced users will find it difficult to interpret the output of the cceap server when it is displaying a hundred packets.

The outputs in the server are displayed one line after the other which is simple to understand when only about 10 to 20 packets are being analysed. Of 20 packets when the screen offers enough room for that. However, when the server's output is a large number of packets and parameters, it becomes strenuous to follow.

Another drawback of the command line is the inability to undo and redo when entering parameters.

The command line reads parameters line after line, so it is difficult to undo/redo in such an environment.

The program parameters are not very understandable for novice users even when reading the help section. This tool is easily understandable by experienced users, however, casting out the novice who are part of the intended audience.

The command line tool is relatively complex and each system has its own independent command line tool that is used differently from other systems. Thus, having knowledge or being experienced with the Windows command line tool does not guarantee the same knowledge could be applied to a Unix command line tool.

Above are only some points that describe the main limitations of the CCEAP. Faced with these, a need to extend features to complete these holes have generated a need for a graphical user interface to interface this command line tool, facilitating the use of the cceap.

The section below describes my solution to this, in the form of a graphical user interface for the command line tool.

What is my contribution to solve the problem

The above section discussed the little limitations of the CCEAP tool that need to be addressed in some way. Faced with these limitations of the tool, I will attempt to provide a durable solution in the form of a **GUI** tool.

This is a graphical program that offers an interface between the command line tool(CCEAP) and the user. The user interact with the GUI and the GUI translates the user inputs into program parameters for the cceap tool.

Such a tool is quite straight forward in requirements and specifications as it is an interface in-between users and the program, permitting users to understand the program parameters and facilitating the understanding and interpretation of the program's output.

Below is a list of the specifications that the finished program should fulfil among other specifications.

The program should be highly usable graphical program, that is intuitive to use so as to facilitate users understanding and interaction.

The GUI should also present the cceap's program output in a clear, understandable format to users.

The program should be highly transportable and usable. This means that the program should run on possibly several platforms i.e. Unix, windows MAC OS etc. without requiring any effort. This implies a meticulous choice of programming tools.

The program should be smart and robust in terms of dealing with users inputs. User's inputs that do not make any sense should not lead to system fail but instead the program should identify the erroneous input and notify the user with the appropriate action to take. In this way helping in the learning process of covert channels and hiding patterns.

The users should be presented the program's output in a format that will be easy to understand and interpret, thereby helping in teaching and increasing the usability of cceap.

Related Work

Cryptography- the science of communicating secret messages in public media is a broad topic with multiple branches and concepts.

Steganography on the other hand focusses on hiding the content of a communication in public, in other words it is the science of privately communicating in public.

This approach sounds contradictory at first hearing but once one has read the available documentation rapidly finds the.....

One of the main branches of steganography being covert channels focusses on the usage of public innocent communication media to communicate secret data in a manner that is unnoticeable if not unidentifiable manner.

One simple way of using covert channel is in the domain of networking(computer networking). Here an underlying protocol for Ethernet communication namely TCP-IP is been used as a covert channel to communicate information illegally using Enet Packet headers. For example

.....

- solutions that are already available
- what is already out there
- the goal is not to reinvent the wheel, instead
- show other scientific publications

Design and Implementation

This chapter discusses the implementation phase of the GUI tool.

Programming Requirements

To implement this GUI-Tool, I have made use of a variety of concepts, tools and other programs. Among some of these

- QT creator as IDE: for developing the layouts and to organize and structure the code. The reasons for selecting QT creator among the hundreds of other tools are discussed below.

- Git for version controls and history management.

Git is the most widely used version control framework today and is taking over the tasks of versioning, document and clouding programs.

Together with its associated tool GitHub, provides an intuitive approach to even beginners in programming. There are several other frameworks that implement version controls but most of them in one way or another make use of concepts from git. An example of such a framework is source tree[source tree](<http://sourcetree.org>)

- gcc, qmake, cmake, to compile

- OS

- ubuntu

- windows

It was imperative to work with 2 operating systems because one of the main features of this tool is its portability and transportability.

Transportability in the sense that program, both source code and executable should be easy transportable among platforms.

As main operating system I used ubuntu 16. and then each time transported the program to my windows platform to generate windows executable .exe files for windows distribution.

In the section **deployment** below, I explain how this process of writing the program under platform and the generating a distributed version of the program for another platform.

Deployment is often done in the target platform, i.e. to get the windows executable can only be done on a windows platform and the Unix version on a Unix platform respectively.

Why Qt Creator is a cross-platform C++, JavaScript and QML integrated development environment.

QT creator comes with several useful programming resources including

- a visual debugger
- an integrated GUI layout and forms designer.
- syntax highlighting and autocompletion in editor's features.
- C++ compiler from the GNU Compiler Collection on Linux and FreeBSD.
- On Windows it can:
 - use MinGW or MSVC
 - Microsoft Console Debugger (when compiled from source code).
- Clang.

Due to these features, it became intuitive to choose it as the development tool.

Design decisions

I started writing the program in the Java programming language due to the fact that Java is a highly portable programming language, it is one of the languages that I know the most and I have gathered some experiences through homework and projects in school.

By saying a highly portable language, I refer to the fact that a program written using a Java language on a given system can be exported to other systems without any strenuous operation.

This is because Java programs are not technically compiled to produce a static compiled output, but instead programs written in the Java language are translated from the high level code of programming language into a java machine language(dynamic code). This java machine is called the Java virtual Machine (JVM).

To be able to transport a program from an architecture (source architecture) to another architecture(target architecture)) the only requirement is the presence of the JVM and JAVAC on the target architecture.

Both the JVM and JAVAC are open-source programs available

<https://www.java.com/en/download/>

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

the system architecture only requires a JVM (Java virtual machine) running in background

- javac JRE
- java JDK
- Eclipse
- Window Builder plug-in for Eclipse
- Windows System
- Ubuntu/any Linux distribution for testing
- virtual box for virtualisation in case only one architecture is available

After more than one week implementing the CCEAP-GUI program in java language, I came to a deadlock and realised that I could not implement such a program using java. The reasons being that the following.

In order to be able to place the UI controls on the screen in the desired positions, the container in which such UI controls would be placed needed an absolute layout such that items(UI-controls) can be placed on the container independent of the positions of the other ui controls already on the container.

However java GUI containers i.e. AWT and swing do not offer absolute layouts but relative layouts, such that an item can only be placed relative to the others, for example in a table or on bordered layout. This was a very serious problem that pulled me back on research.

Another reason for abandoning java in the project was the absence of a designer mode in the most Java programming IDEs. Using the open source eclipse, the only alternative was using plug-ins such as Windows builder, but this plugin was very slow and kept on freezing.

Faced with these problems, I was forced to switch to an alternative language, and after some research I came to choose C with QT creator. This solved my problem of UI designing.

Qt Creator

Qt Creator is a cross-platform IDE supporting the languages C/C++, JavaScript, QML. QT Creator offers features like a visual debugger, an integrated designer for GUI layout and forms. The editor's features include syntax highlighting and autocompletion.

Qt Creator provides support for building, deploying and running Qt applications for desktop environments including Windows, Linux, FreeBSD and Mac OS.

QT creator also provides programming applications for mobile devices including Android, BlackBerry, embedded Linux devices and several others. Build settings allow to switch between build targets, different Qt versions and build configurations.

QT Creator is available under <https://www.qt.io/ide/>.

Problems encountered and Solutions

The program implemented during this project was a simple and quite easy understand. However the implementation was characterized by lots of problems encountered mostly due to the fact that I was familiar to the programming environment and my lack of experience with such types of programs.

At the end most of the problems were solved despite taking relatively much time to be dealt with. Among some of the problems that I faced, the following are the most prominent and are those that required much time.

I started writing the program in the Java programming language due to the fact that Java is a highly portable programming language, it is one of the languages that I know the most and I have gathered some experiences through homework and projects in school. Although I carried out some research on the portable languages to fit the tasks on hand but at some point this research was biased by the fact that I already knew java, so I jumped into implementation and spent about 15% of the whole time for this project on a wrong path.

It is extremely difficult to use Java SWING and AWT classes as means of developing complex User Interface programs.

Although the SWING and AWT widgets are designed to create UI programs, they are better appropriate for some tasks than some others, for my task they were not appropriate. These classes are appropriate for UI such as calculator, video player, etc. where a.

For the CCEAP, the available containers apply useless because some items need absolute positioning on well defined coordinates, whereas AWT and SWING containers only offer Border layout and flow layouts.

Executing an application from QT, and making system calls. The second problem and one of the most time consuming problems was making a system call from the GUI program to starting both the CCEAP client and server.

I have stayed on death lock for more than a week trying to run the server and client program from the GUI app using the parameters that the users entered in the latter.

Each of the approaches that I used didn't work and each time I ran the program nothing noticeable happened, at best when I closed the program a debug message said, client program started and is still running although the GUI app had already exited.

Dead-lock with server freezing while waiting for data. After the above problem was solved, I immediately found myself with another death-lock. This happens when the server GUI is started and waiting for clients, after waiting for some time without receiving any client data, the server freezes and only unfreezes once a client has connected and sent some packets. The server GUI then unfreezes and displays the programs output from the CCEAP.

The last but not the least problem was that of live communication between the CCEAP GUI and the CCEAP app. This is not considered as a problem because it was not included in the programs backlog. It was just intended to be a feature of the initial GUI app but instead it is an extension that I have left behind for the future students that will continue the development of this application.

The feature consists in that, the server GUI should display live output from the server program as it

is been outputted. Currently, the GUI displays the programs output once the cceap server has exited. It would be a nice feature to have the cceap server's output lively displayed on the GUI. I am not sure that it is possible to have such output but this research was out of the scope of my thesis, so I left this task for the future developers of the CCEAP. Nonetheless, I have spent considerable time researching on how to implement this task.

Solutions to encountered problems

Faced with this problem, I was forced to abandon Java and search an alternative solution, thus QT appeared the next best solution due to its portability, as programs written on QT on either architecture, can be easily compiled in another architecture.

With QT, design is relatively simple, items are placed on the container through a simple drag and drop.

How is the GUI implemented, descriptions

sketches

wire frames

mock-ups

CCEAP GUI is developed with QT creator, because it appears to be the best alternative to develop such a GUI program, because

UI controls are easily placed on the window container as compared to the Java alternative. This is because QT creator allows drag and drop of UI Controls on desired positions of the container(Window), as compared to Java where containers are constraint in Layouts, for example a Border layout only allows a ui control to be placed at the left of the previous

pcontrols.

...

....

My remark about the implementation

Despite all the planning that I went through, i have come to learn that, practice is a different topic from theory.

- Problems encountered during the implementation
- Good Things about the tool
- Drawbacks/bad about the tool

Deploying the app to windows

This section describes how to create an executable file for the windows platform. In order words how to run the program on windows in case the application does not provide a windows executable file. The following link offers more detailed information on how to deploy a program developed in QT creator to different target architectures [Deploy an Application on Windows] (http://wiki.qt.io/Deploy_an_Application_on_Windows).

Requirements

- The release version of your app works correctly when you build + run it from Qt Creator
- Qt is installed in C:\Qt\5.2.1\mingw48_32\
- This also applies to
- Qt 5.6 and mingw49_32

Steps (Hard Code)

1. Close Qt Creator.
2. Create a folder to hold the app eg ~\MyApp\
3. cp \QT\Projects\MyApp\MyApp.exe ~\MyApp\
4. cp C:\Qt\5.2.1\mingw48_32\bin*.dll ~\MyApp\
5. cp from C:\Qt\5.2.1\mingw48_32\plugins* ~\MyApp\
6. cp C:\Qt\5.2.1\mingw48_32\qml* ~\MyApp\
7. Test if deployment worked
 1. mv (rename) C:\Qt C:\QtHidden\ (This turns your PC into a clean environment, just like one that doesn't have Qt installed).
 2. ~\MyApp\MyApp.exe
 3. if it works then perfect
8. Cleanup
 - start ~\MyApp\MyApp.exe
 - while ie running,
 - rm ~\MyApp* and skip eroneous files.(this will delete only unnecessary dll files)
9. restart ~\MyApp\MyApp.exe
 - it it works, then the app can be distributed.

Extensions to the application

The problem statement of this thesis requires the development of a GUI tool that provides interface to interact with the CCEAP command line program.

The basic requirements are the simplicity and portability of the program. Portability in terms of the possibility and ease with which the program can be ran on different operating systems and architectures.

The requirements of the program are quite clear and the required features have totally fulfilled.

However, during and after the implementation, I have come to identify some features that could be added to this GUI tool. These features I have called extensions as it is often done in computing to mean features that could be added to an existing program to extend the programs functionalities. Below I have listed some of these functionalities, and these are intended to be developed in the future by students who will continue the development of CCEAP.

Features that could be added to the CCEAP-Gui tool

The first feature will be an Export command. This could be extended to the clients GUI so that once a session with all input parameters for a purpose will be used, these settings could be exported to an external file in JSON, XML, CSV, oData or any other format. , so that next time the user do not need to re enter such parameters but can open the file in which these settings were saved and directly copy from there into the GUI.

This will increase the overall usability of the program.

As a further extension to the above extension, could be the introduction of an import feature, this permits users to directly import settings from a file into the GUI program. This is very practical when for example a client starts an analysis session with 100 packets giving each packet a sequence number. Even though these 100 sequence numbers might have been saved into a file, typing them into the program is quite strenuous and time consuming. Export and Import features have been separated because each export might not absolutely require and import. The user might just need to save settings into a file without forcedly needing to import them.

Live communication between UI tools and programs: This feature should permit data to be displayed on the GUI while the cceap program is performing actions. Currently, the GUI starts the CCEAP program with the parameters entered by the user, then only display the returned output of the cceap after the latter has exited.

The idea here is to display the cceap's output while the latter is running, not simply displaying the latter's output after it exits.

I have not researched on this much because it was out of the scope of my thesis, so I left it behind for future developers.

A further feature but this time the starting point will be testing the GUI and CCEAP on load tests. The tests that were carried during and after implementation were functionality tests to ensure that the programs behave as expected independent of user's inputs and systems architectures.

All tests (both systems and functional) returned positive as the program recognises user's input errors and handles them as expected. After all tests, no known bugs have been identified.

The task here will be to test both cceap and the corresponding GUI tools on their behaviours when faced with overloads for example sending a thousand packets.

These have not been tested because thousand packets as parameters go out of the scope of CCEAP as students might not need to analyse a thousand packets in a session while learning covert channels.

The necessity to test appears now because as CCEAP becomes widely used, several users might have to connect to a single server, the behaviour of the server in response should be tested.

Conclusion

The aim of my thesis has been to implement a GUI (Graphical User Interface) program as a tool for an existing program (CCEAP tool).

The importance of this work lies not only on the program, but also on the application of the concepts that I have acquired during my undergraduate studies. I would like to emphasize on the fact that the application developed in this project is only for an academic purpose, a lightweight GUI-tool with the sole purpose of providing a Graphical User Interface to the already existing command line CCEAP program.

It is not intended for commercial purpose but instead to serve for academic purposes especially to contribute in learning/teaching network steganographic hiding patterns.

This program has not been extensively been tested, due to the fact that there is no immediate need for testing, as the development will be continued by other students like me, who should focus on testing before building from my foundations.

Developing this application has provided me the opportunity to carry out some amount of academic research. During this development, I have come across several difficulties and problems, but with some efforts I have been able to overcome them or find away around.

In the Chapter Related works, I describe some related works, projects and tools that till now provided alternative solutions to the problem that i solved in this project.

In the chapter Implementation, I try to describe the steps that i took in implementing the app. I also attach the Git repository where the project is hosted, with a detailed git log, that could be followed to understand the historic of the development.

In the section 'problems encountered, i list some of the difficult that I encountered followed by my solutions and some advices to other programmers that may come across similar problems.

The chapter extensions describe a list of tasks and features that students that will continue the development of CCEAP should first implement so as to keep

Abbreviations

- JRE: Java-Runtime Environment
- JDK: Java-Development Kit
- SDK: Software Development Kit
- IDE: Integrated Development Environment
- CCEAP: Covert Channel Educational Analysis Protocol
- U: User Interface
- GUI: Graphical User Interface
- OS: Operating System
- Enet: Ethernet
- TCP: Transmission Control Protocol
- TCP/IP: TCP+ Internet Protocol
- OS: Operating System
- Javac: java compiler
- JVM: Java Virtual Machine
- QML: Qt Meta Language/Qt Modelling Language
- XML: Extensible Markup Language
- oData: Open Data source
- CSV: Comma Separated Values
- JSON: JavaScript Object Notation
- CMD: Command Line tool
- IP: Internet Protocol
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- HTTP:

Bibliography

[this publication

(https://www.researchgate.net/profile/Steffen_Wendzel/publication/263773592_Hidden_and_Uncontrolled_On_the_Emergence_of_Network_Steganographic_Threats/links/53eb38eb0cf2dc24b3cea87a.pdf).

[Hidden and Uncontrolled - On the Emergence of Network Steganographic Threats]

(https://www.researchgate.net/publication/263773592_Hidden_and_Uncontrolled_On_the_Emergence_of_Network_Steganographic_Threats).

[Hiding patterns](<http://ih-patterns.blogspot.de/p/introduction.html>)

[CCEAP-Master](<https://github.com/cdp xe/CCEAP>)

[An Educational Network Protocol for Covert Channel Analysis Using Patterns

(<http://dl.acm.org/citation.cfm?id=2989037>)

[This Thesis] (<https://github.com/fabrig eas/bachelor-thesis/>)

[User CCEAP command Line tool](<https://github.com/cdp xe/CCEAP>)

[Javac] <http://www.oracle.com/technetwork/java/javase/downloads/index.html>

[JVM] <https://www.java.com/en/download/>

[QT Creator] <https://www.qt.io/ide/>