CENG 491

Senior Design Project Proposal

Company Name : ESSOFT

Members of the Team

ARDA GÜÇLÜ 1395052

AKİF GENCAY DEMİREL 1394915

KEREM OZARKAN 1395300

MÜJDAT BAYAR 1394725

Project Topic

Auto-Identification/Classification of Common IP Protocols

Definition of Project

Well-known TCP and UDP ports are used to deliver widely used IP based protocols such as HTTP,SMTP,YMSG,SIP,FTP etc.In some cases, any non-standard ports can be used.Our project aims to be able to identify which protocols are delivered through any TCP or UDP port including non-standard once.

Specifications

In this project we are expected to control the non-standart data flow through any port. Because of this we will be capturing the data flow through any port. Data will be taken as PCAP file format, which is used to capture network traffic and it is the format used by the tcpdump program.After taking the data, PCAP files will be read and sent to decoder.Our project starts here.This phase is namely Autosensing which will classify the protocols.

To be more spesific, pcap files will give us the information that is transmitted and because we don't know which protocol is used in any non-standart port, we will try to identify this

information. To do this, we plan to look at the format of the protocols. Looking their headers or any protocol-specific keyword or anyting else, we will guess the protocol correctly and take the other step. Our algorithm is expected to identify these protocols by examining patterns formatted by RFC(for every protocol, there is a RFC format). In this step the hard part is that we will be doing this in real-time.

The next step will be storing the transmitted information knowing the used protocol. Of course we will be storing the data before identifying it. After identifying we will be able to return back and get all the transmitted data.

In final phase, identified data will be saved in database and it will be monitored according to its own format. The monitoring will be easier because the protocol is known about the stored data. In this part not all users will be permitted to monitor the data. This part will be arranged accourding to permissions.

Furthermore, the implimentation will be done by using c++.

Expectations

At the end of this project, we expect to identify and classify commonly used protocols and also to identify complex protocols if we can succeed.

Expected grades of members of the Team

ARDA GÜÇLÜ BB

AKİF GENCAY DEMİREL BB

KEREM OZARKAN CB

MÜJDAT BAYAR CB