CS 6349 Network Security Fall 2013

Programming Project

Implementation of Secure File Transfer System

Initial Description

In this project, you have to implement a secure file transfer communication system in which only authenticated client can download data from a trusted file server. In the following figure, suppose Client wants to download a file from an Enterprise Department File Server (ex. Marketing Dept., Finance Dept., Payroll Dept. etc.). These file servers are not accessible directly from outside because Client doesn't know the address of these Enterprise Department File servers. That is why Client can't directly communicate with Enterprise Department File Server. But Client can directly communicate with the Enterprise Master File Server which is accessible from outside of the Enterprise network. In this project, this Enterprise Master File Server will work as a relay server which will help Client to download files from the corresponding Enterprise Department File Server. But before communicating with the Enterprise Master File Server; Client needs to validate itself as an authenticated user of that department. So, Client has to authenticate itself via Authentication Server. After verifying Client as an authenticated user, Authentication Server will then generate some session keys which the Client, Enterprise Master File Server and Enterprise Department File Server will use to communicate with each other to continue the file downloading session.

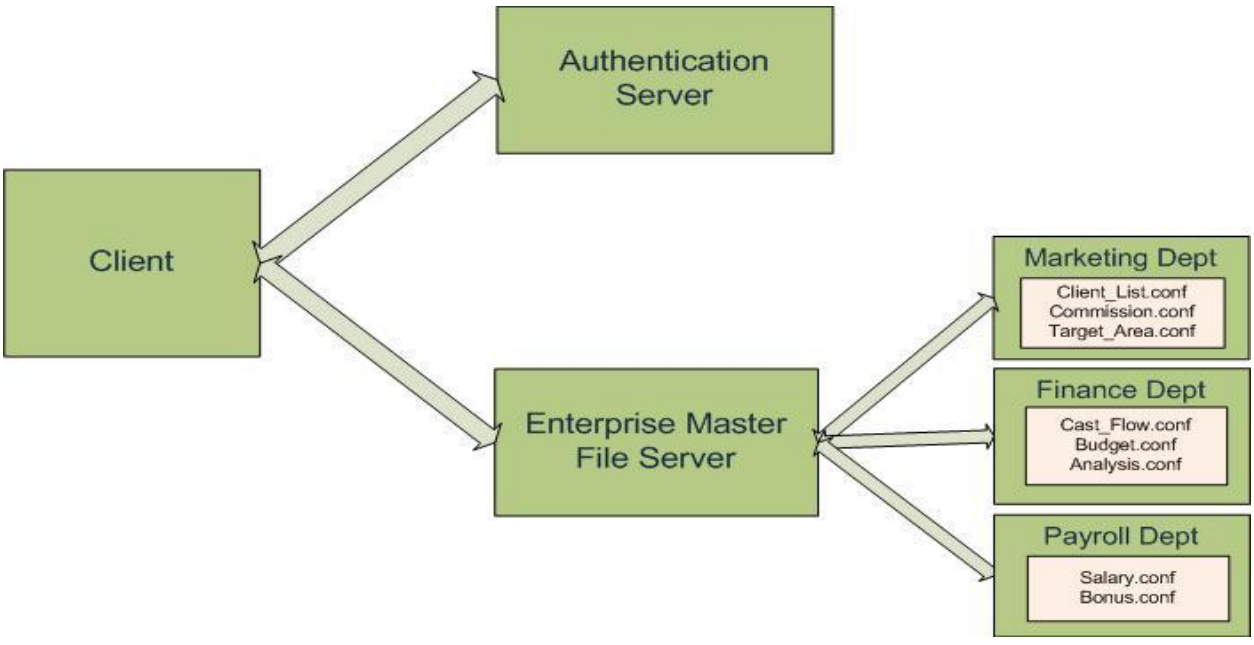

Figure: Components of Secure File Transfer System

There are four components in this communication system:

1. Client
2. Authentication Server
3. Enterprise Master File Server
4. Enterprise Department File Server (Marketing Dept., Finance Dept. , Payroll Dept. etc.)

Enterprise Department File Server contains all the confidential files of that department. Only the authenticated client can download those files. Enterprise Master File Server can facilitate the communication process. But this master server should not be able to decrypt any of the file contents what Client is downloading. Client also needs to be authenticated by the Authentication Server. After authentication process, Authentication Server will generate tickets and give it to the Client for the file downloading session. Client will then contact with Enterprise Master File Server. The master file server will verify clients' identity and the authenticated client's request will be forwarded to corresponding Enterprise Department File Server. This department file server will verify identity of the Enterprise Master File Server, Client as well as Authentication Server. After that communication will start between client and department file server relayed by the Enterprise Master File Server. You need to make sure that Client can also verify the identity of valid Authentication Server, Enterprise Master File Server and Enterprise Department File Server. In this communication process, Enterprise Master File Server should not be able to decrypt any communication message.

Goal:

1. Authentication: Each of the components should be able to authenticate each other.
2. Message Integrity/Consistency: Integrity of the message transmitted between different components and within insecure network should be protected.
3. Privacy/Confidentiality: Ensure confidentiality in the communication process.

For this project, you may work in groups of up to 3 students. Each team is required to submit a plan-of action document that will include details about the implementation of the project as your team interprets it. Each team will present their presentation as a discussion with the TA to ensure that they have understood the scope, goals and expectations of this project.

NOTE:

1. The deadline for submission of the plan-of-action document is November 4, 2013. This document will carry 10% of the project grade.
2. You may use C/C++ or Java for the implementation of this project.
3. You have to use UTD net machines to show the demonstration of the project.

Submission guideline:

1. Each team has to submit their source code and a readme file.
2. You have to show the working of at least one client, one Authentication Server, one Enterprise Master File Server and two Enterprise Department File Servers.
3. Display the messages sent and received on each component.
4. After downloading the file from the server, Client needs to show the contents of the file locally.
5. Each team member should be able to answer the questions regarding the code and the design protocol.
6. You have to show the demonstration in UTD net machines where each of the component will be in different net machine.