Secure QoS Unified Access

Project Report

CS591-F2005

-Sujeeth Narayan

-Ankur Patwa

-Francisco Torres

ABSTRACT:

This document proposes a system where information classification takes place and is transferred securely and quickly amongst users. The document is replicated only when necessary and alerts/notifications are provided on reception of a document, which has to change hands very quickly.

INTRODUCTION:

With the fast development of the Internet, there arises a need to stop eavesdroppers and intrusive people from access of personal documents. There have been many occurrences where some one has hacked into a system to get private data and/ or change data. Information replication being easily done in its electronic version, there is a need to restrict read access along with write/ modifies permissions to information. We researched a system where we cannot only exchange data securely, but also we can guarantee that the document is given importance in terms of fast transfers and transferred urgently. Moreover, we ensure that the document is replicated at right place and time to avoid transfer delays and unnecessary usage of network bandwidth.

The next section explains the proposed setup. The scenarios where the documents will be transferred are discussed next.

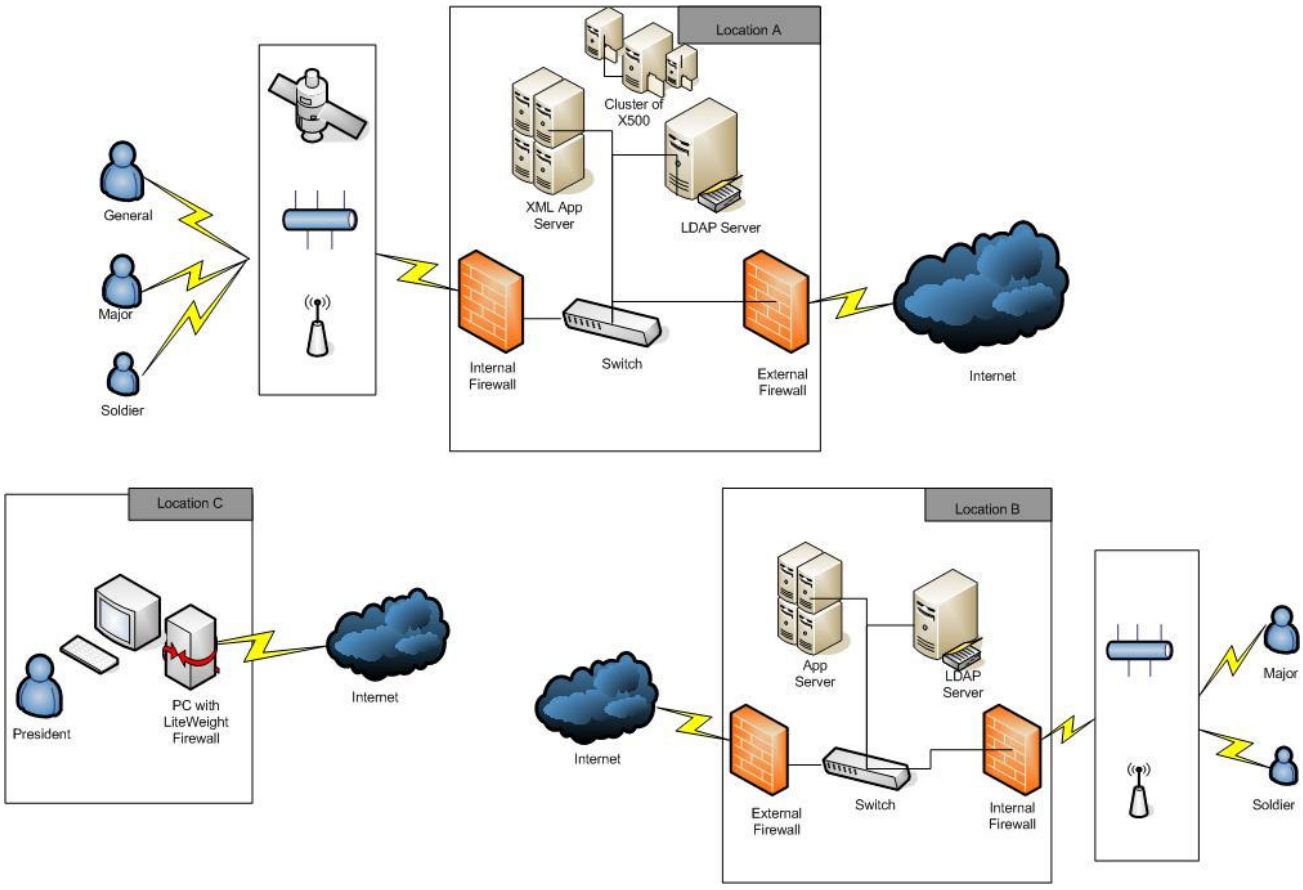
THE SETUP:

The organizational network is assumed to have a number of DMZ protecting Application Servers and different types of network links as shown in the figure.

A network link could be Internet/Intranet/ Wireless or Satellite. Credentials of each user logging into the network are checked with the LDAP server for authentication and identification of their role. Based on their role, a client certificate is issued to the user. The client certificate, which includes a bunch of classification labels pertaining to the role of the particular user, is downloaded into that user's session and made accessible by the machine protocol stack.

Whenever the user sends some data over the network, the TOS field of the TCP header is written with a priority value included as a label in user's certificate. This priority value is sent based on the application layer decision on the security and urgency requirement for those packets.

In addition to security, we need to include the service differentiation based on QoS. If the user needs to communicate with systems part of the local network, then the system makes intelligent decision based on the priority value. If the user packets need maximum security then the packets can be encrypted and sent using tunnels. A RSVP with GRE channel is established if the packet won't leave a corporate subnetwork. But if the packet has to traverse through routers and network components shared by general population, we would have secured VPN connections setup for this purpose. The communication channel could be between user machine and an application server or between end-to-end users.



For our design, we assume that the internal routers make intelligent decision based on the priority value in the TOS field of TCP header of the packet. If the next hop is determined to be insecure and the packets' security label does not match, then a secured channel is established.

If the user packets need to go outside the internal network, the outside firewall takes appropriate steps for security and QoS. Normal packets are sent as normal traffic. For special packets requiring security or QoS, bandwidth allocation and encryption tools are used. QoS for the connection is measured and the packets are sent via the best matching route. If security is also required, IP Tunnels will be established.

Clients working outside the organization network will use IP Tunnels (eg. GRE Tunnel), to connect into organization network. Those users will have special light-weight client services running on their machines which make secure connection decision while considering QoS factors. The clients outside the corporate network will not experience any differentiation of service.

The tool to be developed and deployed at the user's machine will insert XML tags as labels to the sections of the document created by the user. This way, a document can have different sections labeled according to their urgency or secrecy. This tool will then forward the whole document to the nearest application server. This tool will also fetch the user's certificate and policy labels pertaining to the user.

The application server we were referring to in above paragraphs will parse a received document according to classification of its parts and create new documents. The application server will then send the new documents to the storage directory where copies will be made depending on the number of intended recipients.

As a summery of the architecture, the components of the system are as follows:

- Cluster of Servers
    - LDAP Authentication
    - XML Parsing Service
    - Notification Service
    - File Transfer service
- Cluster of File Systems
    - Document distribution
- Client side tool
    - Proposed Tool

The technologies we propose to use are:

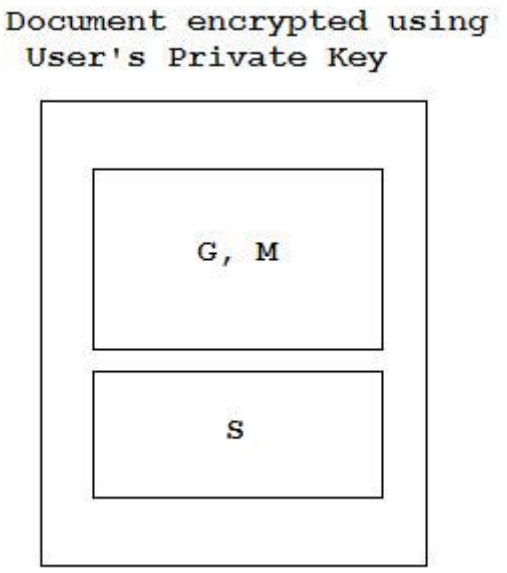
- LDAP – for authentication and credentials
- Bandwidth reservation + GRE Tunnels – for file transfer
    - PasTMon tool + Tunneling for inter-network exchange
    - RSVP + Tunneling for intra-network exchange
- XML Parser – for parsing a document to be sent
- Different modes of sending a new message alert
    - Voice message
    - Email
    - SMS

(For more information about these technologies, follow the links in the references section.)

THE SCENARIOS:

Here we will explain two particular scenarios focusing more on the differentiation part.

The **first scenario** will be when a User logs into the system, and then sends a document. This document needs to be differentiated among different rank of users, let us say Generals, Majors, and Soldiers. The sender can perform this activity by using some type of tags, like XML tags which classify and differentiate amongst the parts of the document.

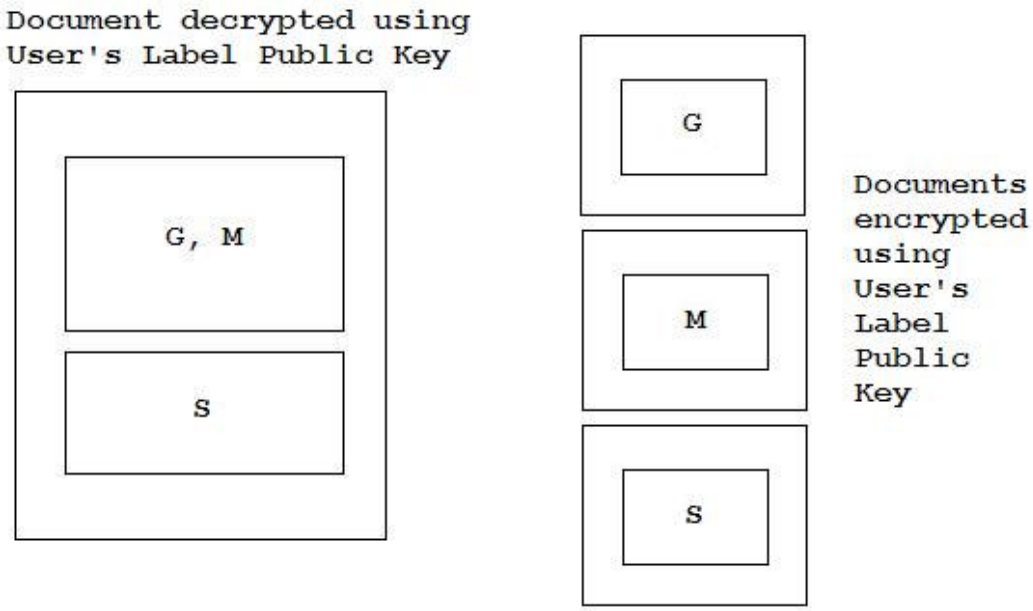


The Software Tool, using the User's Private Key, encrypts the document. The document is then sent to the Application Server where the user got authenticated.

On the Application Server, some information related to the User can be found like username, password, cell phone number, email, and where the User has his/her space in the directory service. This service is located on the directory server where the User got enrolled the first time. We are proposing this approach in order to avoid a bottleneck when a document is to be sent to many users and has to be copied many times, especially if the document is big enough. So, the DMZ checks the document priority: if document has a higher priority and was sent by a high rank user, then this document needs to be sent as soon as possible. Here, we ensure that Security and QoS must be

applied.

Once the best path is found, and the connection is secure, the document is sent to the appropriate X500 directory where the document is decrypted using the Public Key related to the user label. Once this is done, the XML parser parses the document and its copies are created based on the number of users the document needs to be sent. Public Key for each label of the user is used for each of the copies of the document.



After this, the copies of the documents are sent to the appropriate User's space on the X500 directory. The document is stored and an alert/notification is sent to the user to inform him that he has a document waiting to be read.

If the document has a higher priority and the User is not 'online', the system will use other ways to contact him, like cell phone number and email, to let him know that he needs to connect to the system in order to get the information which is urgent.

Otherwise, the user will know a document is waiting to be read once he logs into the system.

As an outcome of the above scenario, the appropriate differentiated copies of the document are sent to the correct users.

The **second scenario** is when the User logs into the system. This takes place as a normal session with no messages sent to the user, or as a result of a message on his cell phone or email warning him that has a document waiting to be read.

Once the user logs into the system, the application server where the User has logged in checks with the appropriate User's X500 in order to see if there is a document waiting for him. If that is the case, the X500 sends the document to the DMZ, and from where the document is sent to the User's computer. Appropriate security and QoS issues are applied.

With the document in User's computer, the Software Tool decrypts the document using that user's Private Key.

As a result of the above scenario, the User has his own part of the document.

FUTURE WORK:

For Future Work, we consider at least three main parts:

- It is hard to implement QoS on the Internet. On a controlled environment, like an intranet, somehow you can guarantee the behavior of differentiated traffic all along the path. But once this traffic arrives into the Internet, the effort needs to be increased. We think that this can be one of the research issues for this project, which is, finding a way to guarantee QoS in Internet.
- For this project we assume that any user can send, and receive, documents from any other user, no matter which rank they have. This could be a general case, but thinking about implementing the system on a specific case could require the use of a model like Bell-La Padula.
- And finally, we are assuming that the document being differentiated is a plain text file. What if is a video file, or a sound file? Would it make sense to try to differentiate such type of files?

REFERENCES:

- Protection:
  http://www.research.microsoft.com/~lampson/09-protection/Acrobat.pdf

- Identity Systems:
  http://books.nap.edu/html/id_questions/

- Trusted Computer System Evaluation Criteria:
  http://www.boran.com/security/tcsec.html

- Security of the Internet:
  http://www.cert.org/encyc_article/tocencyc.html

- Introduction to Computer Security:
  http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

- Designing an Authentication System:
  http://web.mit.edu/kerberos/www/dialogue.html

- Home Network Security:
  http://www.cert.org/tech_tips/home_networks.html

- Open Shortest Path First (OSPF):
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm

- How routing algorithms work:
  http://computer.howstuffworks.com/routing-algorithm3.htm

- Wired-Wireless Network Architectures:
  http://www.symbol.com/category.php?fileName=WP-32_network_architectures.xml

- pasTmon Tool :
  www.pastmon.sourceforge.net

- RSVP:
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm

- GRE with RSVP:

  http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00801982ae.shtml

- Open LDAP:
  http://www.openldap.org/

- X 500:
  http://www.terena.nl/library/gnrt/specialist/x500.html