***3413ICT NETWORK SECURITY - Assignment 1***

***Designing Technical Security Plan for***

***Medium-Scaled Wide Area Network***

Anthony Guevara

Student #: s2877416

Ashmore, QLD, Australia

anthony.guevara@griffithuni.edu.au

**Abstract**

A client that owns a number of motel chains across Australia has expressed an interest in improving the connectivity of his branches with security in mind. As of now these different branches do not have any ties to each other; they are detached segments that operate independently of one another. The concern of the client is that by adding security parameters the workflow of regular operations may be affected. This paper discusses a proposed implementation to satisfy the client’s workflow and security requirements. The proposed technologies to implement include S/MIME for e-mail, IPSec for video conferencing, and Kerberos for network user administration and printing. The implementation details include the required hardware and software giving the appropriate level of detail so that the reader can gain full understanding at the level of involvement for satisfying the requirements. Deployment costs and running costs are also examined to determine if the price range is appropriate.

# Introduction

The purpose of this paper is to provide technical details on meeting a customer’s security requirements. The client is an owner of medium scale motel chain has a number of LAN (Local Area Network) segments located at different branches across Australia. These branches are located in Gold Coast, Sydney, Melbourne, and Perth with the headquarters located in Brisbane. Currently, the LANsegments are not interconnected and operate independently of one another. The client has requested that they would like to connect all of the different branches allowing secure communication to headquarters in Brisbane.

# Requirements

## Workflow

The client has requested that the implementation meet the following workflow requirements:

|  |
| --- |
| 1) The client segments’ users, at each branch, have paid-only access to the printers. |
| 2) The CEO has full access to all machines except client’s portable devices. |
| 3) The staff segment’s users of each branch office is required to send daily confidential progress report to the CEO via management segment of headquarter LAN. |
| 4) The local management of each branch has to send confidential income-expenditure report to the CEO on daily basis. |
| 5) The peer communication between branch managers is carried out on weekly basis, in the form of confidential business-strategic-plan report, to share weekly business activities and strategies. |
| 6) The headquarter and branch offices have monthly confidential video conference meeting to discuss monthly targets and devise operational plan for next month. |

Figure 1

## Security Features

In addition to the workflow requirements there are a number of security requirements that must also be fulfilled to ensure safe communication internally and externally.

|  |
| --- |
| 1) E-mail system that is able to provide following services  • Authentication  • Confidentiality  • Compression  • E-mail compatibility. |
| 2) Secure video conferencing service that is able to provide following services  • Authentication  • Confidentiality |
| 3) Central server that grants time-bound service access to single (or group) of users (hint:  Kerberos). |

Figure 2

# Prerequesites

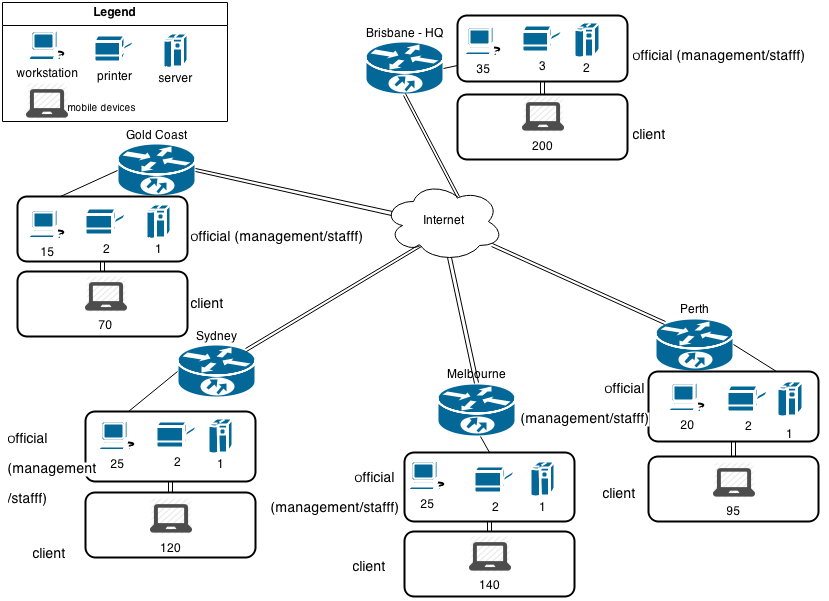
To satisfy the workflow and the security requirements there must be additional hardware and software integrated into the existing system.

## Hardware requirements

For each campus, routers that support *IPSec* (Internet Protocol Security) must be added. Specifically, Cisco’s RV220W router has been selected to deploy at each branch [1].

Additional server infrastructure must be added for Kerberos. An *Authentication Server* (AS) as well as a *Ticket Granting Server* (TGS) will be required at each branch.

A dedicated printing server at each site will also be necessary for managing clientele printing and local or remote administration.



Video conferencing gear such as cameras and projectors and screens will be required for confidential videoconference meetings. Specifically, Polycom’s USB camera VVX 500 [2], JP Offices projector screens [3], and LED-86 Projectors [4].

## Software Requirements

To meet the workflow requirements, additional software must be installed to monitor and control printing. The software chosen for accomplishing this is *CUPS* (Common Unix Printing System). CUPS will allow remote administration and monitoring from any of the campuses. CUPS is an open source printing service developed by apple and is free.

Polycom’s software suite is also required for secure video dialogue (discussed in later sections).

# Network Model

Figure 3 at the top of this page is a network topology diagram of the current system in place. Headquarters is located in Brisbane with all of the other campuses detached from one another. The following sections will discuss different methods for the campuses to communicate securely with one another.

# Technical Requirements

## Secure E-mail

The client has requested that the e-mail system is able to provide the following services: Authentication, Confidentiality, Compression, and E-mail compatibility. *S/MIME* (Secure Multipurpose Internet Mailing Extension) meets all of these requirements.

In terms of general functionality S/MIME behaves similar to a popular encryption program called *PGP* (Pretty Good Privacy). Both allow users to encrypt and sign messages using asymmetric encryption techniques. The main difference between to two is that S/MIME uses public key certificates and its key management is a hybrid between X.509 certificate hierarchy and PGP’s web of trust.

Figure 3

S/MIMEfulfills *Authentication* by using a signing operation. This process involves tacking on the sender’s digital signature in addition to the sent message. The following diagram depicts the signing process:



Figure 4.1 [5]

On the recipient’s side, a verification procedure takes place to verify the authenticity of the digital signature. The recipient uses the sender’s message to generate a another digital signature that is compared to the sender’s digital signature. If the two signatures are the match, the signature is valid. If the two signatures are different, the signature is invalid.

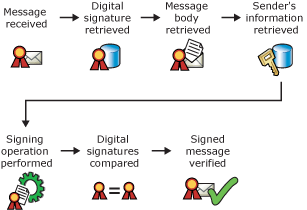


Figure 4.2 [5]

A number of different signature algorithms are supported with S/MIME 3.2. The asymmetric encryption *RSA* (Rivest, Shamir, Adleman) with SHA-256 (Secure Hash Algorithm, 256 bits) is provided by default to use the signature feature. In addition there is support for other algorithms and hash functions such as DSA (Digital Signature Algorithm), SHA-1, and MD5 (Media Digest) may be used.

Encryption provides *confidentiality* during transit and storage. Only the intended recipients are able to read the contents of the message. From a high level, the sender encrypts the outgoing message and the recipients decrypt the message. S/MIME meets these requirements this by providing a service called ‘enveloped data’. Enveloped data works by:

* Generating a pseudo random session key
* For each recipient, encrypt the session key with the recipients public RSA key
* For each recipient, prepare a block known as RecipientInfo that contains the sender’s public key certificate, and identifier of the algorithm used to encrypt the session key, and the encrypted session key
* Encrypt the message content with the session key [6]

*Compression* is a supplementary service offered by S/MIME. It is used strictly to reduce message size and does not provide additional security features. Compression of binary encoded encrypted data is not recommended because it will not yield significant results. However, the benefits are applicable to message text that has been encoded using base64. [7]

*E-mail compatibility* is another concern amongst the client in regards to mail. S/MIME implements Base64 encoding which makes it highly compatible on a variety of different e-mail clients.

In figure 1, implementing S/MIME satisfies points 3 and 4. The staff is able to send daily progress reports to the CEO via e-mail from any branch with encryption and digital signatures that provide confidentiality and authentication. Also, income-expenditure reports can be sent as e-mail attachments that are encrypted during transit. If the reports are too large for attachments, SFTP (Secure File Transfer Protocol) may be used in conjunction with access control lists.

## Secure Communications

While it is important to have security aware software that can provide authentication and confidentiality in video conferencing, there is actually a more important area to address. Instead of focusing on a specific suite of software that satisfies certain services, it is more paramount to have a secure channel in which communication takes place. Once the medium of communication is secure, inherently so is everything on that channel.

IPSec (Internet Protocol Security) will be used to ensure that sensitive data is not compromised during transportation. IPSec was designed with the following services: origin authentication, connectionless integrity, access control, confidentiality and replay protection [8]. IPSec can be used to secure branch connectivity over the Internet which will enable the company to communicate securely over the public WAN (Wide Area Network). Also, the business can now rely on the Internet instead of focusing on developing private infrastructure saving on management overhead.

Additionally, clients or employees from outside the network may connect to the secure network by using *VPN* (Virtual Private Network) software. Since Cisco routers are being used for the transport layer at all of the branches, it makes logical sense to use a Cisco VPN Client to complement this service.

The most beneficial part of employing IPSec is that all data is encrypted at the IP (Internet Protocol) level. This means is that security ignorant applications will become inherently secure and security aware applications become more fortified [9].

Since this technology operates on the transport layer it is transparent to the application layer and end users. This allows for a smooth integration without disturbing the workflow of other applications and users.

Figure 2 point 2 states that authentication and confidentiality must be met for video conferencing. Both of these services are satisfied with the implementation of *ESP* (Encapsulating Security Payload).

The ESP protocol provides a wide variety of security services. The most important ones relating to the client’s needs are access control, confidentiality, and data origin authentication.

A main concept of using ESP’s authentication and confidentiality mechanisms is the security association (SA). This is a one-way relationship between sender and receiver. Before IPSec can provide a security service for the data a secure communication channel between initiator and responder must be set up through a SA [10]. An SA is a method that IPSec uses to track all the details concerning a communication session.

An SA can also work in conjunction with peer relationships. For each new secure channel an additional security association is added. An SA may implement either *AH* (Authentication Header) or ESP, but not both. For this implementation only ESP will be implemented because it includes all the features of an AH in addition to encryption.

IPSec will operate in tunnel mode using the ESP architecture. An advantage of using tunnel mode is that the entire IP packet is protected. This means that no routers during transportation are able to look at the inner IP header information.

*Authentication* takes place using digital certificates. Digital certificates are the preferred method of authentication because it is more scalable than using the traditional method of distributing pre-shared keys. The traditional way of doing this is bulky because when a new device is added to the network all other existing devices that need to communicate with the new machine must trust the new device. When using certificates, a new device simply enrolls using a *CA* (Certificate Authority) and is able to communicate without modifying other machines [11].

Very similar to how S/MIME uses encryption techniques to provide *confidentiality* the same is applicable to IPSec. The following encryption algorithms are supported with IPSec: DES (Digital Encryption Standard), 3DES (Triple DES), AES-CBC 128,192,256 (AES in Cipher Block Chaining Mode). [12]

In summary the Cisco routers are configured through IOS (Internetwork Operating System) to enable secure communication between campuses. The routers are to be configured with ESP architecture using tunnel mode for *encryption* and digital certificates for *authentication*.

Once IPSec is configured and running correctly the video conferencing software that is selected is of little importance because all of the traffic from branch to branch is encrypted.

However, relying on IPSec alone to ensure video conferencing security is foolish. While this is an excellent tool for securing network level traffic, it falls short when trying to communicate securely outside of the company’s LAN. For example, if a user needs to attend a videoconference from home and are unable to access a VPN they will not be able to attend the conference.

For this reason it would be best to apply security on the application level as well. The company Polycom offers secure video conferencing software solutions that are up to date.

Funnily enough at the time of writing this paper, a *SSL/TLS* (Secure Socket Layer/Transport Layer Security) vulnerability was discovered called HeartBleed. Essentially some of Polycom’s software suites were vulnerable to the exploit, which allowed attackers to read confidential information that this software is supposed to protect [13]. This is a reminder that there is no such thing as absolute security and a number of different security mechanisms should be applied in case one fails.

The implementation of IPSec and Polycom’s software suite for videoconferencing satisfy workflow requirements 5 and 6. Peer communication between branches can be carried out in any direction using authentication and providing confidentiality.

## Kerberos and Network Authentication

Kerberos is an authentication service developed by MIT that is both open source and commercial. It consists of three parties: the client, the server, and the key distribution server [14]. It is an important tool used to restrict access to authorized users and is able to authenticate requests for services. Kerberos provides a centralized authentication server whose function is to authenticate users to servers and vice versa.

Kerberos was designed with the following requirements:

* Secure: A network eavesdropper should not be able to impersonate a user.
* Reliable: Kerberos should be highly reliable and have distributed server architecture.
* Transparent: Other than entering a password the user should not be aware that authentication is taking place.
* Scalable: The system should support a large number of clients and servers.

A Kerberos server will be set up at each branch to make the system redundant and able to share resources. Users will be allowed to access their account in the occasion that one server becomes unavailable or access services from another ‘realm’.

In the Kerberos world – having multiple servers that interact with each other are known as ‘realms’. The advantage of using a realm is that it’s not practical to have users and servers in one administrative domain registered with a Kerberos server in another state. If something were to go wrong a local administrator is usually preferred because they are more familiar with that local system. However, remote administration is still available, if required.

An advantage of having multiple Kerberi setup at all of the branches is that the printing service CUPS can work in union with Kerberos. CUPS can be configured to authenticate users and check if they are allowed to print based on available credit satisfying figure 1 requirement 1.

The CEO has requested access to all user accounts in the management and staff section of the different LANs. Through administrative configuration these access rights can be set up and granted by Kerberos to allow access to these accounts. This satisfies workflow requirement 2 in figure 1 requesting that the administrator has access to all staff accounts.

Kerberos is used for authentication and limiting services to validated users. It can be deployed in multiple locations and communicate with other Kerberos machines through the use of realms. In addition Kerberos can communicate with other services such as CUPS to monitor and control printing privileges for temporary guests.

# Cost Analysis

## Deployment Cost

Section II A has been put into a table to estimate cost of required hardware:

Hardware:

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Quantity | Price/Unit | Total |
| Cisco’s RV220W router | 5 | 348.99 | 1744.95 |
| Authentication Server | 5 | 500.00 | 2500.00 |
| Ticket Granting Server | 5 | 800.00 | 4000.00 |
| Printing server | 5 | 400.00 | 2000.00 |
| USB camera VVX 500 | 5 | 213.00 | 1065.00 |
| projector screens | 5 | 163.90 | 819.50 |
| LED-86 Projectors | 5 | 253.40 | 1267.00 |

Section II B has been put into a table to estimate cost of required software:

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Quantity | Price/Unit | Total |
| Polycom RealPresence Desktop Solution | 5 | Unkown, To be determined. Please contact Polycom staff at  +1 800 355 355 for pricing options [15] | TBD |

The total cost of the hardware and software:

|  |  |  |
| --- | --- | --- |
| Hardware Total | Software Total | Grand Total |
| 13396.45 | 0.00 (TBD) | 13396.45 |

It will cost approximately $13396.45 to deploy the proposed system with all required hardware. The cost of the software is to be determined because the prices are not listed on Polycom’s website, a customer service agent must be contacted at the number listed for pricing options.

## Running Cost

Judging from previous jobs it can cost a server anywhere from 15.27 / month to 20.00 / month depending on the price of electricity and the power supply used by the server. In total, there are 15 servers being deployed across five branches. 15 x ((15.27+20.00)/2) will cost approximately $264.52 per month or $3174.30 per year.

A network administrator will also be required to maintain user accounts at each branch and maintain and update new applications such as Kerberos and CUPS. The salary range for this job varies and it is up to the client to find the appropriate staff to fill this vacancy.

# Conclusion

This paper has discussed solutions for allowing different motel subdivisions to communicate securely. S/MIME was examined as a public key encryption mechanism to secure e-mail. IPSec was examined to secure data transmission between campuses providing safe communication for video conferencing. Lastly, the strengths of using Kerberos for managing users and limiting their access were examined. This implementation meets all workflow and security requirements and provides an excellent base platform that can be scaled if the need arises.

##### References

1. http://www.mwave.com.au/product/cisco-rv220w-network-security-firewall-aa37269?gclid=CPCE6amk170CFcLvpAod3jsAsQ
2. http://dstore.com/buy/polycom-vvx-500-and-600-video-conferencing-camera-usb-20-16751989?utm\_source=googauprodfeed&utm\_medium=cpc&gclid=CMeCsY-o170CFYcipQodUkAAWg
3. http://www.jpofficeworkstations.com.au/wall-mounted-projector-screens/
4. http://www.ahappydeal.com/product-164973.html?currency=AUD&gclid=CMzRmveo170CFQEepQodASMANQ
5. http://technet.microsoft.com/en-us/library/aa995740(v=exchg.65).aspx
6. W. Stallings, Principles and Network Security, 2nd Edition, Upper Saddle River, NJ: Prentice Hall, 1999, pp. 374-390
7. http://tools.ietf.org/html/rfc5751
8. **http://search.proquest.com.libraryproxy.griffith.edu.au/docview/1400500080**
9. W. Stallings, Principles and Network Security, 2nd Edition, Upper Saddle River, NJ: Prentice Hall, 1999, pp. 399-440
10. **http://link.springer.com.libraryproxy.griffith.edu.au/article/10.1007%2Fs10207-013-0201-1/fulltext.html**
11. W. Stallings, Principles and Network Security, 2nd Edition, Upper Saddle River, NJ: Prentice Hall, 1999, pp. 325
12. http://technet.microsoft.com/en-us/library/dd125356(v=ws.10).aspx
13. **http://www.google.com/patents/US8639936**
14. http://www.ciscopress.com/articles/article.asp?p=421514&seqNum=4
15. http://www.polycom.com.au/content/dam/polycom/common/documents/brochures/heartbleed-security-advisory-enus.pdf
16. http://www.polycom.com.au/products-services/hd-telepresence-video-conferencing/realpresence-desktop.html