On the security of cloud storage

Juan Luis Prieto Martinez

TFM - E-Commerce

Universitat Oberta de Catalunya

A thesis submitted for the degree of

Masters' Degree in Security of Information and Communication Technologies

June 2015

Abstract

In a connected world where companies can operate anywhere through internet and where customers and employees use more than a single device to access, consume and produce content, companies are being forced to adapt their data storage to this new reality. Cloud storage solutions allow these companies to share documents, photos, etc.; but also enables document edition by a single person or a group of people. It also breaks the bridge between the consumer devices since cloud storage can normally be accessed using a browser for basic operations, using private clients extending the functionality or integrating the cloud storage as part of an application using an API. As companies adopt this new way of sharing and storing information they also need to be confident that their data is secure and private. Most of the solutions available store the information outside of the customer domain and thus issues of security settings and their alignment with data protection standards and regulations become of great importance.

Contents

List of Figures

List of Tables

Chapter 1

Introduction and Definition

1.1 Introduction

Cloud computing has opened a range of opportunities for software companies and their clients allowing them to outsource computing infrastructure, while saving on costs. More companies, especially Small to Medium Enterprises (SMEs), are outsourcing their applications to cloud providers in order to focus on core business activities and lower costs [57]. However, despite the great potential of cloud storage services, cloud security is becoming a major research issue and a concern for companies adopting these infrastructures for their services and customer relations. With cloud providers experiencing a big growth in client base and struggling to meet service level commitments and customer expectations, companies are uncertain about the threat that migrating their services to the cloud entails. This is a critical issue for all stakeholders involved at all stages as users, cloud providers and security providers; however it is especially critical for companies relying on cloud services for their day-to-day operations.

Clouds still have a long way to go in order to build the trust of potential cloud customers in issues of risk, availability, protection rights and security in general [26]. At present, there is a major gap in the research and development of security tools aiming to improve security and trust in the cloud while preventing downtimes and interference to business operations[59]. Tools need to be developed which will assess the security concerns relating to availability, privacy and trust of cloud platforms, taking into account the specific requirements of large enterprises and SMEs.

This need has not gone unnoticed; in fact, many initiatives have been launched in recent years to address these challenges. Some examples include:

- The National Institute of Standards and Technology (NIST) have developed a list of security risk and mitigation in reference to a lifecycle which needs to be followed for performing risk assessment and certification and accreditation for threats in accordance with government laws with a detailed analysis [58].

- The EU funded Horizon 2020 project CloudingSMEs provides support services to European SMEs, in order to facilitate them in adopting and fully leveraging the benefits of cloud computing services. CloudingSMEs has created and launched a toolbox for SMEs wishing to migrate to the cloud, including, among others, a "Cloud Security Scorecard" tool and a "Privacy and Data Protection Guide" tool [44].

In line with these initiatives, the purpose of this final masters' thesis is to analyze and compare the security offerings of 6 cloud storage providers and one open source cloud platform, and propose strategies for risk mitigation in three concrete scenarios wherein companies seek to migrate data and applications to the cloud.

1.2 Scope

For companies, storing data in the cloud not only offers better mobility or world wide access to their documents, but also considerable cost savings 1.1. However, one of the biggest concerns of such companies is the possible loss of control over their data as they upload it to the cloud. In other words, since their data will hosted on the cloud storage provider infrastructure, the control of this data is now managed by a third party rather than directly by the company itself. Responding to their customers' need, storage providers also share this concern and attempt to implement security mechanisms protecting client data from exposure to external parties.

Figure 1.1: Cloud mobility

The work reported in the following chapters focuses on the study and testing of security mechanisms implemented by storage providers or storage services, and the manner in which companies interested in migrating their data into the cloud can adopt this new paradigm.

Before starting with the definition of the characteristics it is important to keep in mind the following terminology referred to throughout the document:

Client: Defines in this document to describe a synchronization client on personal computers and mobile devices.

Service: Is used to refer to an online service offering an Application Program Interface (API) or accessible from a web browser (mainly the cloud storage).

Application: Refers to a client application developed by a company which will use storage services as a documents repository or as datastore.

Specifically, the thesis explores the following characteristics of the cloud storage services:

Online Drive: This would be the basic use of a cloud storage, hence the first thing to study is the cloud storage as an online drive used only to store, edit and share documents. The analysis in this context will identify if the storage provider is using any kind of encryption on the server side, if the access to the service is using authentication, how the service implements sharing mechanism and whether or not a company can import their keys to encrypt the communication between the client and the server side.

API security: Not all the communication between a service and the cloud storage drive is done via the web or a synchronization client. Nowadays, cloud storage services offer an API to integrate their services with the applications. From an information security perspective, this API needs to offer a security mechanism to prevent data leaks across the server, transport or client layer. In this thesis, these APIs will be analyzed and tested to evaluate the extent to which security is correctly addressed.

Datastore: Many services allow a closer integration with applications; rather than just acting as an external drive, they can be the main data store of an application. As the cloud drive is mainly used to store documents, the datastore is more comparable with database integration or the filesystem of the company's application, i.e. the application can be running locally on the company's infrastructure while the real data is being stored in the cloud provider's infrastructure. The analysis of this aspect will focus on the security between the application and the cloud drive used as datastore.

Transport: This analysis will compare and describe the transport mechanisms implemented in the transfer of the data from the customer device (laptop, tablet, mobile) to the cloud server. The scope of this analysis will go beyond just browser uploads and also include client/server synchronization transport.

Legal issues: Not only technical security needs to be addressed: in a globalize world where data can be stored and consumed anywhere, cloud storage providers need to adapt their services to the different legislations and regulations in force in the locations and market sectors where they are operating.

Security certifications are common in the cloud services studied in the thesis. They are proof that the storage services follow best practices, and established guidelines and standards to secure customers' data. These certifications target many aspects of security, from physical security to logical security, procedures or software development. Certifications normally require an annual audit to ensure that compliance is ongoing. During the audit the company behind the services will have to prove that the guidelines and standards have been met by showing reports and following interviews with the auditors. Because of the nature of the storage services, the companies behind them need to achieve the effort of acquiring security certifications for different target users and use cases. Along the service analysis process these are the certifications that have been found:

Payment Card Industry Data Security Standard (PCI DSS): Is a set set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express [42].

International Organization for Standardization (ISO 27001): Is an internationally recognized best practice framework for an information security management system. It helps you identify the risks to your important information and put in place the appropriate controls to help reduce the risk [1].

Service Organization Controls (SOC): Are reports designed to help companies to build trust and confidence on their service delivery process and controls [87]. There are 3 different SOC reports:

1. SOC1 is the *Internal Control over Financial Reporting* which centers the auditory on the fairness of the presentation of management's descriptions of the service organization's system and the design of the controls to achieve control objectives on a specific date or period
2. SOC2 is the *Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* which is intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users? data and the confidentiality and privacy of the information processed by these systems.
3. SOC3 is the *Trust Services Report for Service Organizations* and is intended to meet the assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems

used by a service organization to process users? information ,and the confidentiality, or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report.

CSA Security, Trust & Assurance Registry (STAR): is a comprehensive set of offerings for cloud provider trust and assurance. The CSA STAR is public and used by companies, customers or governments. It has 3 different levels:

1. *Self-assessment*, where cloud companies publish their security compliance themselves.
2. *Third party assessment* is an independent assessment of the security of a cloud provider. This variant has one specific for China meeting the Chinese national standards.
3. *Continuous monitoring*, where cloud providers allow an automatic and continuous security monitoring of their services.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Is set of security rules developed by US Department of Health and Human Services to protect certain health information. These rules cover technical and not technical safeguards that companies should meet to protect individuals health data [71].

Health Information Technology for Economic and Clinical Health (HITECH): addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules [72].

Statement on Standards for Attestation Engagements (SSAE): Is a US standard mirroring and compliance with the ISO norm ISAE 3042 [56]. This certification is the base of the SOC certifications [88].

Family Educational Rights and Privacy Act (FERPA): This federal law protects the students educational records [70]. Despite of being a federal law is has become a standard specially for the storage cloud services since they are used by many students to store academic data.

Children's Online Privacy Protection (COPPA): Prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet [29].

Federal Information Processing Standards Publications (FIPS): These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide [67]. In the scope of the thesis FIPS 140-2 is followed by the cloud storage providers. This standards cover the areas, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Federal Information Security Management Act (FISMA): This Act assigns responsibilities to different agencies to ensure the security of the data in the federal government, the agencies are in charge of keeping the risk on a low level in a cost-effective manner [68].

1.3 Storage services

For the propose of the analysis, I have chosen the seven cloud services presented below. Out of the seven cloud storage services, one - namely, OwnCloud - is unique in that it is not a service by itself. OwnCloud is an open source tool that allows creating and setting up cloud storage service on one's own infrastructure (private cloud). Despite not being a public cloud service like the other six services included in the analysis, the case of OwnCloud is included here as it is very interesting and offers companies the ability to build their own private storage service. Importantly, this is not to be taken as an exhaustive list of cloud storage provider; rather, the intention is to refer to the most common and popular services. Below is a general overview of the 7 cloud services included in the analysis:

Dropbox: Is one of the global market leaders in the cloud storage ecosystem, and offers features relevant to most of the characteristics that will be analyzed during this study. Dropbox is deployed on top of Amazon S3 (amazon storage) and offers clients for the most popular computer and mobile Operating Systems (OS). It also provides a rich API supporting a wide range of programming languages. Dropbox uses Transport Layer Security (TLS) tunnels and Advanced Encryption Standard (AES) cyphers on the sever side to protect customer data.

Box: Is another popular cloud storage service. Lately, Box has made a move towards integrating its storage solution with document editors and it is currently working on to integrate with more enterprise-related services. Box has recently announced that it would allow customers to upload their keys with the Box Enterprise Key Management initiative. This positions Box a step ahead of enterprise cloud storage adoption.

Google Drive & Google Cloud Storage: Are two types of cloud storage service offered by Google. This service integrates with the rest of google services, and by default it uses TSL security. It also provides a very rich API for any of the most popular OSs in the market. Google Cloud Storage is mentioned because it is the storage offering for the cloud platform, this storage allows any application to integrate with it via API. This storage can be used as a file system or to store no SQL (Structured Query Language) databases.

Amazon Cloud Drive & Amazon S3: Similarly to Google, Amazon offers two types of storage for two different profiles or use cases. Amazon Cloud Drive is oriented to profiles looking for a cloud-based hard drive which will synchronize documents between devices and the Cloud. Like in the case of Google Drive and Google Cloud Storage, Amazon S3 is the storage offering that Amazon provides as file system for cloud services. Amazon S3 can host almost any service, structure or data that a company needs to store in the cloud, thus it is of the same scope as Google Cloud Storage.

iCloud: Is Apple's Cloud service which integrates with Mac OX and iOS. This service is very tight to the Apple ecosystem and it cannot be used, or very limited, outside of this ecosystem. The service offers Cloud Storage mainly for data backup of the customer's data and it will synchronize the information with all the devices connected to the service using an iTunes or iCloud account.

OneDrive: Is Microsoft's cloud storage service. This is, for example, the storage service used by the new online version of Microsoft (MS) Office - Office 365. OneDrive can synchronize data with any device and modify online any document with the aforementioned online version of MS Office, its functionality is similar to the above mentioned solutions, i.e. to store documents and share them using the cloud. Since the announcement of Office 365 this service is gaining popularity for its simplicity and compatibility with Microsoft Office suite.

OwnCloud: Is the Open Source solution that is trying to compete with the above mentioned services to store and share documents with different users and to sync data across mobile, pc and cloud. The reason why this is included here is because more and more OwnCloud is being deployed as part of the private cloud of companies, hence, even though it is not a service by itself it is an emerging key player in the cloud storage market. With OwnCloud, a company can control where the data is stored and its deployment under any legal frame (EU versus US servers, for example). OwnCloud allows interaction with active directory or open Lightweight Directory Access Protocol (LDAP) for user authentication and its last versions support remote authentication between two different instances of the server, i.e. a company deploying OwnCloud in two regions can connect the two instances and create a trust relationship between them.

1.4 Scenarios & testing

In chapter 3 three scenarios where a company can adopt cloud storage are tested and explained. Those scenarios are

- **Use Case 1:** Cloud Storage as document repository.
- **Use Case 2:** Cloud Storage as a datastore integrated in an application.
- **Use Case 3:** Deployment and secure of a private cloud storage.

Each scenarios above mentioned have specific security concerns and challenges identified. To achieve a conclusion and let companies decide the best Cloud Storage approach for their needs the following sections introduce those challenges and test executed to analyze the security applied.

1.4.1 Cloud Storage as document repository

This scenario represents the most common and easy use to adopt for this type of cloud services. Using Cloud Storage introduces mobility and agility when employees are producing or consuming documents. By storing documents in the cloud a document becomes available from any device that can connect to the internet, this means that the information can be produced an consumed from computers or a mobile device. But the concern is that the document will normally be stored on the Cloud Storage platform and needs to be secured and only accessible certain users. To simplify the use of the Cloud Storage as a document repository most of the services are offering synchronization clients.This synchronization clients will manage the connection from and to the server side of the service and so this use case will target the following questions:

1. Client side security: is the client applying any kind of encryption on the client side? Can it be done using the API?
2. Communication: how is the communication between the client and the server taking place? Is the service using a private or a standard communication protocol? Is the communication encrypted?
3. Server side:
   (a) Does the service provider apply server side encryption?
   (b) Can a client encrypt its data using its own set of keys?
   (c) Is the service provider offering backup solutions?
   (d) Is the company data duplicated on another datacenter or region of the DC?

The answer of this questions For the purpose of the analysis the work was divided into three tasks:

Task 1 - Installation This task includes creating an account, installing and configuring the security and access on the server and client side using the documentation provided.

Task 2 - Analysis Using the provider documentation the synchronization client will be configured (if possible) to encrypt customer data locally. Communications between client and server are secure, hence a traffic analysis will provide information about how this channel is secured and if data is encrypted.

Task 3 - Testing Execute different types of penetration test with an unprivileged user on the client side.

- Analyze the traffic exchanged between the client and the server
- Execute a vulnerability scan against the web application of the Cloud Storage service
- Execute penetration tests against the web application of the Cloud Storage service

1.4.2 Cloud Storage as a datastore integrated in an application

This use case goes a step forward from the previous scenario. Since the cloud storage services offer APIs, the security of the services developed with them should also be addressed. Companies may want to migrate entire services to the cloud like their intranet, billing system or employee salaries. At the same time they would want to provide better scalability options for the storage used. This use case will thus be focused on the API security and the use of the cloud service as a datastore for a web application. Work was divided into the following four tasks:

Task 1 - Service identification Identify an application that can be migrated to use cloud storage instead of a traditional filesystem.

Task 2 - API installation Register the application with the cloud provider and install the service API.

Task 3 - Development Develop the adaptation of the cloud service using the API and securing the communication between the service and the cloud storage.

Task 4 - Security tests Create a set of security tests that would allow to measure the achievement of a proper security link between the service and the storage.

1.4.3 Deploy and secure of a private cloud storage

Fast growing SMEs with some services already migrated in to the cloud (private or public) could offer a new service to their employees simplifying their mobility by creating an "in-house" cloud storage. This storage service can be offered by deploying an instance of OwnCloud. OwnCloud being open source allows to control the E2E deployment of the service and the configuration with the company security concerns. This use case will lead to a secure installation of OwnCloud where employees can store, synchronize and manipulate any kind of file for their day-to-day work. The tasks related with deploying a secure in-house storage service using OwnCloud are:

Task 1 - Generation of Certificates these certificates will be used to create a secure tunnel between the server and the client and to encrypt the data stored.

Task 2 - Installation of the server this task will focus on the installation of the server using the certificates generated in the previous task.

Task 3 - Installation of the antivirus scan all the files stored in the server will be scanned as they arrive to the server avoiding the storage of any infected files.

Task 4 - Active Directory (AD) / LDAP integration The users will be able to connect to the service using the company AD or LDAP server.

Task 5 - Security tests Create and execute a set of security tests that would allow to measure the achievement of a proper security link between the service and the storage.

Chapter 2

Cloud Storage Analysis

In the previous chapter I have introduced the scope of the thesis, the Cloud Storage services and the 3 use cases used to analyze and proof the security applied on the services. This chapter analyses the selected services using information displayed in their support webs and whitepapers published by each Cloud Storage service company. During the description of the services many security terms are used. To help the understanding of the analysis of each Storage service I will briefly introduce each of those terms.

Multylayer Security: Refers to the multiple security mechanisms that a Cloud Storage service applies to protect customer data. For example, each user password is encrypted with a unique key, the same user synchronization clients when it authenticates agains the server generates a different key; two factor authentication can be applied to mobile devices or non registered connections (a registered connection would be the one done from the same location or client), for instance when connecting from a new computer; on the server side the encryption of the data, data replication, etc. Each of the Cloud Storage providers use these technique to ensure data protection. This topic is continuously changing and research in this area is active. The European project CUMULUS [30] is developing models, processes and tools to certify and validate the security on the cloud environment.

Certification Authority (CA): It is a public entity that issues public keys and certificates for message exchanges [86]. These keys are using to secure the connection between two entities. The CA is also in charge of verifying and certify the identity of an entity trying to connect to a service.

Security Assertion Markup Language (SAML): is an XML standard that allows secure web domains to exchange user authentication and authorization data [69]. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Transport Layer Security (TLS): Is a cryptography protocol designed to secure communications between computer networks [31]. TLS uses X.509 certificates and asymmetric keys to negotiate a symmetric key to secure the communication between two entities.

Active Directory (AD)/LDAP: Is a distributed database to store information relative to a network such as connected computers, printers, users and users groups implemented by Microsoft [61]. But also the active directory integrates services such as Domain Name System (DNS) to translate IP directions to human readable names. LDAP is the protocol implemented in the Active Directory to query information from it [92].

Single Sign On (SSO): It is an authentication process that allows the authentication of a single user in multiple domains or services in the scope of the thesis with a single account.

2.1 Dropbox

Dropbox [34] is the most popular cloud storage service available nowadays for companies and individuals. The most common use case of this cloud storage provider is as file storage and synchronization between different devices (computer, tablet, mobile). As the content stored in Dropbox is accessible from any device with internet connection, the company offers synchronization clients for the most popular platforms on PC, tablet and mobile. Such clients simplify the use of the service making it almost imperceptible for the end user. The client provokes the use of Dropbox as a backup service for users' files. Outside of these two main use cases Dropbox offers the possibility of being used as a datastore integrating the storage service natively on applications using the API.

2.1.1 Terms

Dropbox terms and conditions cover 12 points that the customer and the service provider (Dropbox) need to agree on to start making business together [35]. This list covers issues from the service terms, and customer obligations, to intellectual property and payments. For the purpose of this thesis, the access from third party services, where the user is responsible to grant access to the content using the Dropbox console, is of special interest. Another issue within the scope of the thesis is that of intellectual property rights. The terms and conditions do not explicitly grant Dropbox any intellectual property over the content of an account. Dropbox also gives the customer the control over the content and the user access to this content.

2.1.2 Security

Companies or individual users need to remember that their data is stored outside of their infrastructure and secured by Dropbox [40]. The US-based company does not own any infrastructure and builds their product on top of Amazon Web Services cloud. Hence, all Dropbox customer's data is being stored on Amazon S3. This means that the cloud service inherits all the built-in security of the storage service of Amazon. This allows Dropbox to have data replication in more than one zone, providing to their customers a recovery site to recover from a possible disaster in the platform.

Dropbox keeps a backup of 30 days of all its accounts, free or paid, and extends this time for the paid version [33]. Not just the files are backed-up but Dropbox also keeps the history of each file, so a customer can restore a specific version of a file. Backups of the current data stored by the end user or the company are encrypted with an AES of 256 bits making it close to impossible for an attacker to access any of the stored data under the user space. According to the Dropbox policy, its engineers do not have access to the customer data excluding a small team which needs to access data for customer support purposes. As the data is encrypted in the back-end of the service, communications use TLS to encrypt the communication between the client and the service creating a secure communication link between the synchronization client or browser and the back-end service.

One of the most popular functionalities of Dropbox is sharing contents with other users [37] [39]. File sharing in Dropbox is managed by the owner of the file or folder by indicating that it has to share it and obtaining a public link for the shared content. Dropbox implements this functionality in different ways:

Public link When using a public link, the user is sharing the content with the internet, this link can be indexed by search engines and visited by anyone.

Private link This type of link is sent to a set of users indicated by the user and cannot be accessed outside of that circle. Dropbox can send the link to the users specified by the file or folder owner or the owner herself may send the link directly.

Private link with password This feature is only available for premium customers, i.e. it is not included in the free version of the service. In this case, Dropbox allows the user to set a password to the link that the other users need to type if they want to access to the content.

Expiring links As in the case of the password protected links, this feature is only accessible with a paid account. A user can set an expiration date for the content that she wishes to share.

Using Dropbox as an integrated datastore implies to communicate with Dropbox using the API. The meaning of using Dropbox as a datastore is to provide a mobile or web application a cloud storage in Dropbox. This means that the content created or modified by the application will synchronize automatically with Dropbox. The application would create a secure tunnel with Dropbox using a unique key and a unique secret generated when a developer registers an application in dropbox. Both key and secret are used to authenticate the application agains the authorization service of Dropbox. Once the application is granted access the Dropbox will be used as the application's default storage.

2.1.2.1 Authentication

When opening an account with Dropbox, the service is asking every user to create a password which has to verified. During this process the system evaluates and ranks the user password according to its complexity. Password protection is good for some users, but may not be sufficient for users storing classified or personal data in the cloud storage. For those who require an extra layer of security, Dropbox offers a two step authentication process using one-time tokens [36]. The tokens arrive to the user via text messages to their mobile phones and they are requested to introduce the token when login into the system. For companies Dropbox is offering SSO which allows the use of a single username and password for a set of systems [38]. This way companies can, for instance, integrate Dropbox with their active directory or LDAP or with Auth0 or Salesforce (both preconfigured in the service). The connection between the popular cloud storage service and the CA is based on SAML2 and the company needs to set a valid PEM certificate prior to starting the authentication. As the authentication changes, the users need to re-sync their mobile or desktop clients against their new credentials.

2.1.3 Certifications

How do we verify that Dropbox is a secure place to store our data? As many other providers, Dropbox follows certain standards and certifications [32] [41] [43]. Table 2.1 lists the certifications and standards followed by Dropbox:

Certifications
ISO 27001
SOC 1, SOC 2 and SOC 3
CSA STAR
FERPA and COPPA
UK Digital Marketplace G-Cloud 6
PCI DSS
U.S. E.U. and U.S. Swiss Safe Harbor

Table 2.1: Dropbox Certifications

The listed certifications and standards, especially the security ones, allows a storage provider like Dropbox to prove to its users that it applies the desired security practices to pass the certification. This positions Dropbox in an advantegous position when customers decide where to upload their data to.

2.2 Box

Box [23] is another one of the big competitors in the market of cloud storage. Much like Dropbox, Box provides free plans for individual users and a paid version mainly for companies (SMEs or Large Enterprises) with an extended collection of features. During the last few years Box has been developing a rich online document editor and is not just focused on the storage offering of the service. However, in the early days of the service content visualization or edition were very limited, and it was lacking a good photo viewer or an integrated pdf viewer. During that time, Box was focused on developing an efficient and more business-oriented cloud storage service.

2.2.1 Terms

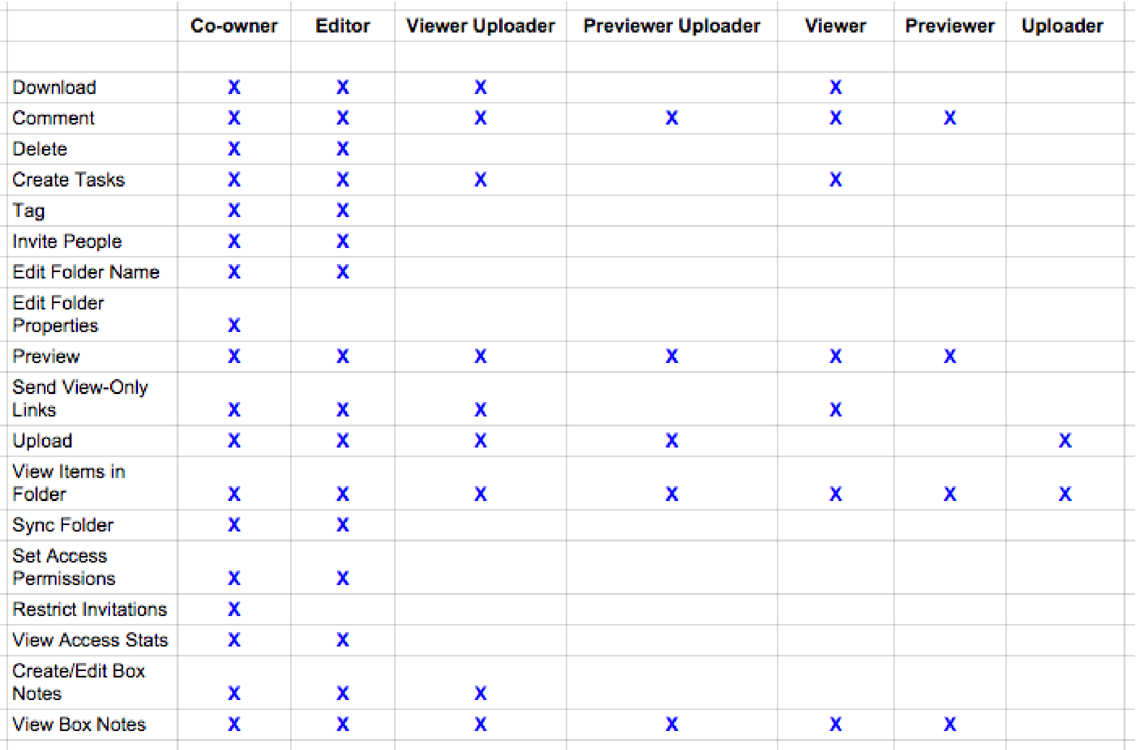
Box leaves on the hands of the user the rights of use of the content stored in its service [19]. Security and backup of the data is also handle by the customer with the possibility of contracting the backup from Box itself. One interesting remark made by Box in its terms and conditions is the fact that the data will be stored in the United Sates of America, and that any customer agrees with the processing of information according to US federal regulations.

2.2.2 Security

Box is the most business-oriented cloud storage service in the market and its security is focused on the integration of its services with the needs of a customer's company [20] [17] [16] [22].

Box owns servers which are deployed on different locations across the United States of America. Uses AES of 256 bits as back-end cypher to encrypt customer data and prevent other users to interfere in their data. This feature is not new on these type of services, however Box goes a step beyond by allowing the customers to upload their own keys for the encryption. Box applies security in layers and so, on top of the crypto security on the backend, the service uses TLS tunnels to communicate the sync clients or the browser on the customer devices, avoiding securing transfer plain traffic during the data transportation.

The common functionality offered by the different storage providers reviewed in this document - namely, file sharing - is very well implemented in Box. While the free version implements basic sharing like the ones offered by Dropbox, the paid Box version offers a very granular functionality for the control of the files and folders [25]. The sharing functionality allows group management on every file and folder. Figure 2.1 shows the roles and permissions over any folder or file.



	Co-owner	Editor	Viewer Uploader	Previewer Uploader	Viewer	Previewer	Uploader
Download	X	X	X		X		
Comment	X	X	X	X	X	X	
Delete	X	X					
Create Tasks	X	X	X		X		
Tag	X	X					
Invite People	X	X					
Edit Folder Name	X	X					
Edit Folder Properties	X						
Preview	X	X	X	X	X	X	
Send View-Only Links	X	X	X		X		
Upload	X	X	X	X			X
View Items in Folder	X	X	X	X	X	X	X
Sync Folder	X	X					
Set Access Permissions	X	X					
Restrict Invitations	X						
View Access Stats	X	X					
Create/Edit Box Notes	X	X	X				
View Box Notes	X	X	X	X	X	X	

Figure 2.1: Box access levels permissions

Box stores and keeps copies of user keys copied in different locations in the data center and changes their location frequently to prevent any leaks. Another important feature of Box is the restriction of the access to the content depending on the device used, this way an admin can grant apps to sync and use Box from a central location [24].

The API provided by Box is only allows data synchronization so the Storage service cannot be natively used as datastore. To use the API a developer needs to request a unique key which will be used to authenticate and secure the application against Box's OAuth and create the secret for the TLS tunnel.

2.2.3 Authentication

Box provides authentication based on user/password for all their free services and, as the other providers, Box assesses the password strength when the new user introduces it for the first time or changes the current password. In the business accounts Box was the fist provider to introduce the SSO in its service [21] . Box uses SAML 2.0 and PEM certificates to communicate with the AD. Once the SSO is configured, users may be requested to reconnect all their devices using the new credentials from the

AD. Having a company AD or LDAP simplifies the control access management of the cloud storage infrastructure as the permissions of the different teams and departments can be managed with the permissions in the cloud storage.

Box works with several third-party SSO solutions, including:

- Intel Expressway Cloud Access 360 [55]
- Okta [73]
- Ping Identity [83]
- VMware Horizon App Manager [91]
- Citrix [27]
- OneLogin [74]
- Symantec 03 Cloud Identity and Access Control Gateway [90]
- Simplified (now RSA) [14]
- SAML federation providers

While Box was quick on offering SSO to their customers, they were one of the last ones implementing two-factor authentication. This feature is available for every user in their system. The two factor authentication, as in Dropbox, uses codes sent to a personal device (generally mobile phone) or secondary email [18]. This code or token is a one time use token used to verify the identity of the end user. The assumption behind this technique of sending the code to a different personal device or email account is that the same person who hacked the password won't have the personal device of the Cloud Service user and this way verify the identity.

2.2.4 Certifications

Box is certified with many certifications which ensure to customers that their data is secured within their infrastructure. On top of the most popular security certifications, Box is certified by the Health Insurance Portability and Accountability Act (HIPAA) which allows the storage of patient information in the US inside of Box's infrastructure.

Table 2.2 lists all the certifications obtained by Box:

Certifications
ISO 27001
SOC 1, SOC 2
CSA STAR
HIPAA , HITECH
SSAE 16 Tipo II
PCI DSS
U.S. E.U. and U.S. Swiss Safe Harbor

Table 2.2: Box Certifications

2.3 iCloud

iCloud [11] is Apple's online storage and sharing center. iCloud is not just focused on storing customer data but also to creating a seamless integration between a customer Apple ecosystem. This means that all Apple devices logged in to iCloud would share information regardless of the operating system, iOS or Mac OX. iCloud, unlike the other cloud drives analyzed in this thesis, is the only service which is not multi-platform outside of the Apple ecosystem; it is a service that can only be synchronized with Apple devices. A customer can choose the content to be synchronized via iCloud from its preferences panel, however by default it will synchronize photos, calendar, contacts, e-mail (if it is @icloud.com), documents, texts, applications, and more.

2.3.1 Terms

iCloud's terms and conditions document is not only focused on the storage service provided but applies for the whole suite [13]. It indicates that the user is responsible for backing-up its content; however, iCloud will automatically backup any iOS device if this feature is set in the customer device. Apple reserves the right to access user data in cases related to law enforcement. The user is responsible for copyright protected and agrees to have the copyright of the data stored in her account.

2.3.2 Security

Apple uses also multilayer security for iCloud [12]. The layers are divided between the end user device, the communication layer and the back-end storage where different techniques are applied. In the backend iCloud uses a minimum of AES 128 bits encryption, unlike the 256 bits used by other cloud services. However, Apple has implemented Keychain: an application which sits on the client side and generates unique keys for each of the applications that would synchronize with iCloud. This application encrypts iCloud keys on the user device (Mac, iPhone or iPad) with AES 256 bits. Using this technique Apple introduces an extra security layer encrypting every customer data with a different key preventing the leak of all customer details in case one of the keys is decrypted. For the communication between end user devices and iCloud Apple uses TLS tunnels to encrypt data exchange.s

Apple is currently developing a full API for iCloud but offers a partial one called CloudKit [10]. Before starting to interact with iCloud's database CloudKit need to authenticate the mobile or web applications with a unique key provided obtained when the application is registered. Because iCloud stores end users details the user needs to be authenticated against iCloud's database to start the message exchange, this authentication needs end user's private key (stored in keychain in his device) and the application key. After this second authentication the mobile or web application would be granted access iCloud's end user data.

2.3.2.1 Authentication

iCloud uses a two-factor authentication for user authentication [9]. As in the other services, the client will receive a text message or email with the token in order to login. However, when accessing the service from the latest iPhones or iPads the user can make use of the biometric sensor (touch id) to authenticate herself. Unlike in the other services, Apple does not allow the integration of iCloud with any Active Directory and every user needs to login with an Apple account in order to use the service.

2.3.3 Certifications

Unfortunately, Apple does not provide any official certification for iCloud.

2.4 Cloud Drive and Amazon S3

Amazon Cloud Drive [8] is the storage service that Amazon has deployed mainly for individual users. Cloud Drive differs from other services as it offers unlimited storage of images. This service is deployed on top of the famous and veteran Amazon S3 [7] which is the most common storage used for

Amazon Web Services. This makes it so that Amazon Cloud Drive inherits most of the security features of S3.

2.4.1 Terms

According to Amazon's terms of use [4], the customer can make use of the service to store, download, modify and share her own files. The customer is held responsible for any virus/malware files in their space and also for any copyright breach of the content in the stored files in the case of an investigation.

2.4.2 Security

Amazon uses the multilayer security strategy to secure its cloud storage. The communication between the service and the user client (sync client, web browser, etc.) is secured using TLS tunnels to encrypt the communication. Once the data is in-house, Amazon encrypts it with AES 256 bit keys. This feature differs the use of Cloud Drive is chosen, or if a company decides to integrate Amazon S3 directly. While Cloud Drive uses an Amazon pre-generated key to encrypt the data, using S3 directly a company can upload its own set of keys and store them directly on the AKMS (Amazon key management service), however S3 offers the possibility of using a key generated by Amazon.

Amazon Cloud Drive offers an API to allow developers synchronize data from mobile and web applications [3]. To start using Cloud Drive API developers need to obtain a unique token that would register the application in Amazon. Then developers need to request access which would be analyzed by Amazon Engineers to whitelist it. The web or mobile application developed can have access to all the documents stored or just to a subset of directories and files. Finally the application would need to authenticate the end user to obtain an access token the Cloud Storage services. These access tokens are valid for 60 minutes and need renewal once they expire.

When using Amazon S3 directly, a company can directly use Amazon IAM (Identity and Access Management) which allows to organize the access to the data in a very fine and customize manner. With IAM the following properties can be configured:

- Users: create individual users.
- Groups: manage permissions with groups.
- Permissions: grant least privilege.

- Auditing: turn on AWS CloudTrail.
- Password: configure a strong password policy.
- MFA: enable MFA for privileged users.
- Roles: use IAM roles for EC2 instances.
- Sharing: use IAM roles to share access.
- Rotate: rotate security credentials regularly.
- Conditions: restrict privileged access further with conditions.
- Root: reduce/remove use of root.

In addition to the user management, groups and roles inside the Amazon S3 tree, the service also permits the definition of Access Control Lists (ACL). With the ACLs a n Amazon S3 customer can restrict the networks, IP addresses or domains granted to access the cloud storage.

Amazon S3 provides a full Software Development Kit (SDK) to the developers [5]. Amazon S3 API follows a different grant access than the Cloud Drive API. Developers don't need to follow the whitelist application process and can start querying the Cloud Storage back end directly after obtaining the application token. The SDK allow developers to work with the data before uploading it to the Storage Service. This means that a web or mobile application developed with the Amazon SDK can encrypt the data on the client side before uploading using the same mechanism used in Amazon S3 backend.

2.4.2.1 Authentication

Amazon Cloud Drive and Amazon S3 use SSO [15] to authenticate users on Amazon services with a single user ID and password. The SSO used in Cloud Drive only allows users to use their Amazon account, but for S3 the SSO is more advanced and uses SAML 2.0 tokens to connect 3rd party certificate authorities such as a company's active directory. As in the other cloud services, a two-step authentication is available for any account regardless of the CA used.

2.4.3 Certifications

Amazon is compliant with the following security standards [6]:

Certifications
HIPAA
SOC 1/SSAE 16/ISAE 3402 (previously, SAS70)
SOC 2
SOC 3
PCI DSS level 1
ISO 27001
FedRAMP(SM)
DIACAP y FISMA
ITAR
FIPS 140-2
CSA
MPAA

Table 2.3: Amazon Certifications

2.5 GoogleDrive

Google Drive [50] for work is Google's online storage for companies who want to store and synchronize their data between their employees and employee devices. Being a Google product, the service integrates perfectly with other Google services such as Gmail or Google Docs, which uses Google Drive as default storage for documents. Google offers clients for the most popular mobile and PC operating systems helping with the synchronization of documents between the company and the backend service.

2.5.1 Terms

Google's terms of services is set for the whole google apps suite [47]. Google Drive is one of them and within the scope of this thesis we will focus on the policy regarding stored content, i.e any content within an account (documents, e-mails, photos,..). For this content Google offers a copyright protection service in case a user feels someone is using their content to their benefit. However, Google itself analyses the content in a user's files in order to provide better and more accurate search results but also for commercial purposes. As in the other cloud storage services, the users themselves are in charge of backups and of access management of their data.

2.5.2 Security

Google is also using a multilayer security for its service [53] [54]. The communications are secured using TLS tunnels for which RSA 2048 bit keys, as in the rest of the services but OwnCloud, are used since August 1, 2013 [46]. Once a company's data is in the datacenter it is logically isolated from other customers', as if it would have its own servers as per Google's application design and architecture.

Sharing files and folders[52]: Google Drive creates a secured link that the user can share with either specific people, to anyone who has the link or make completely public. The user can set basic permissions to the shared content such as edit, view and comment (shared folders cannot be commented). However, to edit a shared file, the other user needs to be logged in with his user account.

Google offers a full SDK to integrate mobile or web applications with Google Drive [51]. Google's SDK covers client and server side which allows mobile and web applications work offline with the back end storage. To start an application a developer needs to get a set of keys, a key for the server side and a key for the client side. The combination of these keys and the unique secret toke associated to each of them grant the application access to Google Drive. Before starting the communication between Google Drive and the web/mobile application Google needs to issue a security token to establish a secure communication layer between the two entities. To issue this token Google needs also the end user credentials and verify them against the Authorization service.

2.5.2.1 Authentication

Google Drive, as part of the Google Apps suite, requires a Google account to access the service. This account password is evaluated when it's set and when it is reset assessing its strength. Two-factor authentication is available for all service users [49]. With this service Google will send a one time token code to a personal device or email to verify the identity of the end user and grant access to the data. Another security feature of Google Apps is the automatic alerts when someone starts a new connection with the same account on another device or browser, or at a different location, that are not the usual for that user. Similarly to other cloud services, Google allows to use an existing LDAP as a user database by using Google Apps Directory Sync (GADS) [48] to synchronize customer's LDAP with their Google accounts.

2.5.3 Certification

Google's cloud drive can store any data for customers around the world. Table 2.4 summarizes Google's security certifications:

Certifications
SOC1 (SSAE-16/ISAE-3402), SOC2, SOC3
ISO27001
HIPAA
FISMA
FERPA and COPPA
U.S.-EU Safe Harbor Framework

Table 2.4: Google Certifications

2.6 One Drive

In the last few years we've seen a migration of Microsoft business from the OS in personal devices (Microsoft Windows) to the cloud. This migration has been driven by competition as most of its competitors started as cloud providers earlier than this Redmond giant attracting more and more companies to their services. Starting with Microsoft Azure, its IaaS, Microsoft has been migrating to the cloud as many services as possible. OneDrive citeod:onedrive is Microsoft's cloud storage offering and it is nowadays the default storage system for the online cloud of Microsoft Office, Office 365. OneDrive is not only the designated Office's 365 storage but it also includes a high quality integration with Outlook and the latest versions of Microsoft Windows (8 and above).

2.6.1 Terms

Microsoft applies the same terms and conditions across a range of services like Outlook.com, Office365 and OneDrive [62]. This make the terms very generic and not specific for OneDrive. However, the content is covered under section 3 of the agreement which is in charge of the content stored at Microsoft's online services. In this section Microsoft gives the user the ownership of the stored data, and also clarifies that the user is in charge of the access management and permissions for the data stored. Microsoft reserves the right of accessing your data for commercial and legal issues if needed, this right applies worldwide and not only certain areas. With the list of agreed content and actions that can be stored at Microsoft OneDrive or any other Cloud Service, Microsoft can remove any content that is not align with the list indicated in the point 3.7 of the terms document.

2.6.2 Security

To achieve a secured service, Microsoft is implementing multilayer security to communication an end storage stack. The connections between the customer's computer and the final storage are encrypted using TLS tunnels and a backend encrypted storage based on AES 256 bit [65]. For business customers, Microsoft is expecting to store confidential or sensitive data. Therefore, to achieve an even higher level of security for this types of users, Microsoft separates files in the final storage, splits big files and separates them as well as encrypts every file or piece of a file with a unique key. Keys are later stored at a password protected keystore whose password changes frequently. All encryptions and passwords used by Microsoft are FIPS 140-2 compliant. As other cloud storage services, Microsofts applies deduplication for customers data, and applies physical security, infrastructure duplicity and periodical backup to keep high availability and roll back of customer's data. File sharing is made by publishing a link protected by HTTPS where the user can specify the role applied to the recipients [60]. They would be able to edit, view (read only) or the content could also be made public, allowing people to search and use the information, but not edit it. If sharing is between two OneDrive users the permissions are restricted to read only and edit. Hence, OneDrive's granularity is not as accurate as Box's.

OneDrive offers an API for developers who want to develop a mobile, desktop or web application and synchronize data with OneDrive [63]. As in the previous cases to connect an application to the Cloud Storage service this needs to be registered. The registration process in the case of OneDrive is different for OneDrive personal or OneDrive business. For personal use Microsoft only need the application to be registered in Microsoft'a "App Registration" system [64]. This process will create an application identifier (key) and a secret hash like in the rest of services studied in the thesis. With these two parameters and the application would authenticate and get access to OneDrive.

However the registration process for business need extra steps to register the application. First the developers an Office 356 account, not just a Microsoft account as for personal use. Then setup an Azure Active Directory tenant which will give access to Azure's administration console allowing users, roles and multiple applications management. Finally register the application against the Azure Active Directory space linked to the Office 365 Account. Once the application is registered in Microsoft it will be able to access OneDrive for Business.

2.6.2.1 Authentication

User authentication on OneDrive is implemented in different ways. The most common is using a Microsoft account to access your private data. This account is the same as the customer would use to login to Outlook.com or Office 365 and must be password protected. A second layer of security is applied with a two-factor authentication sending a text message, email or phone call to the customer's personal device or mailbox. As can be seen from the above, users are in fact authenticated using Single Sign On, as many Microsoft services can be access with a single account so. In this respect, Microsoft has the ability to connect OneDrive seamlessly with a company's Active Directory organization, allowing employees to use their user accounts to authenticate against OneDrive and Office 365.

2.6.3 Certifications

Microsoft Office 365, where One Cloud is included, is compliance with many security standards [66] . Table 2.5 list the certifications obtained for this platform.

Certifications
ISO 27001
FISMA/FedRAMP Authority to Operate
Microsoft Data Processing Agreement
HIPAA Business Associate Agreement
SAS79 / SSAE 16 Assessments
PCI DSS
PCI governed PAN data
U.S. E.U. and U.S. Swiss Safe Harbor

Table 2.5: OneDrive Certifications

2.7 OwnCloud

OwnCloud [78] is the only example of an open source cloud storage service included in this thesis. The service is the only one that a company can install in a private cloud or inside a company's network. While OwnCloud offers the standard operations of commercial cloud storage services shown previously, it also has an enterpriser version licensed and supported by the OwnCloud team. Not only can OwnCloud be used to store and synchronize files and folders, it can also integrate calendars, task lists and other applications.

Being the only service that is available for deployment within the private infrastructure of a company, it is the most recommended for those companies whose information is especially confidential or sensitive as the data will not be shared with any other customer on an external public platform.

2.7.1 Terms

OwnCloud, as mentioned above, is an Open Source Software storage platform. However, it has a commercial brand known as Enterprise Edition which protects those modules developed specifically for this edition giving the copyright to the OwnCloud team [81]. With regards to customer rights and obligations, as well as the ownership of content, specifics are not mentioned as OwnCloud would be deployed and managed by the end user company.

2.7.2 Security

As OwnCloud is a system that can be deployed within a company's infrastructure it implies direct security as information will be kept in-house or on a private cloud [77]. However, this could generate an overhead for the company's IT department related to ensuring high availability of the data. The IT department would need to create proper security controls, backup and restore policy and ensure the connections between employees and the final storage. These two features were implicitly delivered when contracting an external cloud storage like the ones studied in this thesis; however, in this case they fall under the responsibility of the end-user company. As a platform directly managed by the company, OwnCloud permits the company to choose the encryption [79] mechanism needed for the nature of the data stored; however, it is good practice to use the highest level as possible. OwnCloud by default uses AES 256 bit cyphers meeting the same characteristics as the commercial services described in previous sections. OwnCloud creates a public/private key of 4096 bits for each user and file added to their client to securely protect the stored data in combination with the AES 256 bit cypher. OwnCloud requires the configuration of a firewall to implement ACLs and close the ports to the minimum needed, normally only 443 (HTTPS) [80] is required. If the company does not have a firewall in front of the service, the following php modules can be activated to add an extra security layer: ModSecurity and Mod_evasive . As OwnCloud would normally be deployed on a Linux machine, administrators can activate SELinux or AppArmor. However, if not configured properly these systems can be deactivated to install the cloud storage service. Once the data is uploaded to the cloud service, ClamAV (if installed) would scan all the files for viruses and will place infected files in quarantine for administrators to check them. File sharing in OwnCloud sits in between the the advanced features of some of the services studied and the basic services offered by others. These are the sharing options available in OwnCloud:

- Allowing users to share files
- Allowing users to create public links
- Requiring a password on public links
- Allowing public uploads to public links
- Requiring an expiration date on public share links
- Allowing re-sharing
- Restricting sharing to group members only
- Allowing email notifications of new public links
- Excluding groups from creating shares

OwnCloud offers an API to extend the functionality of the service [82]. Since the last mayor version of OwnCloud 8.0.0, the security has been improved extending the security API exposing methods for encrypting or generate hashes or random tokens. The crypto library, in charge of the encryption of data, uses AES-CBC to encrypt the data.To deploy a new application in OwnCloud, developers need to register on OwnCloud's web site and register the application, once registered this will be evaluated by a committee of OwnCloud developers for is acceptance to the public OwnCloud catalog.

2.7.2.1 Authentication

OwnCloud has its own authentication database to create user/password authentication within the scope of the service. OwnCloud also provides a SSO service to connect the company's authentication service (Active Directory or LDAP) to OwnCloud using SAML 2.0, as is the case for the other commercial services reviewed above.

2.7.3 Certifications

OwnCloud by itself does not provide any certification compliance. It is on the hands of the company deploying OwnCloud the job of meeting the requirements needed to certify OwnCloud with any security certification.

2.8 Comparison

In the previous sections of this chapter we have seen specific security characteristics of 7 cloud storage services that are currently popular with companies. The service descriptions provided in the previous sections is based on each of the service's description and support pages. In this section, the main commonalities and differences between these services are summarized.

Figure 2.2: Storage Cloud

Some of the security characteristics have been found for all the providers outside of the scope of the characteristics described in chapter 1:

High availability: Physical security provided to their customers; all operate in data centers (with the exception of OwnCloud where the customer is responsible for its deployment) where the data is distributed across the data center minimizing the data loss if part of the data center has an outage. Also, they all guarantee high availability using at least the well known n+1 equipment.

Data encryption in house: Is something where most of the services coincide using AES 256 bits encryption - all but iCloud, which minimum encryption is AES 128 bits. However, there are two services which differ in the encryption applied to the data: one of them is OneDrive which encrypts all customer files with a unique key and divides big files into small pieces which are then encrypted. The key management is done by a central keystore. The other service to apply extra security is OwnCloud, which creates a single key of 4096 bits for every file stored.

Periodical backup: Using their corresponding synchronization clients, customer data is stored locally and in the cloud maintaining two copies in different locations. In addition, all the services realize periodical backups of customer's data that are stored and encrypted on a different platform. Nonetheless, this backup feature is not always available for free accounts.

Certification compliance: In this topi all services, but OwnCloud and iCloud which information is not public, possess several security certifications which help a potential customer to choose between the different providers depending of its needs and data to be stored. It is good to highlight the best effort of the cloud storage providers of providing control and analysis tools to their customers for auditory needs.

For the characteristics indicated in chapter one these are the comparisons for the studied providers:

Online Drive: All the services offer the functionality of store, edit and query documents from different devices (mobile, tablet, computer,...). Also all of them have develop synchronization clients to simplify the document management between the customer device and the server side of the service. Most of the providers offer clients for the most common OS in the market, but iCloud is only available for iOS and Mac OX.

In all the services user credentials are needed to access the data. To increase the security all services have implemented two-factor authentication mechanisms sending one-time use tokens to a device or an email account of the customer.

Only Box, Dropbox, OneDrive and OwnCloud support the authentication between companies CA, normally their LDAP service or their Active Directory, using SAML 2.0 to perform this federation. Google, on the contrary, can federate other CA using their exposed API, but even then users are required to have a Google account linked. In the case of Amazon, this option is not supported on CloudDrive it is on Amazon S3. iCloud is the only service that does not perform any kind of federation and an Apple account is mandatory to access the service.

File sharing and user management are two key factors of this type of storage since they allow collaboration between users on the same document or project - a function highly relevant for some businesses. These two categories are compared together because of the close link that they have. This point has also been the most divergent among those analyzed. All the services are sharing files and folders exposing an HTTPS link or sharing the shared item between the two users. Services like Dropbox, CloudDrive, iCloud or GoogleDrive are only allowing to share the link with other users, make it public or sending a link to specific people via email (in which case it will be read only). OwnCloud provides more granularity allowing groups, creating password-protected links or even restrictions on the type of devices that connect to the storage (mobile, sync client or web). However, the richest most sophisticated user and file sharing management is offered by Box. With Box groups and roles for each user or group can be defined. Combining those two factors, as many combinations as needed can be created for a specific shared folder. Box also allows for the creation of password protected links or links with expiration dates. OneDrive is positioned in the middle in this respect, as it support the use of the groups created in the company's active directory for the purpose of file sharing. Figure 2.3 places the Cloud Services rank based on the user management granularity:

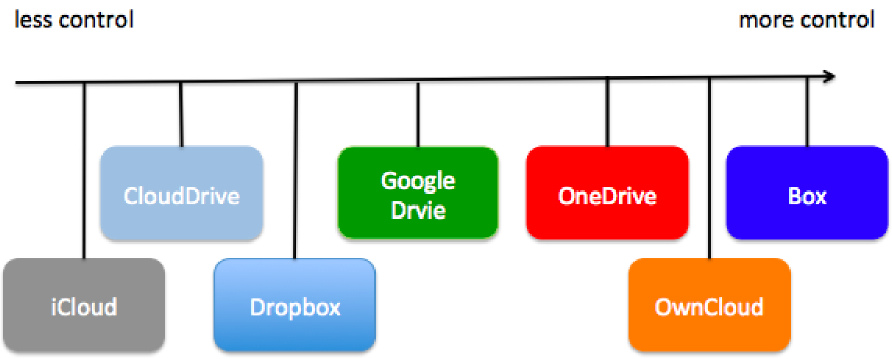


Figure 2.3: Online drive user management comparison

Datastore: In this category only Drobox, Amazon with Amazon S3 and Google with its cloud platform storage meet this characteristic. They allow the use of their services as the native datastore for a custom application developed. As well as for the Online Drive, all the content stored in these platforms is encrypted and replicated across the datacenter.

Transport: All the services studied implement SSL/TLS tunnels to secure the communications and create a first layer of security for their services. This means that by default all the services use HTTPS to drive their transport when using the web browser as a client. However, when using their clients the services user their own protocol to synchronize data between the customer device and the server. Even doing a man in the middle attack the files are not transferred entirely, but only the blocks of the file that have changed are transferred. This is because they implement data deduplication on their services.

Legal issues: Terms and condition applied in all services, but OwnCloud, are essentially very similar. Most importantly, the service provider is not responsible of the data stored in their services. That means that the users agree that the stored content does not break any copyright law, and they themselves are in charge of the integrity of the data. The use of data by third party apps to which a user/company has granted access is, once again, under the responsibility of the user. All providers reserve the right of sharing customer data with the corresponding law enforcement agencies in specific situations. Providers such as Google, Amazon and Apple can also use the content stored to provide a better adaptation of search results or to provide commercial data using other services.

API: Each API is different for the Cloud Services studied. All of them implement authorization mechanisms for the users and for the web or mobile applications developed with them. All of them need al least 2 verification steps prior to publish or connect an application to the cloud storage service. Even Microsoft OneDrive developers need to pass 4 steps to publish and application with the business API. After passing these steps the application would have a unique key and secret to authenticate itself against the Cloud Storage service. After the authentication has succeed a secure communication link would be stablished between the developed application and he back-end service. Figure 2.4 describes the number of steps needed to publish an application for the different services studied.

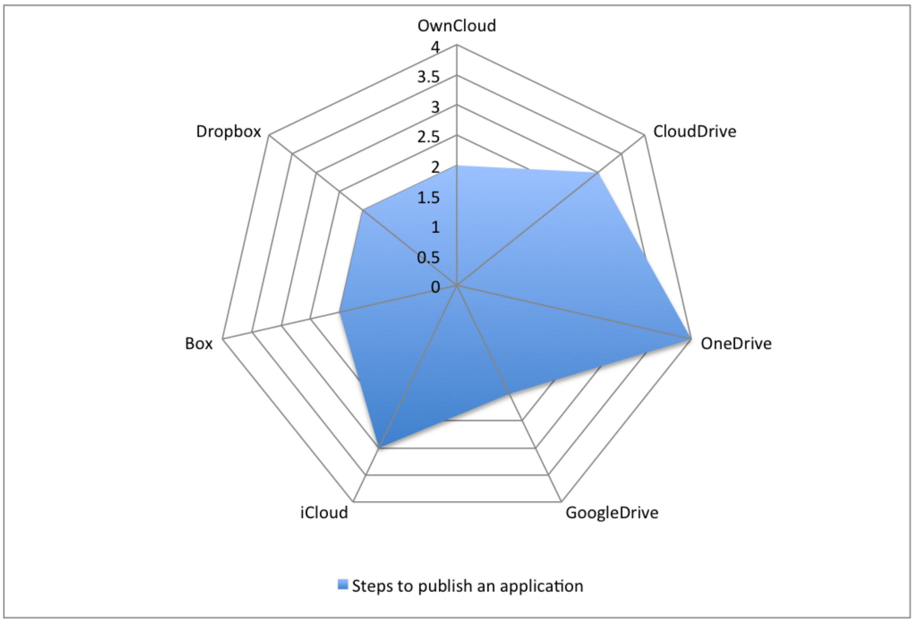


Figure 2.4: Application publishing steps for the different providers

Chapter 3

Use Cases

In this chapter I will describe the three use cases where cloud storage have been used:

Use Case 1: Cloud Storage as document repository.

Use Case 2: Cloud Storage as a datastore integrated in an application.

Use Case 3: Deploy and secure a private cloud storage.

To help with the analysis of the security I had to use different software in order to extract data from the cloud services and the connection between the server and the client. In the following paragraphs I will introduce each software used for this matter in the use cases.

Vega: Used to perform the security tests and vulnerability scans [89]. With Vega I've perform a vulnerability scan against the storage services for use case 1 and use case 3. Each use case include summary report and a more detailed report of the High and Medium vulnerabilities found are in the appendixes.

Wireshark: Used to capture traffic between the synchronization client and the server [93]. Once the capture is ready we can analyze the TCP traffic identifying the HTTPS handshake, key interchange, secured data transmission and disconnection from the server.

rbvmovi: Is a ruby library SDK for vCenter and vCloud director [84]. This open source library is used in the use case 2 to extract data from servers in a public or private cloud.

OpenTSDB: Is an open source time series database to store metrics based on time series [75]. This database in the scope of the use case 2 is used as the backend for the capacity planning implemented.

ActiveMQ: Is a queue management system which is in charge of the communication between the producer and the consumer [2]. As cloud services can be spread across multiple providers queue systems have become very popular to manage information interchange between the services and the backend. Queues allows also an easy way to manage the escalation of new nodes producing data for the application.

ClamAV: Used in use case 3, ClamAV is an open source antivirus that would scan periodically the files uploaded in the private Cloud Storage service deployed [28].

Apache: The popular web server used to deploy OwnCloud [45]. Apache has multiple security modules and supports configuration of certificates and simple ip filtering.

3.1 Use Case1: Cloud Storage as document repository

This use case covers the simplest, but most used in companies. The use of a cloud storage service as an online document repository where files and folders sync from employees devices to the cloud and vice versa.

In the overall analysis and description of the services Box has always been between well positioned in the aspects studied. Specially the key factor why Box is chosen for the use case against the other services is because of the rich user management feature that offers to its customers. Hence it is clearly the most company oriented service among the studied.

The security settings configured are:

- Strong password setting
- Two factor authentication (text message to mobile phone)
- Sharing items with people with the link, from my company and people from associated with a folder
- Allow preview and download of the shared content
- Notifications (via email) for upload, comments and deletion of files/folders
- Notification of access from a new untrusted device

The security tests performed for this use case have been:

Built in security: Test of the security provided by the service itself such as two factor authentication, notification and sharing

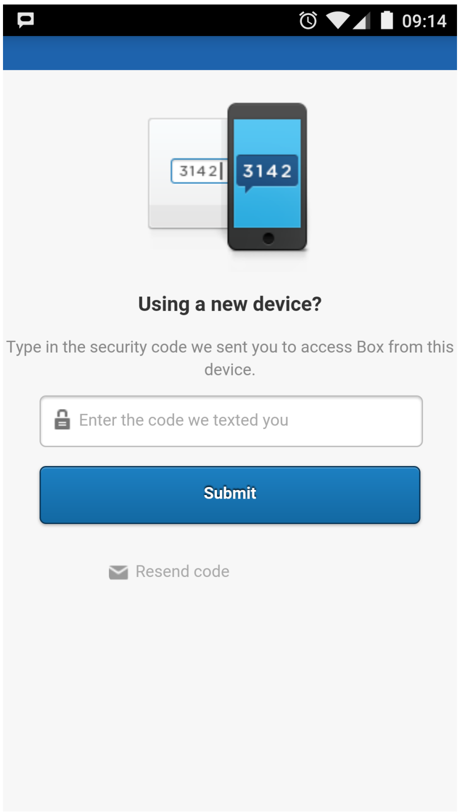
Vulnerability scan: The first thing todo is perform a vulnerability scan against the Box.com web site and subdomains while being connected to have a valid session cookie in our workstation

Traffic analysis: Complete analysis of the traffic between our workstation and Box.com using a traffic sniffer and identifying https handshake, secure transport data and disconnection

While testing the *built in security settings* for our account we've provided Box.com with an email account and a mobile phone for the two factor authentication. As the account had already the clients for Android, iPad, Box sync for Mac and the browser, these devices have been forgotten to force the two factor authentication. Once the device is connected the service won't ask for a second factor since this becomes a trusted source. In figure 3.1 is possible to appreciate the message received (top left) containing the verification code for the Box synchronization client, on top of the token Box.com sent an email verifying the addition of a new client connection.

Notifications have been sent also when sharing content and upload content to our space. Advanced features such as password protected link and expiration time link or fine grain role management are only available for the company subscription.

Box.com as the other storage providers is constantly under attack and new vulnerabilities are frequently found in its service. I have done a *vulnerability scan* using a web application vulnerability software. The software used is the above mentioned Vega. I ran Vega while being logged it and keeping a valid session cookie in my laptop. While Vega was pointed to scan the entrance www.box.com, the scanner found other adresses that were scan as well. https://app.box.com was the main one as this is the web client application of Box.com. As we can see in the figure 3.2 many vulnerabilities have been found while scanning the web application. However, despite of the amount of *Cross-Site- Script Include* vulnerabilities Vega took every embedded or used javascript as a vulnerability, most of them would be false positives (I haven't performed analysis of the scripts found as part of the scope of the thesis). *Session Cookie Without Secure Flag* is found in one of the pages of the help center, outside of the scope of the main application which, despite of being a high vulnerability the risk is lower because it does not have authentication token. The last High vulnerability

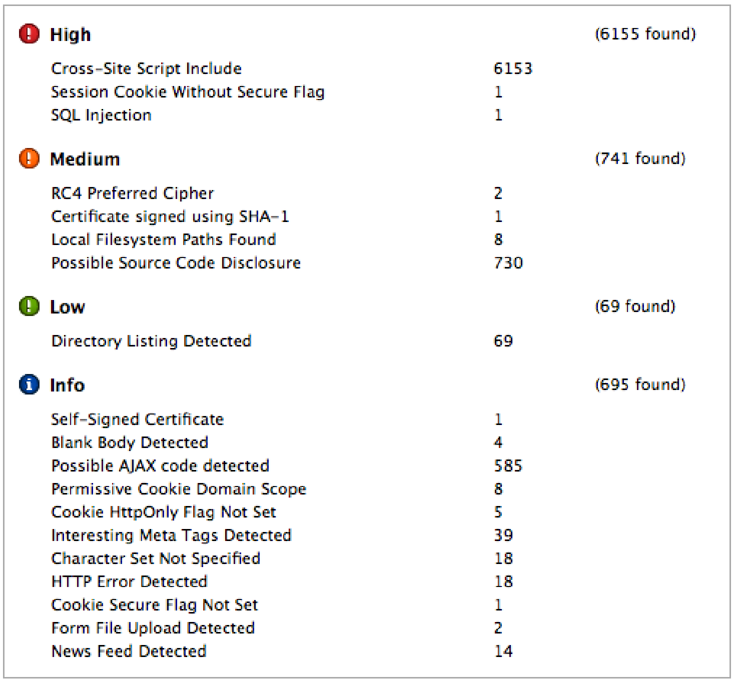


Using a new device?

Type in the security code we sent you to access Box from this device.

Figure 3.1: Box two factor authentication Android

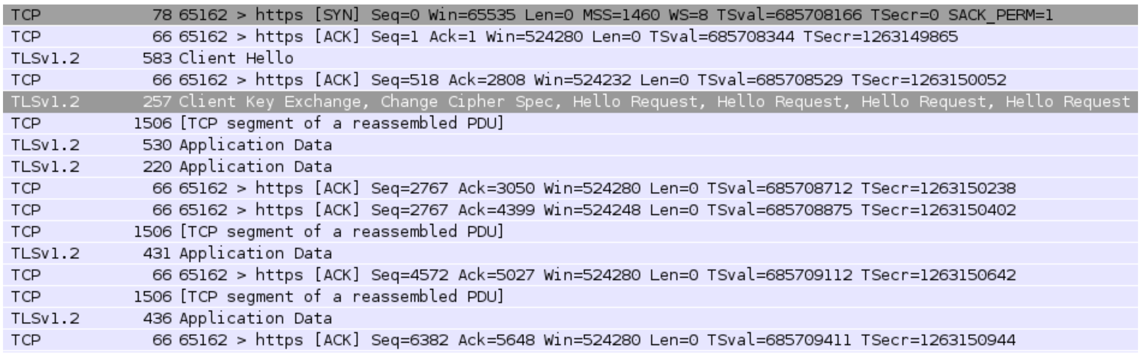
found on Box.com is a *SQL Injection* on the index page of the application. This vulnerability would allow an attacker to perform changes in the backend of the service (the database) and modify the logic of the application. In the appendix we will find a report of these and the medium vulnerabilities found.



High		(6155 found)
Cross-Site Script Include	6153	
Session Cookie Without Secure Flag	1	
SQL Injection	1	
Medium		(741 found)
RC4 Preferred Cipher	2	
Certificate signed using SHA-1	1	
Local Filesystem Paths Found	8	
Possible Source Code Disclosure	730	
Low		(69 found)
Directory Listing Detected	69	
Info		(695 found)
Self-Signed Certificate	1	
Blank Body Detected	4	
Possible AJAX code detected	585	
Permissive Cookie Domain Scope	8	
Cookie HttpOnly Flag Not Set	5	
Interesting Meta Tags Detected	39	
Character Set Not Specified	18	
HTTP Error Detected	18	
Cookie Secure Flag Not Set	1	
Form File Upload Detected	2	
News Feed Detected	14	

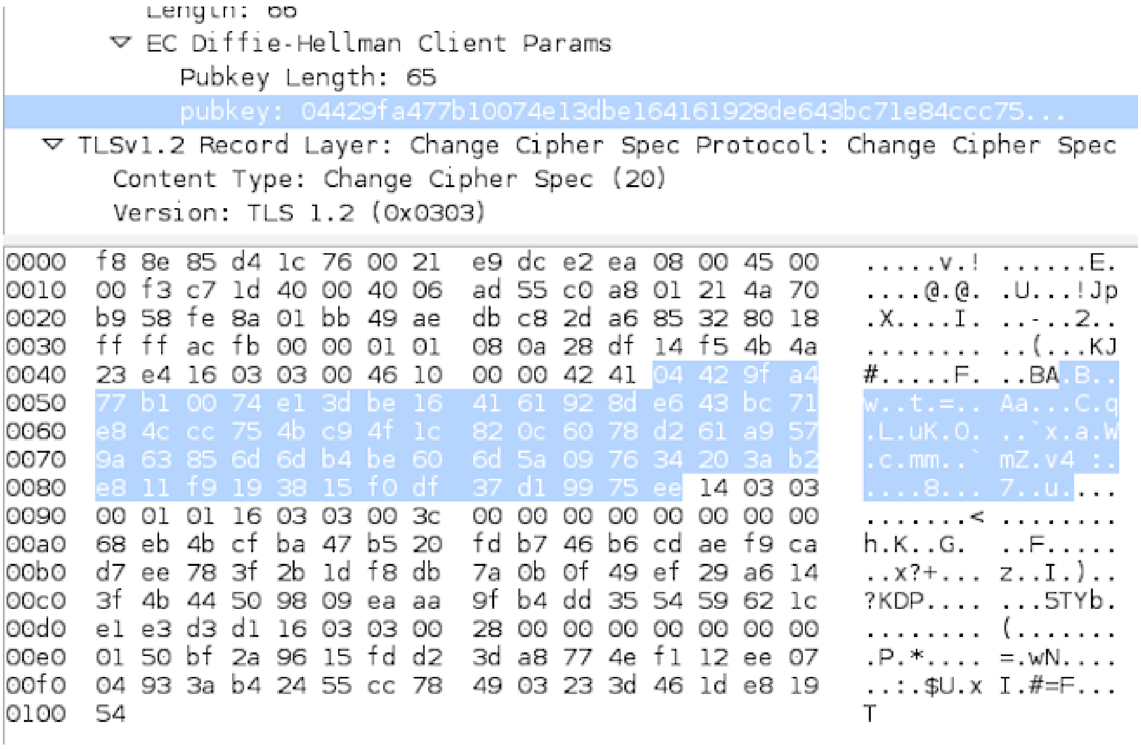
Figure 3.2: Box vulnerability scan

The final test applied to this use case is a traffic analysis between the the laptop and the service. During the analysis I logged in the service with my browser, uploaded some test content and closed the session. For the traffic analysis I have used Wireshark and applied a filter to the IP of the service. In the traffic capture as part of the handshake (figure 3.3) server and client exchange keys (figure 3.4). After the secure tunnel is stored the service would now start transferring encrypted data from and to the service using TLS v1.2. as Box.com only accepts high cyphers the tunnel can be considered as secure and data is transferred encrypted (figure 3.5).



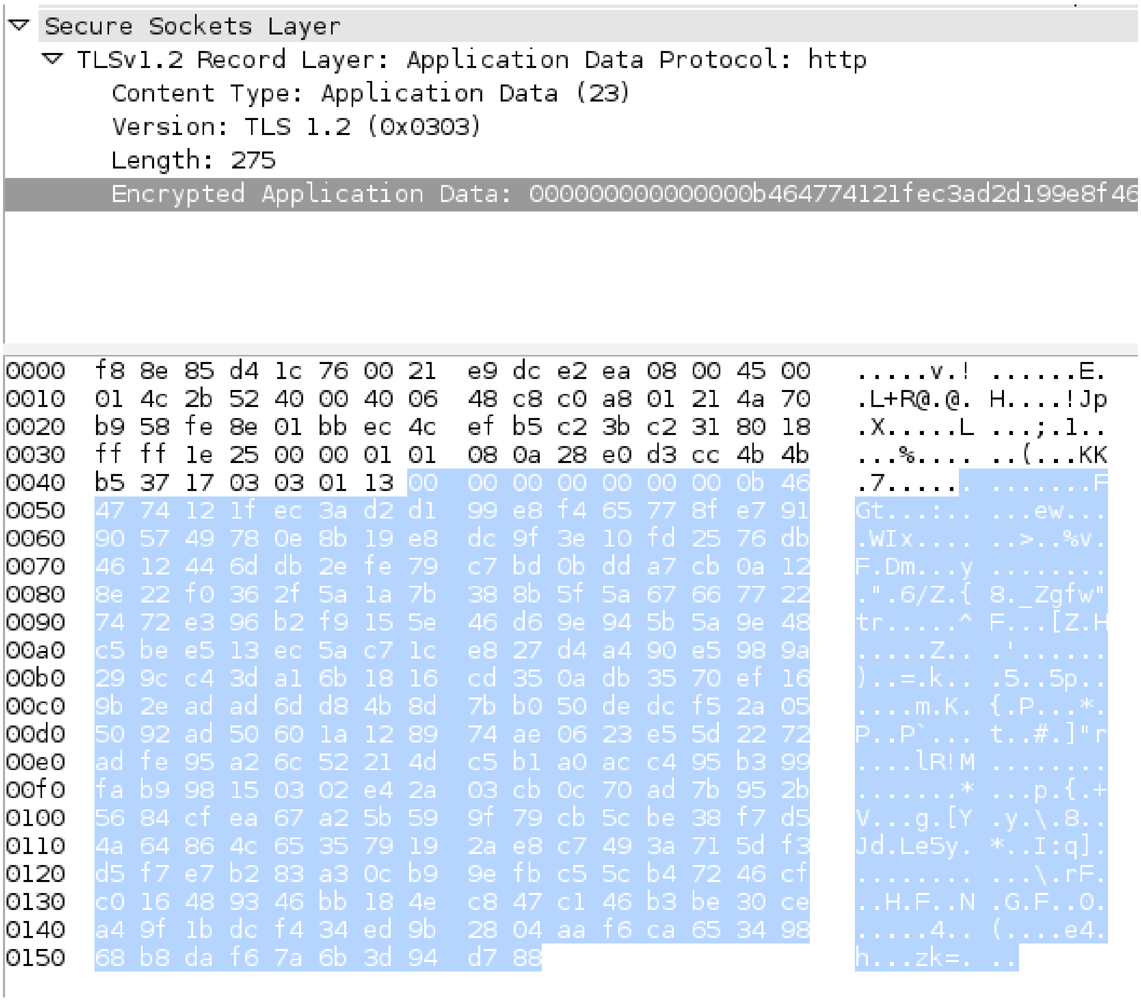
```
TCP          78 65162 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=685708166 TSecr=0 SACK_PERM=1
TCP          66 65162 > https [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=685708344 TSecr=1263149865
TLSv1.2     583 Client Hello
TCP          66 65162 > https [ACK] Seq=518 Ack=2808 Win=524232 Len=0 TSval=685708529 TSecr=1263150052
TLSv1.2     257 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
TCP        1506 [TCP segment of a reassembled PDU]
TLSv1.2     530 Application Data
TLSv1.2     220 Application Data
TCP          66 65162 > https [ACK] Seq=2767 Ack=3050 Win=524280 Len=0 TSval=685708712 TSecr=1263150238
TCP          66 65162 > https [ACK] Seq=2767 Ack=4399 Win=524248 Len=0 TSval=685708875 TSecr=1263150402
TCP        1506 [TCP segment of a reassembled PDU]
TLSv1.2     431 Application Data
TCP          66 65162 > https [ACK] Seq=4572 Ack=5027 Win=524280 Len=0 TSval=685709112 TSecr=1263150642
TCP        1506 [TCP segment of a reassembled PDU]
TLSv1.2     436 Application Data
TCP          66 65162 > https [ACK] Seq=6382 Ack=5648 Win=524280 Len=0 TSval=685709411 TSecr=1263150944
```

Figure 3.3: Box handshake



```
        Length: 66
      ▽ EC Diffie-Hellman Client Params
          Pubkey Length: 65
          pubkey: 04429fa477b10074e13dbe164161928de643bc71e84ccc75...
  ▽ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)

0000  f8 8e 85 d4 1c 76 00 21  e9 dc e2 ea 08 00 45 00   .....v.! ......E.
0010  00 f3 c7 1d 40 00 40 06  ad 55 c0 a8 01 21 4a 70   ....@.@. .U...!Jp
0020  b9 58 fe 8a 01 bb 49 ae  db c8 2d a6 85 32 80 18   .X....I. ..-..2..
0030  ff ff ac fb 00 00 01 01  08 0a 28 df 14 f5 4b 4a   ........ ..(...KJ
0040  23 e4 16 03 03 00 46 10  00 00 42 41 04 42 9f a4   #.....F. ..BA.B..
0050  77 b1 00 74 e1 3d be 16  41 61 92 8d e6 43 bc 71   w..t.=.. Aa...C.q
0060  e8 4c cc 75 4b c9 4f 1c  82 0c 60 78 d2 61 a9 57   .L.uK.O. ..`x.a.W
0070  9a 63 85 6d 6d b4 be 60  6d 5a 09 76 34 20 3a b2   .c.mm..` mZ.v4 :.
0080  e8 11 f9 19 38 15 f0 df  37 d1 99 75 ee 14 03 03   ....8... 7..u....
0090  00 01 01 16 03 03 00 3c  00 00 00 00 00 00 00 00   .......< ........
00a0  68 eb 4b cf ba 47 b5 20  fd b7 46 b6 cd ae f9 ca   h.K..G.  ..F.....
00b0  d7 ee 78 3f 2b 1d f8 db  7a 0b 0f 49 ef 29 a6 14   ..x?+... z..I.)..
00c0  3f 4b 44 50 98 09 ea aa  9f b4 dd 35 54 59 62 1c   ?KDP.... ...5TYb.
00d0  e1 e3 d3 d1 16 03 03 00  28 00 00 00 00 00 00 00   ........ (.......
00e0  01 50 bf 2a 96 15 fd d2  3d a8 77 4e f1 12 ee 07   .P.*.... =.wN....
00f0  04 93 3a b4 24 55 cc 78  49 03 23 3d 46 1d e8 19   ..:.$U.x I.#=F...
0100  54                                                 T
```

Figure 3.4: Box handshake key exchange data



```
▽ Secure Sockets Layer
  ▽ TLSv1.2 Record Layer: Application Data Protocol: http
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 275
        Encrypted Application Data: 000000000000000b464774121fec3ad2d199e8f46

0000  f8 8e 85 d4 1c 76 00 21  e9 dc e2 ea 08 00 45 00   .....v.! ......E.
0010  01 4c 2b 52 40 00 40 06  48 c8 c0 a8 01 21 4a 70   .L+R@.@. H....!Jp
0020  b9 58 fe 8e 01 bb ec 4c  ef b5 c2 3b c2 31 80 18   .X.....L ...;.1..
0030  ff ff 1e 25 00 00 01 01  08 0a 28 e0 d3 cc 4b 4b   ...%.... ..(...KK
0040  b5 37 17 03 03 01 13 00  00 00 00 00 00 00 0b 46   .7...... .......F
0050  47 74 12 1f ec 3a d2 d1  99 e8 f4 65 77 8f e7 91   Gt...:.. ...ew...
0060  90 57 49 78 0e 8b 19 e8  dc 9f 3e 10 fd 25 76 db   .WIx.... ..>..%v.
0070  46 12 44 6d db 2e fe 79  c7 bd 0b dd a7 cb 0a 12   F.Dm...y ........
0080  8e 22 f0 36 2f 5a 1a 7b  38 8b 5f 5a 67 66 77 22   .".6/Z.{ 8._Zgfw"
0090  74 72 e3 96 b2 f9 15 5e  46 d6 9e 94 5b 5a 9e 48   tr.....^ F...[Z.H
00a0  c5 be e5 13 ec 5a c7 1c  e8 27 d4 a4 90 e5 98 9a   .....Z.. .'......
00b0  29 9c c4 3d a1 6b 18 16  cd 35 0a db 35 70 ef 16   )..=.k.. .5..5p..
00c0  9b 2e ad ad 6d d8 4b 8d  7b b0 50 de dc f5 2a 05   ....m.K. {.P...*.
00d0  50 92 ad 50 60 1a 12 89  74 ae 06 23 e5 5d 22 72   P..P`... t..#.]"r
00e0  ad fe 95 a2 6c 52 21 4d  c5 b1 a0 ac c4 95 b3 99   ....lR!M ........
00f0  fa b9 98 15 03 02 e4 2a  03 cb 0c 70 ad 7b 95 2b   .......* ...p.{.+
0100  56 84 cf ea 67 a2 5b 59  9f 79 cb 5c be 38 f7 d5   V...g.[Y .y.\.8..
0110  4a 64 86 4c 65 35 79 19  2a e8 c7 49 3a 71 5d f3   Jd.Le5y. *..I:q].
0120  d5 f7 e7 b2 83 a3 0c b9  9e fb c5 5c b4 72 46 cf   ........ ...\.rF.
0130  c0 16 48 93 46 bb 18 4e  c8 47 c1 46 b3 be 30 ce   ..H.F..N .G.F..0.
0140  a4 9f 1b dc f4 34 ed 9b  28 04 aa f6 ca 65 34 98   .....4.. (....e4.
0150  68 b8 da f6 7a 6b 3d 94  d7 88                     h...zk=. ..
```

Figure 3.5: Box encrypted data transference

3.2 Use Case 2: Cloud Storage as a datastore integrated in an application

This use case will probably be the less accepted use case for a company who would want to move their data to the cloud. However is one approach that day by day companies are accepting on new services as they move to a cloud environment. This use case is motivated because of an authentication and secure transfer issue found when developing a capacity planning tool for private and public cloud. As part of the services in the portfolio of a service provider no SQL databases are offered as a service to customers. These data bases are MongoDB and the new one, still under implementation, OpenTSDB. The application developed is an extensible collector framework to collect metrics from a cloud platform (VMware vCenter in this case) and store them inside the OpenTSDB pool.

On the one side the connection y authentication of the framework with vCenter is secured using VMware's SSO and user/password authentication. Once the user is authenticated a secure connection between the framework end point and vCenter is created and maintained during the whole connection. In this specific implementation rbvomi, the SDK used to connect the developed framework and the vCenter, handles this connection. On the other side, the issue found is that OpenTSDB does not support authentication and data can be stored anonymously and the connection lacks of any security. Figure 3.6 provides an schema of the architecture, the red arrows indicates that the connection is unsecured.

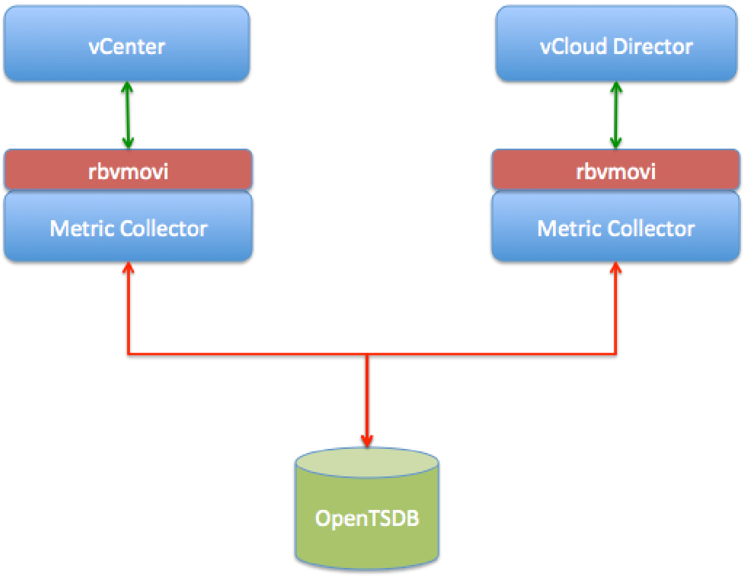


Figure 3.6: Use Case 2 Insecure Architecture

Since the storage and the framework would grow as more collectors are developed and more data is stored inside the database. The database platform will spoon new instances exposing new end points. The engineering team of the service provider has implemented a layer on top of the database that would provide security and elasticity to the service. The communication then would be driven by the use of queues, very populars nowadays when developing cloud computing services that grow and shrink with the needs of the application. ActiveMQ is in this case the queue manager selected for this scenario and Java Authentication and Authorization Service (JAAS) the authentication module [85] [76]. With this layer in the middle the communication between the collector framework and the database is secured and extensible adding new database instances or new collectors consuming or producing data in the queue. Figure 3.7 resumes the architecture of the secured service.

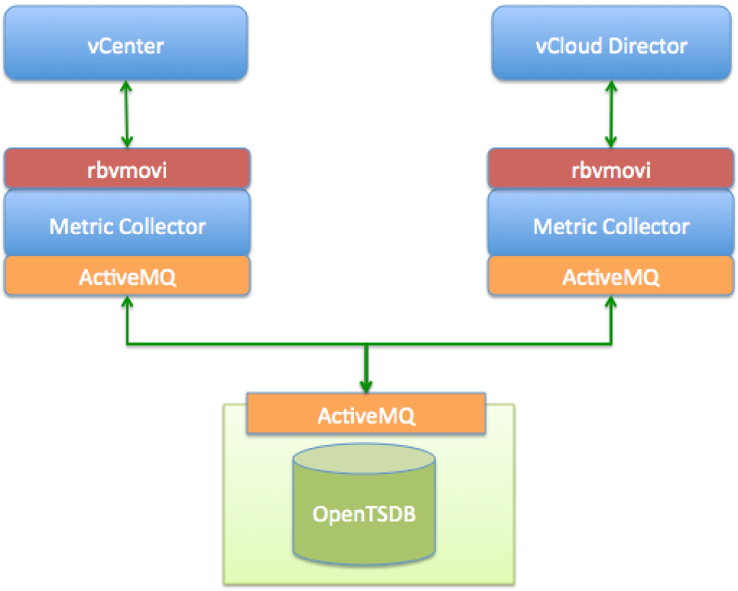


Figure 3.7: Use Case 2 Secure Architecture

The following code 3.1 is an example of producer which will write data in the queue. As parameters it uses a user, password and password to authenticate to the queue and grant the write operation.

```
Module Collector
  module Producer
    class Activemq < Base

      def setup
        @user , @pass , @host , @port , @queue = nil
      end
      def send(data)
        write(data)
      end

      def write(data)

        client = Stomp::Client.new @user, @pass, @host, @port,
           true
        data_json = JSON.generate(data)
        client.publish( @queue, data_json )
        client.close
      end

    end
  end
end
```

Listing 3.1: Queue producer code example

On the other side, above the OpenTSDB the code in 3.2 shows an example of a consumer. This consumer is located in the same VM as the database on a separate network as the different producers and with ACLs allowing connections on port 6163 (ActiveMQ port) from the networks where the producers live in. With the ACLs in the firewall in front of the database, the authentication at the ActiveMQ lever the data stored in OpenTSDB are secure.

```
#!/usr/bin/env ruby
begin; require 'rubygems'; rescue; end
require 'stomp'
require 'json'
require 'pp'

begin
    @port = 6163
    @host = ""
    @user = ""
    @password = ""
    @destination = ""

    $stderr.print "Connecting to stomp://#{@host}:#{@port} as #{
       @user}\n"
    @conn = Stomp::Connection.open(@user, @password, @host, @port,
        true)
    $stderr.print "Getting output from #{@destination}\n"

    @conn.subscribe(@destination, { :ack =>"client" })
    while true
      @msg = @conn.receive
      msg = JSON.parse(@msg.body)
      puts "====\n"
      puts "Timestamp: #{@msg.headers["timestamp"]}"
      puts "Destination: #{@msg.headers["destination"]}"
      puts "Body: #{msg.pretty_inspect}"
      puts "=====\n\n"
      @conn.ack @msg.headers["message-id"]
    end
rescue Exception => e
  puts "rescued: #{e}"
end
```

Listing 3.2: Queue consummer code example

3.3 Use Case 3: Deploy and secure a private cloud storage

This use case focuses on the deployment and security configuration of a private cloud storage service. As mentioned above, OwnCloud is an open source software which allows the installation of a storage service within a company's premises or private cloud. As being managed by the company itself, the service is free of charge if the community version is installed (raw storage and traffic are billed separately by the infrastructure provider). Managing a cloud service like this for a company becomes an overhead for the IT department.

For the execution of this use case I have used a lab environment within a private network and where the OwnCloud server is reachable from the local network only. The distribution selected to install the server is Raspbian (Debian Wheezy), the web server is Apache, ClamAV and the last stable version of OwnCloud community 8.0.3.

The installation of the web server is a simple installation using the apt-get package manager of the system. This installation is very basic and includes a basic security profile which is not active by default. The installation of the OwnCloud server has been done also in the simplest way in order to configure the security during the post installation phase. After the base installation is ready, the OwnCloud is not serving any security at all.

The following steps will explain the security of an OwnCloud service.

1. Certificate creation: the first thing to do is to purchase a certificate from a trusted CA or create a self signed certificate using OpenSSL citesoft:openssl

```
$ openssl req -new -sha256 -x509 -nodes -days 365 -out owncloud.
  company.net.pem -keyout owncloud.company.key
```

Place your certificate and the key under the necessary folder to be used by Apache.

2. Configure the OwnCloud login configuration on owncloud/config/config.php

```
'logtimezone' => 'Europe/Madrid',
'logfile' => '/var/log/owncloud.log',
'loglevel' => '2',
```

3. Open the OwnCloud apache configuration and set the following 2 lines:

```
SSLCertificateFile    /etc/ssl/certs/owncloud.home.net.pem
SSLCertificateKeyFile /etc/ssl/private/owncloud.home.net.key
```

4. Enforce the use of HTTPS only by redirecting the Apache sever listening on port 80 to redirect to the https on port 443. Restart the apache service to apply the new configuration.

```
<VirtualHost *:80>
        Redirect permanent / https://192.168.1.21/
        ErrorLog ${APACHE_LOG_DIR}/error.log
</VirtualHost>
```

5. Install fail2ban, fail2ban is a tool that scan the log file of an application and changes the firewall configuration to stop the attacker's IP.

   (a) Configure a filter to extract OwnCloud login failures, fail2ban will reconfigure the server firewall (iptables) to stop the brute force attack. Edit /etc/fail2ban/filter.d/owncloud.conf

   ```
   [Definition]
   failregex={"reqId":".*","remoteAddr":"<HOST>","app":"core","
      message":"Login failed: .*","level":2,"time":".*"}
   ```

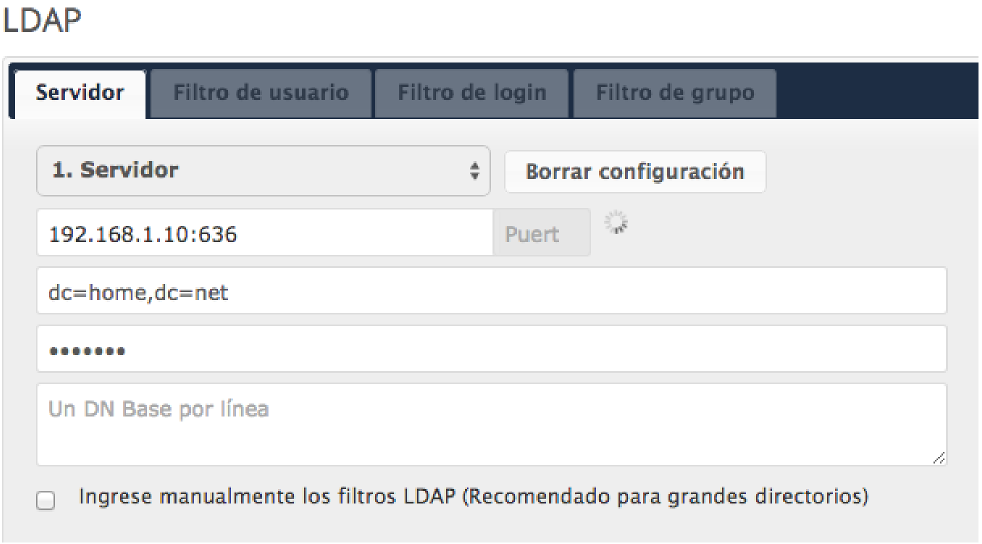
   (b) Create a jail for OwnCloud editing /etc/fail2ban/jail.local

   ```
   [owncloud]
   enabled = true
   filter  = owncloud
   port    = https
   logpath = /var/log/owncloud.log
   ```

6. Install ClamAV and Freshclam using the package manager of the server (apt-get in this case).

7. The connection with LDAP is generated via the app ”LDAP user and group backend”. With this application an administrator can filter which groups of the

domain have access to the service and the roles for each of the groups or the user login user attribute. Figure 3.8 shows the LDAP app configured for the domain home.net.



1. Servidor

192.168.1.10:636 Puert

dc=home,dc=net

•••••••

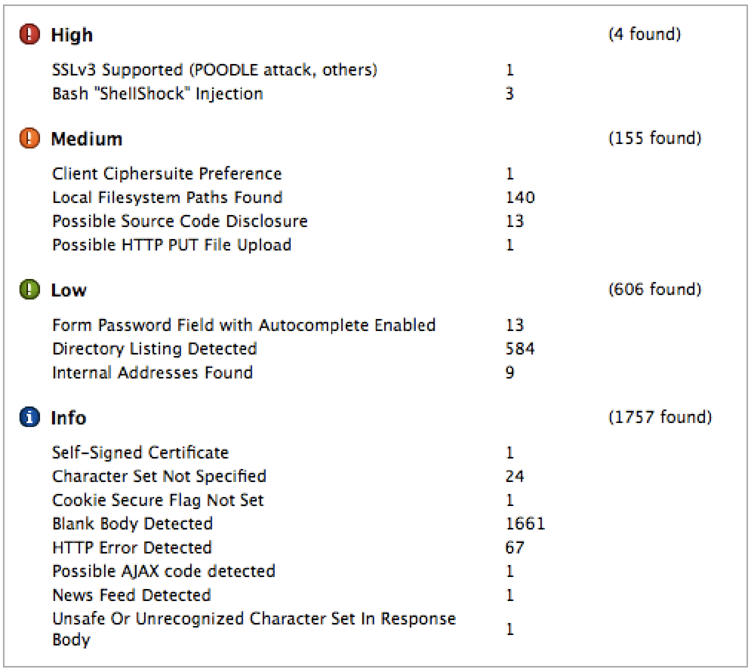
Un DN Base por línea

□ Ingrese manualmente los filtros LDAP (Recomendado para grandes directorios)

Figure 3.8: OwnCloud LDAP

At this point our OwnCloud is online using only HTTPS connection because of the redirection applied.

The following vulnerability scan represented in figure 3.9 was performed with the security applied in the steps indicated above.



High		(4 found)
SSLv3 Supported (POODLE attack, others)	1	
Bash "ShellShock" Injection	3	
Medium		(155 found)
Client Ciphersuite Preference	1	
Local Filesystem Paths Found	140	
Possible Source Code Disclosure	13	
Possible HTTP PUT File Upload	1	
Low		(606 found)
Form Password Field with Autocomplete Enabled	13	
Directory Listing Detected	584	
Internal Addresses Found	9	
Info		(1757 found)
Self-Signed Certificate	1	
Character Set Not Specified	24	
Cookie Secure Flag Not Set	1	
Blank Body Detected	1661	
HTTP Error Detected	67	
Possible AJAX code detected	1	
News Feed Detected	1	
Unsafe Or Unrecognized Character Set In Response Body	1	

Figure 3.9: OwnCloud vulnerability scan

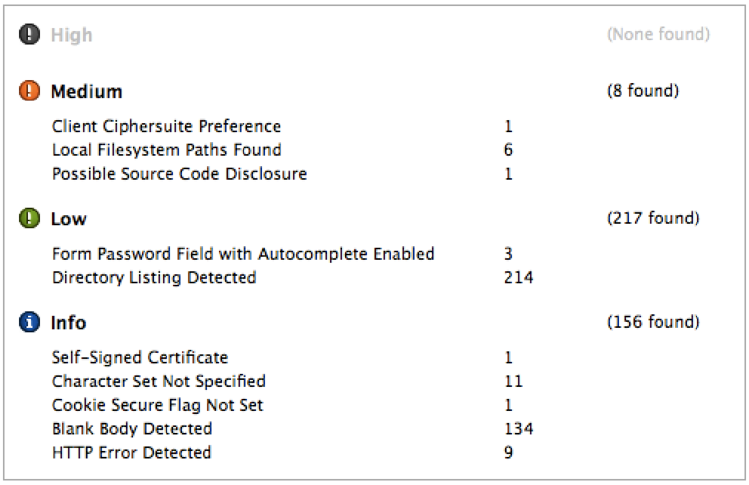
At the end of the scan there are 2 high vulnerabilities:

- SSLv3 Supported (POODLE attack, others): This vulnerability is not set on the OwnCloud service itself but in the range of cyphers accepted in our Apache server. Leaving the default configuration allows the use of a wide range of cyphers and protocols including those that are very weak such as SSL_v2 and SSL_v3. To remediate this vulnerability we need to indicate the collection of cyphers that our server would support.

```
# SSL protocol configuration
SSLProtocol All -SSLv2 -SSLv3
SSLCipherSuite HIGH:!aNULL:!MD5
```

- Bash ”ShellShock” Injection: this vulnerability discovered in Q3 of 2014 allows an attacker to convert a variable embedded on a header to a Bash environmental variable which could lead to execute commands on the host itself. To mitigate this we need to upgrade the Bash package in our server.

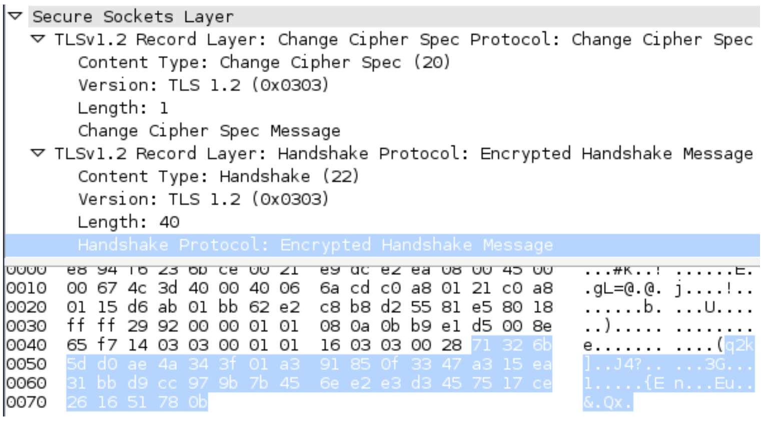
Amending the vulnerabilities following the recommendations noted before the following vulnerability. Amending high vulnerabilities, specially updating the OS would amend lower risk vulnerabilities. For the porpoise of this test the second vulnerability scan was stopped after not seeing any HIGH in the report. This second scan execution does not show any high vulnerability (figure 3.10).



```
High                                                     (None found)

Medium                                                   (8 found)
  Client Ciphersuite Preference                 1
  Local Filesystem Paths Found                  6
  Possible Source Code Disclosure               1

Low                                                      (217 found)
  Form Password Field with Autocomplete Enabled 3
  Directory Listing Detected                    214

Info                                                     (156 found)
  Self-Signed Certificate                       1
  Character Set Not Specified                   11
  Cookie Secure Flag Not Set                    1
  Blank Body Detected                           134
  HTTP Error Detected                           9
```

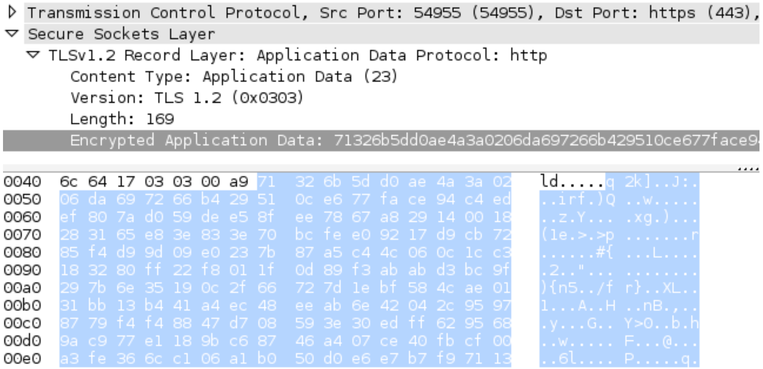
Figure 3.10: OwnCloud vulnerability scan after amending high vulnerabilities

The following Wireshark captures (figure 3.11 and figure 3.12) show the security handshake key exchange and the encrypted data transmission over TLS_v1.2 (the same as Box.com uses)



```
▽ Secure Sockets Layer
  ▽ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ▽ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
0000  e8 94 f6 23 6b ce 00 21  e9 dc e2 ea 08 00 45 00   ...#k..! ......E.
0010  00 67 4c 3d 40 00 40 06  6a cd c0 a8 01 21 c0 a8   .gL=@.@. j....!..
0020  01 15 d6 ab 01 bb 62 e2  c8 b8 d2 55 81 e5 80 18   ......b. ...U....
0030  ff ff 29 92 00 00 01 01  08 0a 0b b9 e1 d5 00 8e   ..)..... ........
0040  65 f7 14 03 03 00 01 01  16 03 03 00 28 71 32 6b   e....... ....(q2k
0050  5d d0 ae 4a 34 3f 01 a3  91 85 0f 33 47 a3 15 ea   ]..J4?.. ...3G...
0060  31 bb d9 cc 97 9b 7b 45  6e e2 e3 d3 45 75 17 ce   1.....{E n...Eu..
0070  26 16 51 78 0b                                     &.Qx.
```

Figure 3.11: OwnCloud handshake



```
▷ Transmission Control Protocol, Src Port: 54955 (54955), Dst Port: https (443),
▽ Secure Sockets Layer
  ▽ TLSv1.2 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 169
      Encrypted Application Data: 71326b5dd0ae4a3a0206da697266b429510ce677face9

0040  6c 64 17 03 03 00 a9 71  32 6b 5d d0 ae 4a 3a 02   ld.....q 2k]..J:.
0050  06 da 69 72 66 b4 29 51  0c e6 77 fa ce 94 c4 ed   ..irf.)Q ..w.....
0060  ef 80 7a d0 59 de e5 8f  ee 78 67 a8 29 14 00 18   ..z.Y... .xg.)...
0070  28 31 65 e8 3e 83 3e 70  bc fe e0 92 17 d9 cb 72   (1e.>.>p .......r
0080  85 f4 d9 9d 09 e0 23 7b  87 a5 c4 4c 06 0c 1c c3   ......#{ ...L....
0090  18 32 80 ff 22 f8 01 1f  0d 89 f3 ab ab d3 bc 9f   .2.."... ........
00a0  29 7b 6e 35 19 0c 2f 66  72 7d 1e bf 58 4c ae 01   ){n5../f r}..XL..
00b0  31 bb 13 b4 41 a4 ec 48  ee ab 6e 42 04 2c 95 97   1...A..H ..nB.,..
00c0  87 79 f4 f4 88 47 d7 08  59 3e 30 ed ff 62 95 68   .y...G.. Y>0..b.h
00d0  9a c9 77 e1 18 9b c6 87  46 a4 07 ce 40 fb cf 00   ..w..... F...@...
00e0  a3 fe 36 6c c1 06 a1 b0  50 d0 e6 e7 b7 f9 71 13   ..6l.... P.....q.
```

Figure 3.12: OwnCloud encrypted data transmission

The communications and the web server are now secured and the server is patched with no high vulnerability. But the data of our users is still stored in plain and not yet encrypted. As mentioned in the analysis of the software OwnCloud has a strong encryption mechanism built in but it is not activated by default. Instead the administrator has to install the *Server-side Encryption* application. With this application active all the user data will be encrypted on the server side using AES 256 cypher. Users will be required to logout and login to encrypt the data already stored in the server (this operation can take a long time depending on the amount of data stored). As an example we will use the same file as used to test he data transmission. A simple text file with the following text:

```
This is a text file to see the owncloud encryption
```

In the server this file is now illegible due to the encryption and only with the generated key associated with the user the file can be decrypted.

```
$:/var/www/owncloud/data/juanlu/files# cat test_owncloud_client.
    txt
HBEGIN:cipher:AES-256-CFB:HEND.....DpjaDrjiAk8W+
    jg7lW0nl60KZDFhLZJZFV2/
    KBFZlea3QBq9QqFHftXn2sbAmCGLhHTe00iv00flFtIAL6l44w4T6axx
```

Chapter 4

Conclusions

This thesis has described the main cloud storage services available in the market. This analysis aims to help companies understand the risks of the migration of their documents and data from a local storage in their offices to the cloud.

For an enterprise migrate all their content to the cloud is practically impossible but specific teams within the organization such as sales, marketing, etc. could use this type of storage to share content with customers or consume the content on mobile devices. The most recommended approach for this type of companies is the deployment of a private cloud storage (OwnCloud) where the company can control the security level and apply their own terms over the content and the use of this type of services. However, having this type of service in-house creates an overhead for the IT department which has to ensure the security, periodical backup and high availability for service and data.

SMEs and StartUPs would be the ideal target audience of this type of services. Certainly this companies are more dynamic and change faster than the enterprises. This type of service may help with the mobility and dynamic of the company and would allow them to focus on their core business. Having a cloud storage integrated with the employees credentials, i.e. Active Directory, is seamless, and from the employee point of view, the cloud storage would be as a simple folder which gets sync periodically. Generally the security concerns of this type of companies are not as strict as the ones of an enterprise, and services such as Box.com, OneDrive or Dropbox (this one in a lesser extent) provide enough security to the communication and the data stored.

Some of the providers in their business plans offer the possibility to upload custom certificates and keys to verify identities and encrypt data and communications, which adds a small bonus on the trust that a company could have on a cloud storage service as they know that the data is secured with the company's keys.

The less used use case, but growing day by day, for this type of storage is the integration as datastore for an application. This fits again with SMEs and StartUPs expertise as these services provide scalability at storage level and the data can grow as needed. Hence services such the one described in the use case 2 are becoming more popular and develop better security mechanisms. Integrating this type of storage companies will not have to address the necessity of secure and manage storage connections between the application and the backend.

Cloud computing can be coined as the next big thing in the industrial revolution. Cloud computing has substantially decreased the initial capital investment required from software companies as they can now rely on external IT infrastructures. This has had a tremendous effect on lowering barriers for software businesses and promoting software entrepreneurship. Nonetheless, ISPs, PaaS and IaaS companies are still struggling with meeting the expectations of their customers, mostly SaaS companies, for IT infrastructures that are secure, trustworthy, always available and fully elastic.

Appendix A

Box.com vulnerability report

This appendix summarizes the High and Medium vulnerabilities found by Vesa while performing the analysis of the service.

A.1 High vulnerabilities

A.1.1 *SQL Injection*

AT A GLANCE

Classification	Input Validation Error
Resource	https://app.box.com/index.php
Parameter	pic
Method	GET
Detection Type	Blind Text Injection Differential
Risk	**HIGH**

Table A.1: SQL injection summary

REQUEST

```
GET /index.php?rm=pic_storage_auth&pic=1%21rNoS5o5nQ1cNPeW8osMbEkANRH9
G12YuEt4avaya_16__6KDOJh9N6JafmceW4c9AJQ_aq81X64KZbLhalpElDNxlIaqqyJc
8O0nPURjoalTyHxibVyQqtiB-NJqlIKkltmQfbUvWglt0GQ0B8XWfvbsJ95DaCuEnc8uB0lj
V49FiB8DiwKGcKbYhlHCu3HM9ujZO3oRJ-3THlXWPUAZ0u-
fLG_nO8Rq5YWGUoPKp_s2KAf1dC
3kCg1tn94n1ude7ku8y6gX9IAgkYc6EZn7WxkrbWPSZQC2ps51MbjV
AWDa8tovHqNH5hPtfBuKmMwyHKs.’"
```

DISCUSSION

Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintented actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.

IMPACT

- Vega has detected a possible SQL injection vulnerability.
- These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
- Attackers may be able to obtain unauthorized access to the server hosting the database

REMEDIATION

- The developer should review the request and response against the code to manually verify whether or not a vulnerability is present.
- The best defense against SQL injection vulnerabilities is to use parameterized statements.
- Sanitizing input can prevent these vulnerabilities. Variables of string types should be filtered for escape characters, and numeric types should be checked to ensure that they are valid.
- Use of stored procedures can simplify complex queries and allow for tighter access control settings.
- Configuring database access controls can limit the impact of exploited vulnerabilities. This is a mitigating strategy that can be employed in environments where the code is not modifiable.
- Object-relational mapping eliminates the need for SQL.

A.1.2 *Session Cookie Without Secure Flag*

AT A GLANCE

Classification	Information
Resource	/hc/en-us/
Risk	**HIGH**

Table A.2: Session Cookie Without Secure Flag

REQUEST

```
GET /hc/en-us/
```

RESOURCE CONTENT

```
_zendesk_shared_session=-OTM3WWY1VnE3RGFBMHBNdlNqTnpPTld6OUJ5WWJ0RklwR3VDdkt
wcmp2ZE55ZVhHMHMzUlVQNU9pczFWTkh4aXJMeWt3OG94cTZvODV4ZEJMbXJPVENyQjZEcFE
yblFWc1Z0eXZ2QmhnblJRbFozYW5YZnU4bXhlWG5hUTJxOEYwWDVHekNDK1B4dzdGT3JSUG9v
b25BPT0tLVg3Q280UWNEdmFBMjRVWERNU0FPbkE9PQ%3D%3D--b098114e6bcdd8765a496bf9
eab764cc929bad08; path=/; HttpOnly
```

DISCUSSION

Vega has detected that a known session cookie may have been set without the secure flag.

IMPACT

- Cookies can be exposed to network eavesdroppers.
- Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

REMEDIATION

- When creating the cookie in the code, set the secure flag to true.

A.1.3 *Cross-Site Script Include*

AT A GLANCE

Classification	Environment
Resource	/
Risk	**HIGH**

Table A.3: Cross-Site Script Include

REQUEST

```
GET /
```

RESOURCE CONTENT

```
Local domain: app.box.com
Script source: https://e2.boxcdn.net/_assets/js/section_application_static.mi
```

DISCUSSION

Vega detected that content on a server is including Javascript content from an unrelated domain. When this script code is fetched by a user browser and loaded into the DOM, it will have complete control over the DOM, bypassing the protection offered by the same-origin policy. Even if the source of the script code is trusted by the website operator, malicious code could be introduced if the server is ever compromised. It is strongly recommended that sensitive applications host all included Javascript locally.

IMPACT

- Vega has detected that script code is being included from an unrelated domain.
- This gives the operator of the server where the code originates control over the DOM, and the web application .
- Even if the source is trusted, there are implications if the website hosting the script code is ever compromised.

REMEDIATION

Servers should host their own Javascript, especially for critical applications.

A.2 Medium vulnerabilities

A.2.1 *Certificate signed using SHA-1*

AT A GLANCE

Classification	Configuration
Risk	**MEDIUM**

Table A.4: Certificate signed using SHA-1

DISCUSSION

Vega detected a certificate signed using SHA-1. SHA-1 is a hash algorithm used in digital signatures. It is currently considered deprecated due to the increasing feasibility in breaking it.

IMPACT

- Certificates can be forged by capable adversaries.
- Forged certificates can be used in MITM attacks against connecting clients.

REMEDIATION

- Renew certificates with SHA-256 signatures. This should be done before 2016.

A.2.2 *Local Filesystem Paths Found*

AT A GLANCE

Classification	Information
Resource	/home/ nosuchpage123
Risk	**MEDIUM**

Table A.5: Certificate signed using SHA-1

REQUEST

```
GET /home/~nosuchpage123
```

RESOURCE CONTENT

```
/home/~nosuchpage
```

DISCUSSION

Vega has detected a possible absolute filesystem path (i.e. one that is not relative to the web root). This information is sensitive, as it may reveal things about the server environment to an attacker. Knowing filesystem layout can increase the chances of success for blind attacks. Full system paths are very often found in error output. This output should never be sent to clients on production systems. It should be redirected to another output channel (such as an error log) for analysis by developers and system administrators.

IMPACT

- Vega has detected what may be absolute filesystem paths in scanned content.
- Disclosure of these paths reveals information about the filesystem layout.
- This information can be sensitive, its disclosure can increase the chances of success for other attacks.

REMEDIATION

- Absolute paths are often found in error output.
- Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers. This output should be sent to another output stream, such as an error log.

A.2.3 *RC4 Preferred Cipher*

AT A GLANCE

Classification	Configuration
Risk	**MEDIUM**

Table A.6: RC4 Preferred Cipher

DISCUSSION

Vega detected RC4 as a cipher prioritized by the vendor. RC4 has known issues and it is suspected that even more severe vulnerabilities may be unknown publicly. It is recommended that more secure ciphers be prioritized by the server. Consult the guidance provided by Mozilla in their Server Side TLS configuration guide.

IMPACT

- RC4 has known weaknesses and may be found to be broken in the future.
- Data confidentiality may be at risk.

REMEDIATION

- RC4 should not be prioritized as the most preferred cipher by the server.
- This can be changed in the server configuration settings. Mozilla has guidelines on server-side TLS configuration for a number of implementations.

The HTTPS server would likely need to be restarted for configuration changes to take effect.

A.2.4 *Possible Source Code Disclosure*

AT A GLANCE

Classification	Information
Resource	/_assets/js/section_marketing_global-E3-R6k.js
Risk	**MEDIUM**

Table A.7: RC4 Preferred Cipher

REQUEST

```
GET /_assets/js/section_marketing_global-E3-R6k.js
```

RESOURCE CONTENT

```
Possible ASP or JSP code:
<%=\s*(\w+)\s*%>
```

DISCUSSION

Vega has detected fragments of text that match signatures of application source code. Application source code unintentedly visible to remote clients can be a security vulnerability. This can occur in applications using technologies such as PHP and JSP, which allow for code to be mixed with static presentation content. For example, in-line code is sometimes commented using HTML comments, resulting in it being transmitted to remote clients. For an attacker, source code can reveal information about the nature of the application, such as its design or the use of third-party components. Sometimes sensitive information, such as a database connection string, can be included in source code.

IMPACT

- Could result in disclosure of sensitive information to attackers.
- Source code fragments can include information about the design/structure of the application, including use of third-party components.
- This information may not otherwise be easily known by an adversary.
- Sometimes source code also contains highly sensitive information, such as passwords (database connection strings).

REMEDIATION

- The developer should verify that the output detected by Vega is in fact application source code.

The cause should be determined, and the material removed or prevented from being output.

Appendix B

OwnCloud vulnerability report

This appendix summarizes the High and Medium vulnerabilities found by Vesa while performing the analysis of the service.

B.1 High vulnerabilities

B.1.1 ***SSLv3 Supported (POODLE attack, others)***

AT A GLANCE

Classification	Configuration
Risk	**HIGH**

Table B.1: SSLv3 Supported (POODLE attack, others)

DISCUSSION

Vega detected server support for SSL 3.0. This version of the protocol has numerous known weaknesses and is considered deprecated in favor of newer versions of TLS. Some of the known weaknesses can result in a compromise of sensitive data such as user session tokens.

IMPACT

- Data security is at risk due to multiple known weaknesses in SSL 3.0.
- This includes the POODLE attack, which could allow decryption of sensitive data, such as session cookies.

- It should be noted that an attacker with MITM capabilities may be able to force clients to use SSL 3.0.

REMEDIATION

- Remove support for SSLv3.
- Mozilla has recommended settings for Apache, Nginx, Haproxy and others. These settings include explicitly supporting TLS (while excluding SSLv2, SSLv3). See guide below.

It is likely that the HTTPS server must be restarted for any configuration change to take effect.

B.1.2 *Bash "ShellShock" Injection*

AT A GLANCE

Classification	Information
Resource	/cron.php/()%20%20:%3B%3B%20/bin/sleep%2031
Method	GET
Detection Type	Blind Timing Analysis Checks
Risk	**HIGH**

Table B.2: Bash "ShellShock" Injection

REQUEST

```
GET /cron.php/()%20{%20:%3B}%3B%20/bin/sleep%2031
```

RESOURCE CONTENT

```
{"status":"success"}
```

DISCUSSION

The issue Vega identified is due to a vulnerability in the Bash shell. This vulnerability may manifest itself remotely in web applications if user-supplied input is passed to the Bash shell environment, which can occur if header or parameter values are converted to local environment variables. If successfully exploited, this vulnerability may lead to command execution on the underlying host.

IMPACT

- Vega has detected a possible command injection vulnerability.
- Attackers may be able to run commands on the server.
- Exploitation may lead to unauthorized remote access.

REMEDIATION

- The bash shell should be upgraded on the affected host. This can often be done through the package management system, such as apt or yum.
- Developers should examine the code corresponding to the page in detail to determine if the vulnerability exists.
- Execution of system commands through a command interpreter, such as with system(), should be avoided.

If absolutely necessary, the developer should take extra care with validating the input before it is passed to the interpreter.

B.2 Medium vulnerabilities

B.2.1 *Local Filesystem Paths Found*

AT A GLANCE

Classification	Information
Resource	/apps/files_sharing/lib/connector/
Risk	**MEDIUM**

Table B.3: Local Filesystem Paths Found

REQUEST

```
GET /apps/files_sharing/lib/connector/
```

RESOURCE CONTENT

```
/lib/connector
```

DISCUSSION

Vega has detected a possible absolute filesystem path (i.e. one that is not relative to the web root). This information is sensitive, as it may reveal things about the server environment to an attacker. Knowing filesystem layout can increase the chances of success for blind attacks. Full system paths are very often found in error output. This output should never be sent to clients on production systems. It should be redirected to another output channel (such as an error log) for analysis by developers and system administrators.

IMPACT

- Vega has detected what may be absolute filesystem paths in scanned content.
- Disclosure of these paths reveals information about the filesystem layout.
- This information can be sensitive, its disclosure can increase the chances of success for other attacks.

REMEDIATION

- Absolute paths are often found in error output.
- Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers.

This output should be sent to another output stream, such as an error log.

B.2.2 *Client Ciphersuite Preference*

AT A GLANCE

Classification	Configuration
Risk	**MEDIUM**

Table B.4: Client Ciphersuite Preference

DISCUSSION

The server can override client ciphersuite prioritization during the TLS handshake. This is useful for enforcing better, more secure ciphersuites for all visiting clients. Vega has detected that this is not configured in the server, potentially leaving older clients at risk.

IMPACT

- User browsers may select less secure cipher suites creating opportunities for attack.

REMEDIATION

- HTTPS server should be configured to enforce server ciphersuite preferences. How this is configured will vary by server.

Mozilla has included guidelines for configuring server ciphersuite preference for various implementations. See link below.

B.2.3 *Possible Source Code Disclosure*

AT A GLANCE

Classification	Configuration
Resource	/core/vendor/underscore/underscore.js
Risk	**MEDIUM**

Table B.5: Possible Source Code Disclosure

REQUEST

```
GET /core/vendor/underscore/underscore.js?v=9787365d9e62f8305a0d1b747ae1fb6d
```

RESOURCE CONTENT

```
Possible ASP or JSP code:
<%([\s\S]+?)%>
```

DISCUSSION

Vega has detected fragments of text that match signatures of application source code. Application source code unintentedly visible to remote clients can be a security vulnerability. This can occur in applications using technologies such as PHP and JSP, which allow for code to be mixed with static presentation content. For example, in-line code is sometimes commented using HTML comments, resulting in it being transmitted to remote clients. For an attacker, source code can reveal information about the nature of the application, such as its design or the use of third-party components. Sometimes sensitive information, such as a database connection string, can be included in source code.

IMPACT

- Could result in disclosure of sensitive information to attackers.
- Source code fragments can include information about the design/structure of the application, including use of third-party components.
- This information may not otherwise be easily known by an adversary.
- Sometimes source code also contains highly sensitive information, such as passwords (database connection strings).

REMEDIATION

- The developer should verify that the output detected by Vega is in fact application source code.

The cause should be determined, and the material removed or prevented from being output.

Appendix C

Planning

This chapter will show the planning of the tasks needed to drive the analysis, execution of experiments and final thesis exposition.

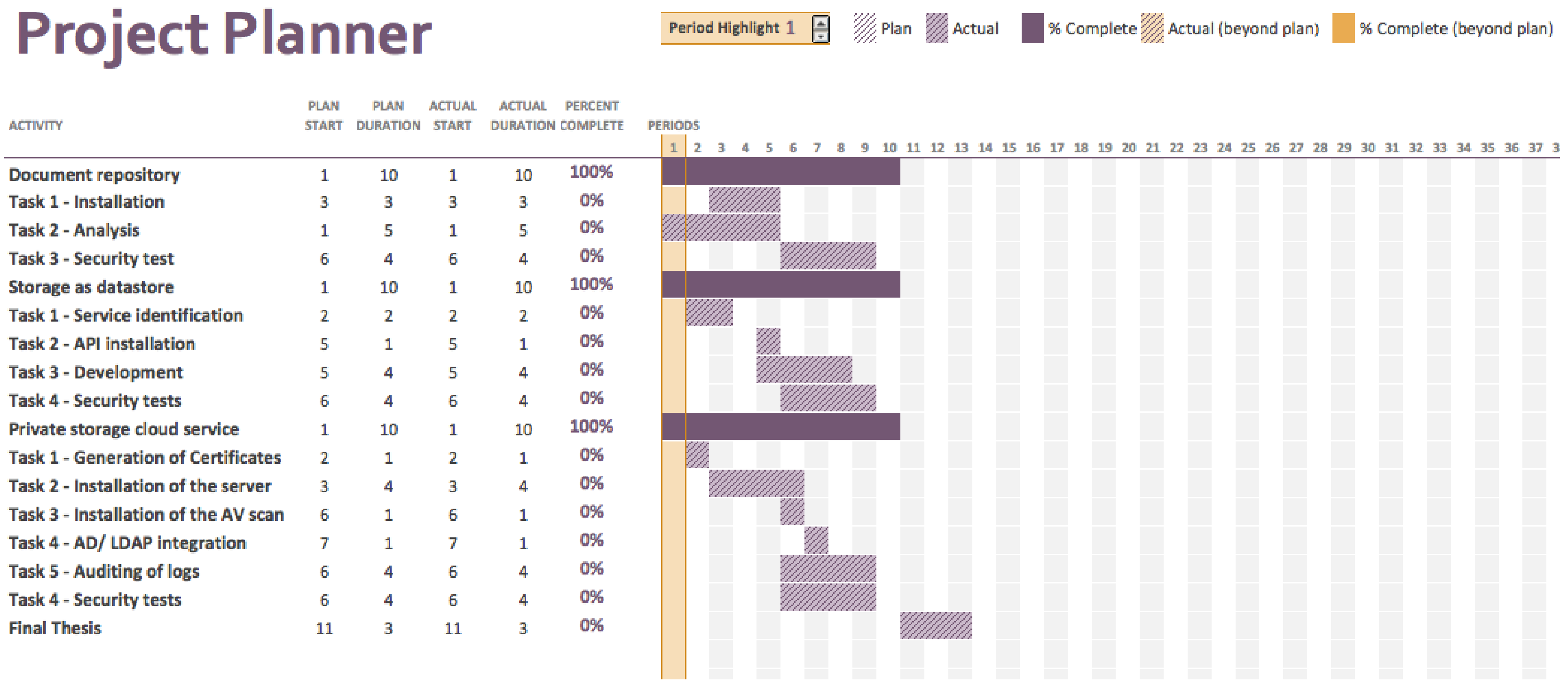
The project execution will have a duration of 13 weeks counting from the 9th of March and finishing on the 8th of June with the final presentation of the final master's thesis presentation. To dive a correct execution of the thesis in this period we will have the following 4 milestones:

Date	Milestone
09/04/2015	Analysis
11/05/2015	Development ant testing
08/06/2015	Final dissertation for the TFM
15/06/2015	Presentation of TFM

Table C.1: TFM Milestones

In the gantt diagram C.1 we can see the duration, begin and finish date for each of the tasks described in the use cases. the time metric used on the gantt diagram is a week. However, for the day to day analysis and development tasks an agile methodology will be implemented helping with the tracking of the small task, the tool selected to track this tasks is Trello[1].

[1] https://trello.com



Project Planner

ACTIVITY	PLAN START	PLAN DURATION	ACTUAL START	ACTUAL DURATION	PERCENT COMPLETE
Document repository	1	10	1	10	100%
Task 1 - Installation	3	3	3	3	0%
Task 2 - Analysis	1	5	1	5	0%
Task 3 - Security test	6	4	6	4	0%
Storage as datastore	1	10	1	10	100%
Task 1 - Service identification	2	2	2	2	0%
Task 2 - API installation	5	1	5	1	0%
Task 3 - Development	5	4	5	4	0%
Task 4 - Security tests	6	4	6	4	0%
Private storage cloud service	1	10	1	10	100%
Task 1 - Generation of Certificates	2	1	2	1	0%
Task 2 - Installation of the server	3	4	3	4	0%
Task 3 - Installation of the AV scan	6	1	6	1	0%
Task 4 - AD/ LDAP integration	7	1	7	1	0%
Task 5 - Auditing of logs	6	4	6	4	0%
Task 4 - Security tests	6	4	6	4	0%
Final Thesis	11	3	11	3	0%

Figure C.1: Gantt chart

Appendix D

Acronym

ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Program Interface
CA	Certification Authority
COPPA	Children's Online Privacy Protection
CSA	Cloud Security Alliance
DC	Data Center
EU	European Union
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
JAAS	Java Authentication and Authorization Service
LDAP	Lightweight Directory Access Protocol
MPAA	Motion Picture Association of America
MS	Microsoft
OS	Operating System
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PEM	Privacy Enhanced Mail
SAML	Security Assertion Markup Language
SOC	Service Organization Controls
SQL	Structured Query Language
SSAE	Statement on Standards for Attestation Engagements
SSL	Secure Sockets Layer
SSO	Single Sign On
TLS	Transport Layer Security
US	United States
VM	Virtual Machine

Table D.1: Acronym

References

[1] ISO 27001. Iso 27001. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[2] ActiveMQ. Activemq, 2015. http://activemq.apache.org/.

[3] Amazon. Amazon cloud drive api, 2015. https://developer.amazon.com/public/apis/experience/cloud-drive/content/getting-started#authorization.

[4] Amazon. Amazon cloud drive terms of use, 2015. http://www.amazon.com/gp/help/customer/display.html/?nodeId=201376540.

[5] Amazon. Amazon s3 api, 2015. http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingAWSSDK.html.

[6] Amazon. Aws compliance, 2015. https://aws.amazon.com/compliance/?nc1=f_ls.

[7] Amazon. Aws s3, 2015. http://aws.amazon.com/s3/?nc1=f_ls.

[8] Amazon. Clouddrive, 2015. https://www.amazon.com/clouddrive/home.

[9] Apple. About icloud security code alert messages, 2015. https://support.apple.com/en-us/HT202755.

[10] Apple. Cloudkit web services reference, 2015. https://developer.apple.com/library/prerelease/ios/documentation/DataManagement/Conceptual/CloutKitWebServicesReference/Introduction/Introduction.html.

[11] Apple. icloud, 2015. https://www.icloud.com.

[12] Apple. icloud security and privacy overview, 2015. https://support.apple.com/en-us/HT202303.

[13] Apple. icloud terms and conditions, 2015. https://www.apple.com/legal/internet-services/icloud/en/terms.html.

[14] Symplified Technology Assets. Symplified sso, 2015. http://www.emc.com/security/rsa-identity-and-access-management/rsa-myaccesslive-sso.htm.

[15] Matthew Berryr. Single sign-on: Integrating aws,openldap, and shibboleth. Technical report, Amazon, 2015. http://d0.awsstatic.com/whitepapers/aws-whitepaper-single-sign-on-integrating-aws-open-ldap-and-shibboleth.pdf.

[16] Box. Box: redefiniendo la seguridad para la nube. Technical report, Box. https://cloud.app.box.com/s/ajzwsycwbgptfw8a05d9hvagy08q55h8.

[17] Box. Building a trust ecosystem:solutions and controls for content protection. Technical report, Box. https://cloud.app.box.com/Trust-Ecosystem.

[18] Box. Admin console: 2-step login verification, 2014. https://support.box.com/hc/en-us/articles/200520628-Admin-Console-2-Step-Login-Verification.

[19] Box. Box terms of service, 2014. https://www.box.com/legal/termsofservice/.

[20] Box. The future of security. Technical report, Box, 2014. https://cloud.app.box.com/Future-of-security.

[21] Box. Increase the security of your box account with single sign-on. Technical report, Box, 2014. http://www.comtact.co.uk/wp-content/uploads/2013/09/Box-Single-Sign-On-Comtact-Ltd.pdf.

[22] Box. What security settings can i enforce for my users?, 2014. https://support.box.com/hc/en-us/articles/200520738-What-security-settings-can-I-enforce-for-my-users-.

[23] Box. Box.om, 2015. https://app.box.com.

[24] Box. Can i restrict which applications my users integrate with box?, 2015. https://support.box.com/hc/en-us/articles/200526698-Can-I-restrict-which-applications-my-users-integrate-with-Box-.

[25] Box. What are the different access levels for collaborators?, 2015. https://support.box.com/hc/en-us/articles/200520918.

[26] D. Catteddu and G. Hogben. Cloud Computing: Benefits, Risks and Recommendations for information security, Technical Report. *European Network and Information Security Agency (ENISA)*, 2009.

[27] Citrix. Citrix password management, 2015. http://support.citrix.com/proddocs/topic/passwordmanager-5-0/pm-landing-page-version-50.html.

[28] ClamAV. Clamav, 2015. http://www.clamav.net/index.html.

[29] Federal Trade Comission. Coppa. https://www.ftc.gov/consumer-protection/childrens-privacy.

[30] Cumulus. Cumulus, 2015. http://www.cumulus-project.eu/.

[31] T. Dierks. The transport layer security (tls) protocol version 1.2, 2008. https://tools.ietf.org/html/rfc5246.

[32] Dropbox. Complying with standards and regulations, 2015. https://www.dropbox.com/business/trust/compliance/certifications-compliance.

[33] Dropbox. Does dropbox keep backups of my files?, 2015. https://www.dropbox.com/help/122.

[34] Dropbox. Dropbox, 2015. https://www.dropbox.com/home.

[35] Dropbox. Dropbox for business agreement, 2015. https://www.dropbox.com/privacy#business_agreement.

[36] Dropbox. How do i enable two-step verification on my account?, 2015. https://www.dropbox.com/help/363.

[37] Dropbox? How do i link to a file or folder?, 2015. https://www.dropbox.com/help/167.

[38] Dropbox. How do i set up single sign-on (sso) for my business account?, 2015. https://www.dropbox.com/help/1909.

[39] Dropbox. How do i share folders with other people?, 2015. https://www.dropbox.com/help/19.

[40] Dropbox. How secure is dropbox, 2015. https://www.dropbox.com/help/27.

[41] Dropbox. Star self-assessment, 2015. https://cloudsecurityalliance.org/star-registrant/dropbox-inc/#self.

[42] PCI DSS. Pci dss. https://www.pcisecuritystandards.org/security_standards/.

[43] Ernst and Young LLP. Service organization controls 3 (soc 3) report, 2014. https://cert.webtrust.org/pdfs/soc3_dropbox.pdf.

[44] Stamatelopoulos F. and Lenis A. Deliverable D3.3.2: Cloud Computing Toolbox for SMEs. *CloudingSMEs*, 2015.

[45] Apache Fundation. Apache http server, 2015. http://httpd.apache.org.

[46] Google. Changes to our ssl certificates, 2013. http://googleonlinesecurity.blogspot.com.es/2013/05/changes-to-our-ssl-certificates.html.

[47] Google. Google terms of service, 2014. https://www.google.com/intl/en/policies/terms/.

[48] Google. About google apps directory sync, 2015. https://support.google.com/a/answer/106368?hl=en.

[49] Google. Add 2-step verification, 2015. https://support.google.com/a/answer/175197?hl=en&ref_topic=2759193&rd=1.

[50] Google. Google drive, 2015. https://drive.google.com.

[51] Google. Google drive sdk, 2015. https://developers.google.com/drive/web/about-sdk.

[52] Google. How to share, 2015. https://support.google.com/drive/answer/2494822.

[53] Google. Security, 2015. https://support.google.com/work/answer/6056693?hl=en.

[54] Google. Your security and privacy, 2015. https://support.google.com/a/answer/60762.

[55] Intel. Intel expressway cloud access 360, 2015. https://software.intel.com/en-us/articles/intel-application-security-and-identity-products-cloud-access-360.

[56] ISAE. Isae 3402. http://www.isae3402.com/.

[57] Jeffery K., Neidecker-Lutz B., Schubert L., and Tsakali M. Cloud Computing: The Next Big Thing? *ERCIM News*, (83), 2010.

[58] Scarfone K., Souppaya M., Cody A., and Orebaugh A. Information Security Testing and Assessment, Special Publication. *National Institute of Standards and Technology*, 2008.

[59] I.M. Khalil, A. Khreishah, and M. Azeem. Cloud Computing Security: A Survey. *Computers*, 3(1):1–35, 2014.

[60] Microsoft. Share files and folders and change permissions. http://windows.microsoft.com/en-us/onedrive/share-file-folder.

[61] Microsoft. Active directory architecture, 2000. https://technet.microsoft.com/en-us/library/bb727030.aspx.

[62] Microsoft. Microsoft services agreement, 2014. http://windows.microsoft.com/en-us/windows/microsoft-services-agreement.

[63] Microsoft. Onedrive api, 2014. https://dev.onedrive.com/index.htm.

[64] Microsoft. Onedrive appregistration, 2014. https://dev.onedrive.com/app-registration.htm.

[65] Microsoft. Data encryption in onedrive for business and sharepoint online, 2015. https://technet.microsoft.com/en-us/library/dn905447.aspx.

[66] Microsoft. Office 365 compliance, 2015. https://technet.microsoft.com/en-us/library/office-365-compliance.aspx.

[67] NIST. Fips. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=902003.

[68] NIST. Fisma. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

[69] OASIS. Saml, 2012. https://wiki.oasis-open.org/security/FrontPage.

[70] U.S. Department of Education. Ferpa. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[71] U.S. Department of Health and Human Services. Hipaa security rule. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

[72] U.S. Department of Health and Human Services. Hitech act enforcement interim final rule. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf.

[73] Okta. Okta sso, 2015. https://www.okta.com/product/identity-management/#sso.

[74] OneLogin. Secure single sign-on solution, 2015. https://www.onelogin.com/product/sso.

[75] OpenTSDB. Opentsdb, 2015. http://opentsdb.net/.

[76] Oracle. Java authentication and authorization service, 2014. http://docs.oracle.com/javase/7/docs/technotes/guides/security/jaas/JAASRefGuide.html.

[77] OwnCloud. Optimizing owncloud security, 2014. https://owncloud.com/wp-content/uploads/2014/10/WP-Optimizing-ownCloud-Security-1.3.pdf.

[78] OwnCloud. Owncloud, 2014. https://owncloud.org/.

[79] OwnCloud. owncloud?s data encryption model, 2014. https://owncloud.com/wp-content/uploads/2014/10/Overview_of_ownCloud_Encryption_Model_1.1.pdf.

[80] OwnCloud. Ssl / encryption app, 2014. https://doc.owncloud.org/server/8.0/admin_manual/configuration_server/performance_tuning.html#ssl-encryption-app.

[81] OwnCloud. Commercial license, 2015. https://owncloud.com/licenses/owncloud-commercial/.

[82] OwnCloud. Owncloud api, 2015. http://api.owncloud.org.

[83] Ping. Ping identity, 2015. https://www.pingidentity.com.

[84] rbvmomi. rbvmomi, 2015. https://github.com/rlane/rbvmomi.

[85] ActiveMQ Security. Activemq security, 2015. http://activemq.apache.org/security.html.

[86] Global Sign. Certification authority, 2015. https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/.

[87] SOC. Soc. http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx.

[88] SSAE16. Ssae16. http://ssae16.com/.

[89] Subgraph. Vega vulnerability scanner, 2014. https://subgraph.com/vega/.

[90] Symantec. Symantec o3, 2015. http://www.symantec.com/page.jsp?id=O3.

[91] VMware. Vmware horizon application manager, 2012. https://www.vmware.com/support/pubs/horizon_pubs.html.

[92] M. Wahl, T. Howes, and S. Kille. Lightweight directory access protocol (v3), 1997. http://www.faqs.org/rfcs/rfc2251.html.

[93] Wireshark. Wireshark, 2014. https://www.wireshark.org/.