

# System Description and Risk Analysis

Mustapha Malik Bekkouche      Oscar Felipe Toro  
Steffen Mogensen      Yumer Adem Yumer

April 18, 2016

## Contents

<b>1</b>	<b>System Characterization</b>	<b>2</b>
1.1	System Overview . . . . .	2
1.2	System Functionality . . . . .	2
1.3	Components and Subsystems . . . . .	2
1.4	Interfaces . . . . .	3
<b>2</b>	<b>Risk Analysis and Security Measures</b>	<b>3</b>
2.1	Assets . . . . .	3
2.1.1	<i>Physical assets</i> . . . . .	3
2.1.2	<i>Logical assets</i> . . . . .	3
2.2	Threat Sources . . . . .	4
2.3	Risks and Countermeasures . . . . .	5
2.3.1	<i>Evaluation Asset Firewall</i> . . . . .	5
2.3.2	<i>Evaluation Asset Website</i> . . . . .	6
2.3.3	<i>Evaluation Asset Database</i> . . . . .	6
2.3.4	<i>Evaluation Asset Images</i> . . . . .	7
2.3.5	<i>Evaluation Asset Username and Password</i> . . . . .	7
2.3.6	<i>Evaluation Asset Customer confidence</i> . . . . .	7
2.3.7	Risk Acceptance . . . . .	8

# 1 System Characterization

## 1.1 System Overview

The mission for the server is to host a web application, where users can upload their images, and share them with each other. The users have the power to choose who they wish to share their images with, and also if they would like to unshare an image with another user. When a user uploads an image, we own that image, therefore, the user cannot delete or remove the image from the web application.

The server is a Unix-based system, build on Ubuntu 14.04. It has a bare minimum of users on the server since there should only be one for maintaining the services running on the system.

This web application is set to start-up as soon as the server is booted. This is expected to be the best case, since the main purpose of the service, is to host this application. So in case of failure where the system reboots (E.g. power out, or alike), it will be available again as soon as possible, without having personal to start up the application manually.

The server is also set-up so that it can be accessed remotely. This is for maintenance reasons, and will require the proper use of login and password for gaining access. For sending files to and from the server, this should happen within the encrypted connection services running on the server, and not by additional software.

## 1.2 System Functionality

As originally stated in the project description, the system implements the main requirements, namely:

1. the system should allow the user to upload pictures
2. the user can share his own pictures with other named users on a picture-by-picture basis
3. the user can view his own pictures and pictures other has shared with him
4. the user can comment on any picture he can view
5. and the user can view comments on any picture he can view

## 1.3 Components and Subsystems

We recognize mainly two elements of the system, the web application and the database. Both sitting on top of the Ubuntu Server. In order to connect to the server we are using the OpenSSH suite.

- Platform: the virtual machine is running Ubuntu Server 14.04.01 which is the Long Term Support version of the server.
- Web Application: The web application is build in Python 2.7, together with the micro-framework Flask. Hence, the web server is SimpleHTTPServer, that is a part of the python standard library. The framework offer inbuilt security features, such as sanitisation of fields and it only offers the minimum building blocks which http server, micro framework, only the minimum
- Database: SQLite3 is used as storage of users for the web application, and all the content that is in addition with it. This means that there is no daemon running, since everything is stored in the same file. To access and manipulation of the database, it is needed to have access to this file. This means that for altering,
- SSH: Open-SSH is installed on the system, this is so it is possible for a system administrator to connect to the system and do any configuration that is necessary, without having to be in front of the machine. This also means that scp is available for uploading and downloading files to the server.

## 1.4 Interfaces

Specify all interfaces and information flows, from the technical as well as from the organizational point of view.

# 2 Risk Analysis and Security Measures

## 2.1 Assets

### 2.1.1 *Physical assets*

Server - The web server is located on a virtual machine and is up to date. The administrator is responsible of installing all the patches guarantying the proper function of the server. Physical access to it may allow an adversary to gain control of the system. A server can, for example, be booted with a different operating system.

### 2.1.2 *Logical assets*

It includes the operating system, the website, the database, the information related to the users and customer confidence.

*Firewall* - The IP table (firewall) of the server is properly configured and restricts access to the server. It keeps track of each connection passing through it and filters all the attempts to connect to the server except through allowed ports. The firewall is kept up-to-date and the administrator installs all security-relevant updates.

*Website* - The website provides the following functionality - uploading images, sharing them with others user, and posting comments. Only a user authorised for a picture can view, comment or read comments on that picture. No unauthorised user can prevent an image or a comment from being shown to authorised users. The website runs on the web-server which is kept up-to-date. The web developer is responsible for updating the functionality of the website.

*Database* - it keeps all the information related to the users, using the website. The username, passwords, pictures are stored in the database. It runs on the server and the access to it is restricted. The administrator is responsible for its maintenance.

*Information* - all the informations related the users are valuable and proper measures are taken to guarantee their confidentiality. The informations include especially the username, password, pictures uploaded by users.

*Pictures* - all the uploaded images are kept on the server and are visible to the owner and other users allowed by the owner. There is no restrictions on the size of the images.

*Username and passwords* - They identify the owner of the pictures. All password are saved, using the proper hash functions guarantying the security.

*Customer confidence* - since the user can upload private pictures, which should be hidden for the world, user confidence is important for a successful business relationship.

## 2.2 Threat Sources

- *Employees* : the employees in our tiny company consist of a system administrator who has access to the server and a web developer, they could possibly leak sensitive information (intentionally or unintentionally) or weaken the system security,
- *Hackers* : since the system is connected to internet, it is exposed to various attacks, the attackers vary from highly motivated people with good skills actively trying to penetrate the system to script kiddies just messing around.
- *Malware* : as any it system, malware could possibly be a problem, it could be directed malware (unlikely) or undirected malware (more likely).

## 2.3 Risks and Countermeasures

Impact	
Impact	Description
High	Complete shutdown of the system, user data is compromised, a major loss in asset value, complete loss of the customers confidence
Medium	System slow down, loss in asset value
Low	Relatively affect the credibility of the company, lower the customers confidence and a relative loss in asset value

Likelihood	
Likelihood	Description
High	The threat source has the power to exploit vulnerabilities in the system, the countermeasures are inexistant or ineffective.
Medium	The threat source is motivated, some countermeasures are implemented which may prevent him to do harm
Low	The countermeasures are completely effective, (almost) nothing to worry about

Risk Level			
Likelihood	Impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

### 2.3.1 Evaluation Asset Firewall

Table 1: Evaluation Asset Firewall

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Malware: Virus/worm spreads over the Internet possibly affects system files and change firewall settings	Proper maintenance of the server, security patches installed, restricted user rights	Low	Medium	Low

### 2.3.2 *Evaluation Asset Website*

Table 2: Evaluation Asset Website

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Skilled hacker gains control over the website, steals confidential data, modifies website settings because of vulnerability either in the server or on the website	The server is hardened and regularly updated. System administrator is trained to notice irregularities on the server.	Low	Medium	Low
2	Script kiddies makes modifications on the website as a result of an attack	The server is properly maintained, the website is hardened, all input is sanitized	Low	Medium	Low

### 2.3.3 *Evaluation Asset Database*

Table 3: Evaluation Asset Database

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Skilled hacker gains control, over the database, steals confidential data, make changes on the database like deleting tables, editing records	Hardened server and kept up-to-date, use of hashed and salted passwords	Low	High	Low

#### 2.3.4 *Evaluation Asset Images*

Table 4: Evaluation Asset Images

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Web developer unintentionally breaks confidentiality during the update of the website	Well trained web developer	Low	High	Low

#### 2.3.5 *Evaluation Asset Username and Password*

Table 5: Evaluation Asset Username and Password

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Script kiddies try to guess the username and the password	Advising users not to choose simple usernames and passwords	Medium	Medium	Medium
2	Skilled hacker attacks with special software to break passwords	Encryption passwords with strong hash functions choosing arbitrary salts	Medium	High	Medium

#### 2.3.6 *Evaluation Asset Customer confidence*

Table 6: Evaluation Asset Customer confidence

No.	Threat	Implemented/planned countermeasure(s)	L	I	R
1	Theft of confidential data	State-of-the-art security measures, hashing and salting all passwords not keeping any sensitive data	Low	High	Low

### 2.3.7 Risk Acceptance

No. of threat	Proposed countermeasure
2.3.5	Allowing users only 3 login attempts
2.3.5	using one time password sent by sms
2.3.5	forcing users to create long passwords (including capital letters, numbers and special characters)