FYP Plan

Supervisor: Dr. Chin. T. W.
Student: Xie Fan (3035021546)
Yang Dong(3035023075)

Anonymous Public-accumulated Crime Investigation System

Project Background:

There is no society in any part of the world, which is without crimes. In America, Just about everyone has been exposed to some form of crime in their lifetimes, if not performing crimes themselves. In Hong Kong, 39805 crimes occurred from Jan. to Jul. 2014, including 6397 violent crimes. Yet only approximately 40 percent of them can be uncovered-- still a relatively high detection rate around the world. Each crime investigation requires sufficient evidence and information. Net users, which make up 72% of HK population, have became a solid source of evidence and information to facilitate crime investigation. However, most net users would rather provide information without revealing their own identities.

According to the current crime reporting system of Hong Kong, the way to report a crime diverse with cases. For emergency, always dial 999; for non-emergency crimes, call 101 or local police; for anonymous reporting, call HK Crimestoppers at 0800 555 111, or send online form to HK Crimestoppers. However, an anonymous crime form could be too vague to match a certain cases. Net users need a more reliable and comfortable panel to provide information anonymously.

Project Objective:

Our project aims at implementing an anonymous System collecting useful evidence
and information from the public to facilitate crime investigation.

1. Information Gathering

The system is expected to have two reporting approach for information gathering: Provide Information for a “Wanted Case”, or report “New Crime”.

Provide Information for a “Wanted Case”: Police will use this approach to give crime cases that are in need of more information. Police will display some known information of a crime case under investigation, then the public can access the information and provide further information to help with the investigation.

“New Crime”: When public witnessed a new crime scene that is not found in existing given list, he or she may fill and submit a uniform crime report and add a new crime case. If police is interested in this information, the police will contact to the provider in this system.

2. Information processing: The system will try to take some basic processing on information gathered. Information that likely belongs to a same crime case in the “New Crime” approach will be added to a “May be relevant pack”. This pack will be presented when police exam a case in “New Crime”.

3. Authenticity check: This system is implanted in order to prevent malicious fake information and crime reporting. According to police feedback, every time user report fake information, the system will counts a credit deduction. As constant deduction indicates the user has been giving fake information maliciously, he/she will get banned and following actions will be taken.

4. Confidentiality: The system does not hold any personal information except IP address. Then as long as a user would not violate the law (like maliciously give fake information talked above), the IP address of users will be encrypted and garanteed to be kept safe and secretly. For the information given by a user, it would only be seen by himself or herself, the system manager and the police.
Project Methodology:

1. Thread like information gathering system.
The information gathering system is build like a forum. The two reporting approach are two blocks of a forum. Report to a “Wanted Case” is like replying to a thread, and Report to a “New Case” is like starting a new thread. As a user cannot see “posts and thread” from other normal users, from user’s view, the system is like a two people “forum”, only the police and himself or herself. From police’s view, the system is just like a normal forum.

2. Information processing.
For “New Crime” approach, crime report form during information reporting contains elements like crime time, location, crime category. Some algorithms will be implemented to try grouping report provided by different users based on these elements. For example, two reports A and B have about same crime time, location and category, then A and B are likely describing the same crime scene. Then when police is looking report A, report B is presented in “May be relevant pack” as a suggestion. Also based on these elements, a search system should also be implemented.

3. Defining the user groups.
User group are introduced to support authenticity check.
Considering the importance of time saving, the system allows non-registered visitors to give information for “Wanted Case”.
Then only registered users are able to raise “New Crime” report, for user credit are being considered.
Above two kinds of users can only access police given information and their own reported information
System manager accounts and police force accounts have access to all information. The difference between is police force accounts cannot access user IP address even if IP is already encrypted.

4. Credit and authenticity check system.
Every registered is associated to a credit value. Initially, the value should be 0. According to police feedback, authentic and useful information will increase the users’ credits. As most public are untrained people, the memory of a crime scene will not be very clear, so false information is considerably acceptable. Because of this assumption, false information will cause deduction to users’ credits, but after a time (specific length yet to be discussed), minus credits point will recover to 0. The special case is someone is found to report false information constantly in quite short time. We consider this kind of act to be giving fake information maliciously, so we would report this condition to police and wait feedback to take further actions.

5. Confidentiality Guarantees.
For both registered users and visitor, their IP address will be encrypted and kept safely and secretly. Unless special cases involved, like a user violated law, the IP address will now be shown to any other party.
Also during registering and all other actions, no personal information like phone number, e-mail address is required.

## Tentative Schedule and Milestone

<table>
<thead>
<tr>
<th>Date</th>
<th>Milestone</th>
<th>Milestone Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>28/09/2014</td>
<td>Project plan &amp; web page</td>
<td>Project plan and web page are complete</td>
</tr>
<tr>
<td>15/10/2014</td>
<td>Design &amp; layout review</td>
<td>System design is complete, correct, approved and suitable to design</td>
</tr>
<tr>
<td>15/11/2014</td>
<td>UI complete</td>
<td>User interface of browser version has been built an it runs (not necessarily without errors)</td>
</tr>
<tr>
<td>Date</td>
<td>Task Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>04/01/2015</td>
<td>Background server complete</td>
<td>Background server has been built and it runs (not necessarily without errors)</td>
</tr>
<tr>
<td>11/01/2015</td>
<td>Test case &amp; Debug 1st step complete</td>
<td>Program successfully run and debugged</td>
</tr>
<tr>
<td>31/03/2015</td>
<td>Encryption complement</td>
<td>IP address successfully encrypted</td>
</tr>
<tr>
<td>07/04/2015</td>
<td>Test case &amp; Debug 2nd step complete</td>
<td>Encryption successfully work on browser.</td>
</tr>
<tr>
<td>optional</td>
<td>Mobile platform client complete</td>
<td>Develop another version for mobile (Android) platform if time is allowed</td>
</tr>
</tbody>
</table>