AN ANDROID APP FOR THE SAFETY OF WOMEN

[1] Ashish Sharma

[1]Assistant Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2] Pooja Tyagi, [3]Vasundhara Gupta

[23]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

Abstract:

In today's world, people using smart phones have increased rapidly and hence, a smart phone can be used efficiently for personal security or various other protection purposes. The heinous incident that outraged the entire nation has wakened us to go for the safety issues and so a host of new apps have been developed to provide security systems to women via their phones. This project presents Abhaya, an Android Application for the Safety of Women and this app can be activated this app by a single click, whenever need arises. A single click on this app identifies the location of place through GPS and sends a message comprising this location URL to the registered contacts and also call on the first registered contact to help the one in dangerous situations. The unique feature of this application is to send the message to the registered contacts continuously for every five minutes until the "stop" button in the application is clicked. Continuous location tracking information via SMS helps to find the location of the victim quickly and can be rescued safely.

Keywords: Android; GPS; URL; Registered Contacts

WORKSTATION MONITORING USING BOTNET

[1] Anupam Kumar

[1]Assistant Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2] Varidhi Garg, [3]Deepansh Sachdeva, [4]Akshay Rohtagi

[234]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

Abstract:

Botnet1, 2 acts as a base for many illicit works, according to cyber community. Botnet has been categorized into centralized, decentralized and hybrid structures. In Centralized Structure 3, one or group of compromised client machine will be remotely controlled by single server: Examples of Centralized Structure are IRC-based and HTTP-based. IRC-based Botnet is the oldest method followed by hacker. Main feature is it acts as communication protocols to reroute with compromised networks. Many defensive techniques have been proposed. Behalf of this, these communication protocols has been isolated from normal traffic. But IRC [Internet-Relay-Chat] based Botnet is still exists. Later, Hacker developed HTTP based Botnet to achieve the destination by disrupting defensive techniques which was built against them. The main feature of HTTP-based Botnet is to hide from the users using the concept of dynamic domain name service, as a resolution to update and frequently changes the server location. In Decentralized Structure 4, each Bot [compromised machine] acts as client and server. There is no centralized point of failure in such approaches. Examples of Decentralized Structure are P2P-based and fast-flux-based. These two approaches use the concept of fully qualified dynamic domain name service [FQDDNS] for frequent updates of new Botnet in automate manner. Many detection approaches are still being developed recent years. But it finds very difficult in shutdown and disrupt the Botnet resilience. Hybrid structure involves the combination of both centralized and decentralized structure. Recently, these types of structures are used as deliberate to spread Botnet in distributed environment.

Keywords: Botnet, Honeypot, IDS, Malware Analysis, OpenDNS