Geo Fencing Security System

G.Abirami[1], U.Akileshwari[2], M.Deeba[3], Mr.M.Markco M.E.,(Ph.D)[4]
[1, 2, 3] Dept of CSE
[4]Assistant Professor, Dept of CSE
[1, 2, 3, 4] E.G.S.Pillay Engineering College, Nagapattinam

Abstract- *A geo fence is a virtual perimeter for a real world graphic area. The system is composed of client- server architecture the server collects risk information from various information sources and the client watches the user to notify the information as the need arises.To detect the user's movement, the client creates a virtual fence called geofence at the dangerous area based on the risk of information stored in the server, and monitors the user's entry and exit of the fence.A system can be implemented A system can be implemented for defense against unauthorized access on secrete files. It Provides an authentication based on three types, such as Media Access Control (MAC), Internet Protocol (IP) and Geo-Fence Area or boundaries. A Malicious users are copy the secret files around the system within the geo-fence boundary, At the same time our system is automatically trigger and it generate the harmful virus for scrap the copied file. The users are insert the secondary device (Pen drive) into the outside of the geo-fence area, the virus file first check the GPS location , MAC Address and IP address of the current system, if it is mismatch the virus file wipe out the secret files and it also wipe out the whole system of malicious user's. our system is also block the mail preview of the secret files.*

Keywords- Geo-Fencing Boundary Fixing, Attacker Module,Malware Injection, Wipe out System, Performance Evaluation.

I. INTRODUCTION

A **geo-fence** is a virtual perimeter for a real-world geographic area. A geo-fence could be dynamically generated as in a radius around a point location, or a geo-fence can be a predefined set of boundaries (such as school zones or neighborhood boundaries).The use of a geo-fence is called **geo-fencing**, and one example of usage involves a location-aware device of a location-based service (LBS) user entering or exiting a geo-fence. This activity could trigger an alert to the device's user as well as messaging to the geo-fence operator. This info, which could contain the location of the device, could be sent to a mobile telephone or an email account.Geofencing, used with child location services, can notify parents if a child leaves a designated area. Geofencing used with locationized firearms can restrict those firearms to fire only in locations where their firing is permitted, thereby making them unable to be used elsewhere.Geofencing is critical to telematics. It allows users of the system to draw zones around places of work, customer's sites and secure areas. These geo-fences when crossed by an equipped vehicle or person can trigger a warning to the user or operator via SMS or email. In some companies, geofencing is used by the human resource department to monitor employees working in special locations especially those doing field works. Using a geofencing tool, an employee is allowed to log his or her attendance using a GPS-enabled device when within a designated perimeter.Other applications include sending an alert if a vehicle is stolen and notifying rangers when wildlife stray into farmland. Geo-fence can be used for location based messaging for tourist safety and communication.

II. RELATED WORK

With rapid growth in technology and increase use of mobile devices, many enterprises have started to move away from fixed workstations to wireless mobile workstations. Moreover, some of the mobile applications may require access to sensitive data with the permissions being determined by the current location of a user. Typical access control systems are expensive and hard to maintain, especially systems that include location based access control. The complications arise from the purchase of additional equipment and time to integrate and secure a solution into the existing system. In such systems, one of the biggest problems is to figure out a cost effective and easy to implement solution to a problem of access permissions being determined by the current location of a user. In this paper we propose a simple scheme that uses near field communication technology along with Wi-Fi access point to securely validate the location of a user. Our scheme is efficient, secure and can be incorporated with other existing access control systems[1]. The service router then forwards the request to the target service provider. After processing the request, the provider sends a response back to the service router. Finally, the service router sends the response further to the mobile application. Geo-fencing applications provide mobile users with services, i.e. information or functionality, when the users are within certain geographical areas. Current development on geofencing applications allows different geo-fencing areas served by multiple service providers. This idea requires a *service router*to forward requests from users to target service providers by considering the users' current locations. In this paper, we present a location-based request forwarding mechanism and its implementation on a service router. The mechanism includes a caching mechanism to make efficient the forwarding process[2].Most UAS safety regulations involve setting off areas that are restricted for flight. Therefore, in order to create a UAS safety system, a virtual perimeter needs to be set up around real world geographic areas. This is also known as geo-fencing. Paired with the real-time geographic location of the UAS provided by a GPS, we can tell whether or not the aircraft is in a restricted airspace. Prebuilt maps, such as open street map, can provide information on certain points, stating what type of location it is. As a result, this safety system can be easily implemented with just a GPS and prebuilt map[3].UAV works under a complex environment and features a high flight freedom in low altitude flight, and path planning is a difficult point in guaranteeing economy and safety of flight. This paper abstracts the path planning of UAV into multi-objective optimization and puts forward a path representing method with a multi-gene structure. On this basis, the paper puts forward a path planning method based on self-adapted difference multi-objective optimization algorithm and achieves a comprehensive assessment of path flight. The simulation result indicates that the path planning algorithm can effectively create a 3D optimal path that meets constraint conditions and each performance index of UAV and fulfill the function of obstacles sensing and avoidance under a complex low altitude[4].Android requires third-party applications to request for permissions when they access critical mobile resources, such as users' personal information and system operations. In this paper, we present the attacks that can be launched without permissions. We first perform call graph analysis, component analysis and data-flow analysis on various parts of Android framework to retrieve unprotected APIs. Unprotected APIs provide a way of accessing resources without any permissions.We then exploit selected unprotected APIs and launch a number of attacks on Android phones. We discover that without requesting for any permissions, an attacker can access to device ID, phone service state, SIM card state, Wi-Fi and network information, as well as user setting information, such as airplane, location, NFC, USB and power modes of mobile devices. An attacker can also disturb Bluetooth discovery services, and block the incoming emails, calendar events, and Google documents. Moreover, an attacker can set volumes of devices and trigger alarm tones and ringtones that users personally set for their devices. An attacker can also launch camera, mail, music and phone applications even when the devices are locked. We compare our research on two Android versions, and discover that as platform providers incorporate more APIs, the number of unprotected APIs increases and new attacks become possible. We thus suggest platform providers to inspect Android frameworks systematically before releasing new versions[5].This paper discusses the various Geofencing constructs and concepts. Constructs are concepts, models, or schematic ideas: In our case they are the theoretical constructs of the Geofence used as a Security Strategy Model. Our concept considers Location Based Services and RFID as central to the security of wireless network security. Therefore Location Based Service and RFID Technology emerge as key constructs. Using the Geofencing application framework an organisation can turn from less secure when it uses a wireless network to highly secure. The Geofencing application framework was developed with the projection that applying the concepts of statistical process control to wireless network security will encourage wireless network usage as a secure method of communication by organizations prone to war driving and hacking. This paper is divided into two parts. The first part is experimental work, in which field measurement trials were conducted in order to observe and collect Positioning Technology data - taking into account the different noises in the Test Bed environment and the measurement scenarios. The second part of this paper presents the experiment setup, components and positioning methodology with a brief description of future work for researchers and industry practitioners[6]. In addition, to account for the characteristics of feature representations, we propose a hybrid hierarchical clustering algorithm which combines the merits of hierarchical clustering and k-medoids algorithms and a weightedsubspace K-medoids algorithm to generate base clusterings. The categorization results of our AMCS system can be used to generate signatures for malware families that are useful for malware detection. The case studies on large and real daily malware collection from Kingsoft Anti-Virus Lab demonstrate the effectiveness and efficiency of our AMCS system[7]. PC Leaks, a tool based on inter component communication (ICC) vulnerabilities to perform dataflow analysis on Android applications to find potential component leaks that could potentially be exploited by other components. To evaluate our approach, we run PCLeaks on 2000 apps randomly selected from the Google Play store. PCLeaks reports 986 potential component leaks in 185 apps. For each leak reported by PCLeaks, PCLeaksValidator automatically generates an Android app which tries to exploit the leak. By manually running a subset of the generated apps, we find that 75% of the reported leaks are exploitable leaks. In this paper is used to crash the malware application when the application leaks the data[8].Data sharing in cloud storage is receiving substantial attention in Information Communications Technology, since it can provide users with efficient and effective storage services. To protect the confidentiality of the shared sensitive data, the cryptographic techniques are usually applied. However, the data protection is still posing significant challenges in cloud storage for data sharing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To tackle this, we propose a new data protection mechanism for cloud storage,which holds the following properties. Furthermore, the security analysisand performance evaluation show that our proposal is secure and efficient, respectively[9].Challenges of authentication in decentralized mobile networks arise from frequently changing topologies and unreliable contention-based transmissions. We propose a new protocol to speed up authentications, reduce communication costs and support opportunistic routing under fast-changing topologies. The messages can be verified altogether, once a key is matched. The communication overhead thus becomes independent of the number of keys tried. Closed-form expressions for authentication rate, delay and throughput are derived through a new three-dimensional Markov model. Validated by simulations, analytical results corroborate the robustness of the proposed protocol against changing topologies, as well as the substantially improved resistance to collusion attacks, as compared to the state-of-the-art[10].

III. MODULES

3.1 Geo-Fencing Boundary

Fixing

Geo-fencing allow a administrator to set up triggers so when a device enters (or exits) the boundaries defined by the administrator, an alert is issued. Many geo-fencing applications incorporate Google Earth, allowing administrators to define boundaries on top of a satellite view of a specific geographical area.

3.2 Attacker Module

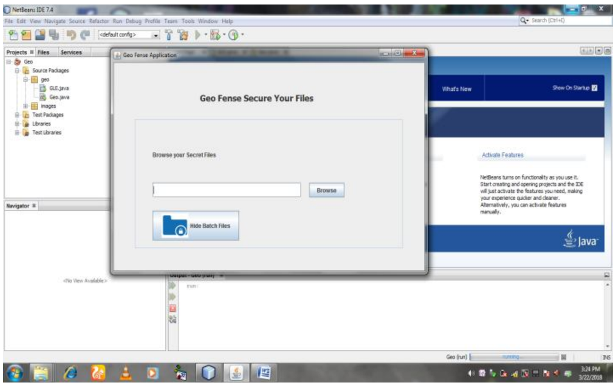
In Adversary module, the user can use the data on outside of the geo-fence area. It contains two types of attacker involves the system one is the attacker can be used an external device for copy the data in defense area, and another one is sending the data to the email. It is an one type of cyber attacks, because an attempt to hackers to damage or destroy whole computer networks or system.

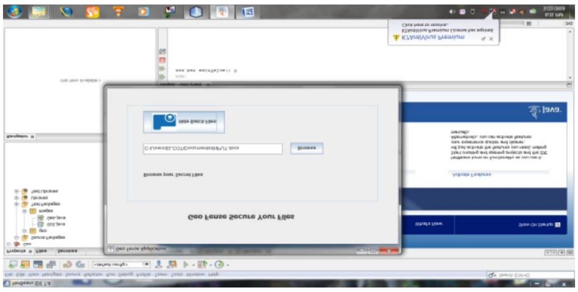
3.3 Victim File Injection whole

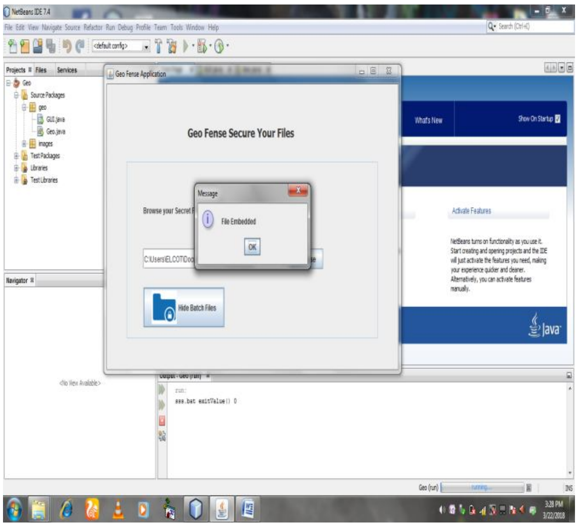
In this module is used to automatically inject the malware file to the original file. The victim file, is perform the main role of our system, it is an .exe file format..

3.4 Wipe out System

In the wipe out module, is wipeout the files and destroy the system when an exe find the system is adversary system. Auto exe is first check the adversary system having internet connection, if it is having a internet connection, victim file reading the current system MAC , IP and Geo Location and compare with the server it doesn't match to send the adversary system information to the mail and wipeout the files and system. otherwise it does not care of anything scrap the system and data.

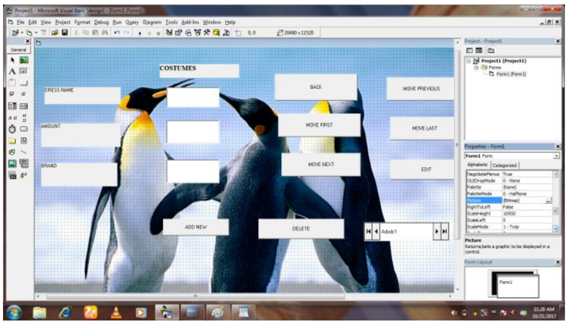






File Embedded

```
run:
sss.bat exitValue() 0
```



NegotiateMenus	True
OLEDropMode	0 - None
Palette	(None)
PaletteMode	0 - Halftone
Picture	(Bitmap)
RightToLeft	False
ScaleHeight	10950
ScaleLeft	0
ScaleMode	1 - Twip

Picture
Returns/sets a graphic to be displayed in a control.

IV. CONCLUSION

In this paper, we introduced a novel privacy-aware framework for provide data security, which enables the participation of workers without compromising their location privacy. We identified geo fencing as a needed step to ensure that privacy is protected prior to workers consenting to a task. We provided heuristics and optimizations for determining effective geo fencing regions that achieve high task assignment rate with low overhead. It also generate the victim files, it automatically checks the geo - fencing boundary values and wipeout the system and files when geo - fencing and MAC Address is mismatch.

REFERENCE

[1] Maksim Avdyushkin Dept. of Comput. Sci., Thompson Rivers Univ., Kamloops, BC, Canada " Secure Location Validation with Wi-Fi Geo-fencing and NFC " **Published in:** Trustcom/BigDataSE/ISPA, 2015 IEEE.

[2] Teduh Dirgahayu , Feri Wijayanto Department of Informatics, Universitas Islam Indonesia, Yogyakarta, " Location-based Request Forwarding in A Geo-fencing Application with Multiple Providers" **Published in:** Technology, Informatics, Management, Engineering & Environment (TIME-E), 2015 International Conference.

[3] Eric Wang International Bilingual School at Hsinchu Science Park, Hsinchu 300, Taiwan "Identification of Flight Safety Zones for Unmanned Aerial SystemsUsing Geo-Fencing Data Provided by Prebuilt Maps" **Published in:** Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT), 2016 11th International

[4] Yang Liu , Renli Lv, Xiangmin Guan Civil Aviation Management Institute of China, Beijing, 100121, China "Path Planning for Unmanned Aerial Vehicle under Geo-Fencing and Minimum Safe Separation Constraints" **Published in:** Intelligent Control and Automation (WCICA), 2016 12th World Congress

[5] Su Mon Kywe , Yingjiu Li School of Information Systems, Singapore Management University, Singapore " Attacking Android Smartphone Systems without Permissions " **Published in:** Privacy, Security and Trust (PST), 2016 14th Annual Conference on Auckland, New Zealand.

[6] Anthony .C. Ijeh, David .S. Preston, Chris .O. Imafidon Member, IAENG " Geofencing Security Engineering"