East Carolina University

College of Technology and Computer Science

Department of Technology Systems

Geo-fencing Technologies and Security

William Jason Haddock

ICTN 4040 – Enterprise Information Security

Dr. Phil Lunsford

April 11th, 2016

Abstract:

The author explains geo-fencing and how it works and its applications in the real world, including how they pertain to information security and also elaborates the strengths, weaknesses, opportunities, and threats associated. The author includes more information about implementing a geo-fence within a wireless network and the methodology used to contain, fingerprint, and allow mobility of secure data across a network. Geo-fencing is shaping our world and information security professionals need to develop strategies for it in regard to information assurance.

Geo-fencing Technologies and Security

Geo-fencing is a trending innovation that is only beginning to gain ground in today's mobile devices and security, even though it has been used in certain industries since the concept was invented. A geo-fence is a virtual perimeter for a real-world geographical area based of global positioning systems. The existence of global positioning systems (GPS) allow for device tracking and exploitation of mobile networks to increase productivity and revolutionize our daily activities. This explosion in tracking data and the use of mobile devices is increasingly of great concern for information security and information assurance. The development and use of geo-fencing allow for tracking, mobility, security, and management of those devices while entering or exiting a secured wireless network.

There are several technologies that allow a geo-fence to work; geo-location, geo-tagging, and geo-triggers. Geo-location, or GPS, is used to locate a person, vehicle, or any mobile object. It allows for location based services (LBS) to be integrated into applications like Google Maps, Waze, or any application that requires the user to turn on location tracking in the settings to work properly. Geo-tagging is the process in which geographical identification is added to any piece of information that can be transmitted, such as texts, photos, documents, which all can be used to track where the information was transmitted from. Geo-triggers are events in which a virtual barrier is crossed, which allow the tracking of entry and departure from a geographical zone or buffer. Geo-fencing allows a notification service to be setup for when geo-triggers, geo-tagging, or applications use LBS. The implementation of geo-fencing requires the construction of a virtual object in the computer application, designed using any geometric shape and representing the perimeter around the geographical zone being monitored (*Nait-Sidi-Moh 129). It is necessary to set parameters specific to the issue or area, such that a calculation will allow an

administrator to see if the device has breached the limits or not. There are several applications or uses a geo-fence could provide. Imagine an imported container that has a RFID/GPS tag, and is on a container ship entering a port of call. The geo-trigger would be the ship being detected as crossing the virtual barrier, and an alert message is sent to the administrator, or in this case the dispatcher handling the truck meant for hauling that container. Now imagine that the truck hauling the container has left the port, and arrives at its' destination. At the destination there is another geo-trigger that sends an alert to the dispatcher that the container ship has been delivered. There are several points at which there may be a geo-fence being crossed and geo-triggered in this example. This is just one example of a geo-fence. Imagine on a lot grander scale with the 25 billion devices we will have connected by 2020 (Smith 37). There are other uses and different types of geo-fencing applications that can also be implemented. Geo-fencing zones can function as a point of access control and the ability to access proximity information. Geo-fenced time areas can control access of a user to scheduled time-frames, and limit hours of access to certain sites, like parking garages or a server room. Geo-fenced routes can control entering and exiting of devices and can prohibit access to a the area that was crossed, basically like making sure for example an airplane follows a predetermined route. Dynamic geo-fences can make measurements based on LBS, and for example can actively check the speed of a truck regularly and determine if the driver is speeding, and issue a fine or violation ticket. Many of these types of geo-fences are basic in concept, but still require development

There are strengths, weaknesses, opportunities, and threats faced in the implementation of geo-fences. The implementation of geo-fencing have benefits such as increasing work efficiency, productivity, tracking, interconnectivity between networks, and security of those devices while within the geo-fenced network. However, there are some weaknesses, such as

requiring the approval of the user to turn on LBS, and is only effective when data from other sources is mobilized in unison. The heavy usage of the battery, network capacity, device capacity, and battery life are constraints for this technology (Ghanchi). As compared to alternate technologies like Beacon, which gives location data in micro spaces, geo-fencing is limited to a fixed area, but good for large areas. The opportunities for geo-fencing are tremendous. Enabling businesses to track their customers with whom have activated the LBS within the application for the specific device will allow for them to specifically target their customers if they were to say, walk into an shopping mall, where they would receive a text message or pop-up from the application for their store advertising a sale on a particular product (Brousell 14). This leads to increase in sales and business growth and reaching the widest audiences with notifications. Threats to information security are rare, but can be hacked simply because if someone were able to breach a network that has LBS enabled, they would be able to track specific devices down to the user level, and that would be a tremendous breach of security, especially if the hacker were able to isolate the user's device. Geo-fenced devices are naturally very secure, often times only given access to an internal network if a VPN had been setup previously to the device from a network administrator, and also previously fingerprinted from within the system.

Geo-fencing allows for the security of those devices while the mobile device traverses across one wireless access point to another, but also allows for specific fingerprinted devices to have access to information while connected to a specific access point within a geo-fenced area. This is called containment. Once a device exits the geo-fenced area, their access will automatically cut off, but once they step back in, they will have to log in again (*Ijeh 110). Devices can be fingerprinted for better synchronization and ease-of-access. The methodology

behind determining the precise geographical location of a wireless device when it performs one or all of the following:

a) If the wireless device was logged onto within the geo-fenced area.

b) If the wireless device was logged onto outside the geo-fenced area.

c) If the wireless device was able to stay logged on outside of the geo-fenced area, if taken from within to the outside of the geo-fenced area.

d) If the wireless device can be logged onto on the boundary of the geo-fenced and non geo-fenced area.

(*Ijeh 110).

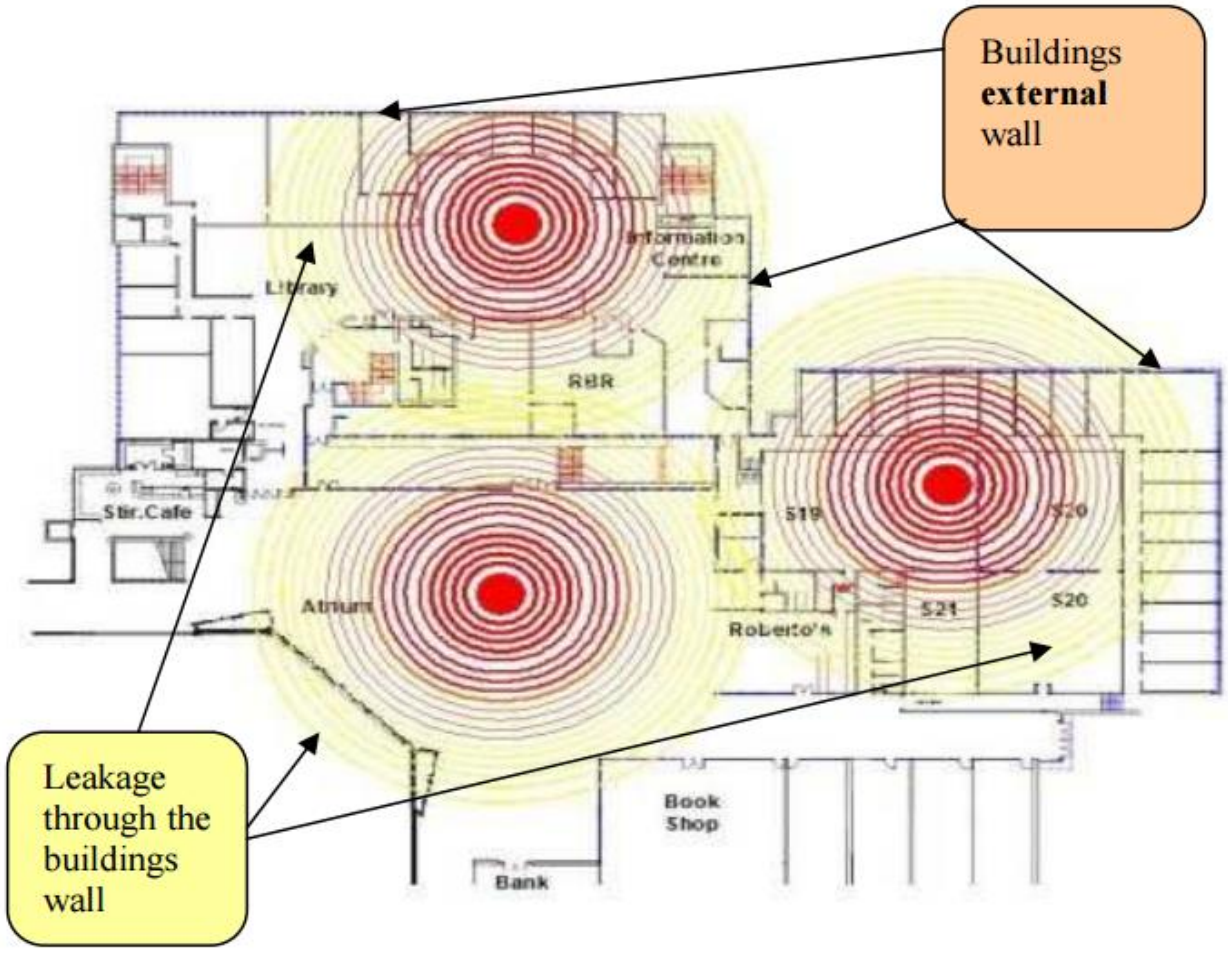

Figure 1. Illustration of leakage across geographical spaces of a wireless network. (*Ijeh 105)

The security of a geo-fence largely depends on setting up predefined areas, with a set of rules and enforcements for the specific area. For example, a computer can get on only a specific wireless access point in a specific building or apartment. Limiting radio wave leakage is also key, to limiting network access to devices on the boundary of the network, by placing an access point in an area that lets the access point cover only the area intended, separating different departments or buildings from each other. See Figure 1. Wireless networks are still susceptible to attacks from an external source.

In conclusion, geo-fencing is shaping our world we live in, and information security professionals need to develop security strategy models in order to help circumvent the amount of data that is traversing the internet of things, and to help keep data secure across their network by developing a geo-fenced network, whether it uses any of the types of geo-fences, it will increase efficiency and productivity, and allow for seamless transition when traversing between networks. Geo-fencing is a trending innovation and more and more businesses and information security professionals are using. Geo-fencing has tremendous opportunities for development and business uses and will continue to help drive sales and reach more consumers with notifications through the device itself, as it is detected as entering a mall or storefront.

Works Cited

Brousell, Lauren. "5 Things You Need to Know: Geofencing: This location-based mobile service lets marketers send messages to smartphone users when they enter a defined geographic area, such as a shopping mall." CIO 26.14 (2013) *ProQuest*. Web. 10 April 2016.

Ghanchi, Juned. "Advantages and Disadvantages of Geofencing Applications." *IndianAppDevelopers*, 1 June 2015. Web. 10 Apr. 2016.

Ijeh, Anthony C., Allan J. Brimicombe, David S. Preston, and Chris O. Imafidon. "Geofencing in a Security Strategy Model." Proceeding. *SpringerLink*, 01 Jan. 2009. Web. 10 Apr. 2016.

Nait-Sidi-Moh, Ahmed, Bakhouya, Mohamed, and Gaber, Jaafar, eds. Geopositioning and Mobility (1). Somerset, US: Wiley-ISTE, 2013. *ProQuest*. Web. 10 April 2016.

Sheehan, Matt. "Mobile GIS and GeoFencing." GeoInformatics 16.3 (2013): 16. *ProQuest*. Web. 10 April 2016.

Smith, Michael S. "Protecting Privacy in an IoT-Connected World." Information Management 49.6 (2015): 36. Web.

Whitehead, Jennifer. "Analysis: Geofencing Tipped as Hot Trend for 2014." Retail Week (2014) *ProQuest*. Web. 10 April 2016.