ISSN 2349-0292
Impact Factor 2.365

Global Journal of Advanced Engineering Technologies and Sciences

INFORMATION SECURITY AND SAFETY IN CYBERPARKS

Jamal Raiyn[*1]
[*1]Computer Science Department Al Qasemi Academic College, Baqa Al Garbiyya, Israel.

Abstract

This paper discusses information security and safety issues in public open spaces. Public open spaces may include high streets, street markets, shopping centres, community gardens, parks, and playgrounds, each of which plays a vital role in the social, cultural and economic life of a community. In this paper we introduce the term *CyberPark*, which refers to an outdoor public place mashed-up with various ICT tools. Security and safety in public places may include video surveillance of movement and the securing of information and location based service. In this paper, we provide an overview of secured information in communications between user end devices and service providers.

Keywords: Secured Information, cyberParks, public places.

Introduction

Cities offer various kinds of public places, and these are created for different targets. There are public places for students and others on academic campuses, for visitors to historical sites, and for families and tourists. Public open spaces that are supported by various kinds of modern information communication technologies are called Cyberparks [16]. The major goal of using information communication technologies a CyberPark is to promote better use of the outdoor environment. Nowadays, we are witnessing many developments in internet technologies and communication that are providing connectivity services to users on their personal computers, smart phones, tablets and other mobile end devices. Many users use internet technologies for storing private data; planning travel by bus, train or plane; and shopping. Furthermore, internet technologies are used for communication in business, the military, medicine, education [18], and government and public services. Over the last decade, as well, crime in virtual life has increased. Some people use internet to attack others. Cyber attacks are performed through internet networks that target individual machines, mobile end devices, communications protocols, or smart phone application services, in order to acquire private information. Cyber attacks are performed by spreading malware, by creating phishing web sites, and by other means[6, 7]. The attackers, also known as hackers, carry out attacks for different reasons and with different motivation. Typically, they attempt to gain sensitive information regarding the victim. Cyber criminals Information and information systems [1,4,5,9].

The next section presents an overview of, and discusses techniques to counter, various cyber types of cyber attacks, which can involve the use of malware like computer viruses, worms, Trojan horses, spyware and adware, as well as denial-of-service attacks, phishing, and man-in-the-middle attacks [10,12]. Cyber security aims to prevent unauthorized access to digital devices like PCs, laptops, and smart mobile phones, as well as to wireless communication protocols and wireless routers. Web browser's privacy protocols mostly have default settings that can be affected by malware attacks by allowing communication with cookies and other applications that contain information about internet activity. For instance, many smart phones include a GPS that knows the device's current location. Cyber attacks use smart phone apps to track online activities and users plans.

This paper is organized as follows: Section 2 introduces information security strategies. Section 3 introduces the security model. Section 4 introduces the security concept. Section 5 concludes the paper.

Information Security Strategies

This section introduces various information security strategies that have been proposed to ensure the safety of mobile end users in CyberParks. The private information of CyberPark visitors should be secure. Many web services and smart phone applications incorporate a user's location in order to offer relevant information. Some mobile services use the smartphone's location to offer directions, public places, or to offer other location-specific information to the user. Furthermore user's location can be determined by using social media services like Twitter,

Instagram, and Facebook. Following are some information security strategies have been proposed to secure information [12].

Authentication
Authentication refers to process of obtaining a confirmation that a user who is requesting a service, is a valid user. It is accomplished via the presentation of an identity and credentials, such as passwords, one-time tokens, digital certificates, and phone numbers (calling/called) [3].

Authorization
Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication. The process may involve restrictions, for example time-of-day restrictions, physical location restrictions, or restrictions against multiple logins by the same user. Examples of services include IP address filtering, address assignment, route assignment, encryption, QoS/differential services, and bandwidth control/traffic management.

Network Access Server (NAS)
A network access server (NAS) is a service element that clients dial in order to get access to a network. The server usually has interfaces both with the backbone and with the telco (POTS or ISDN) and receives calls from hosts that want to access the backbone via dialup services. A NAS is located at an internet provider's point of presence to give their customers internet access [2].

Four-Way Handshake
The authentication process involves two considerations [7]:
The service provider still needs to authenticate itself to the client and keys to encrypt the traffic needs to be derived. The earlier EAP exchange provided a shared secret key, the pairwise master key (PMK). This key is designed to last an entire session and should be exposed as little as possible.

Extensible Authentication Protocol (EAP)
This is protocol [8] is based on the point-to-point protocol (PPP) and facilitates remote authentication. The EAP allows for end-to-end authentication between a mobile station and an authentication server (AS). The EAP is a generic protocol that allows different authentication mechanisms (called EAP methods) to be transported.

PGP Encryption/ Decryption
Nowadays, the PGP is in common use. During encryption in PGP the plaintext is first compressed, to reduce message transmission time and to increase security. Compressing the plaintext increases security against cryptanalysis. PGP decryption is the reverse process used by message receiver. The receiver decrypts the session key using his or her private key. Then, the PGP uses the same key to decrypt the plaintext. In addition to text is visual cryptography is used for image encryption, The image is divided into transparencies, which are sent to the user at the receiving end they are decrypted to get the original image [14].

Security Models

To implement information security policies and safety in CyberParks [16], security models are needed that lay out guidelines for securing information and communication. CyberPark security models are based on formal models of access rights to smart phone applications and web services. This paper introduces a system model that is based on adaptive agents to increase security and safety in CyberParks. Visitors to the CyberPark can use various information technology applications: cell phones, web services, and interactive digital maps to obtain information about the CyberParks. An adaptive agent recognizes the applications that being used, and a mobile agent platform [17] creates mobile agents to serve the CyberPark visitors. By monitoring the behavior of users, detection systems ensure information privacy.

ISSN 2349-0292
Impact Factor 2.365

Mobile Agents Tasks

A mobile agent aims to fulfill user's preferences based on a dynamic environment. The mobile agent's structure is divided to three parts, as follows:

Source code: The program consists of several classes to define the agent's behavior. In the source code, we create the backbone of the agent, which contains the basic rules. The agent then grows and develops itself according to the requirements of its environment.

State: The agent's internal variables enable it to resume it is activities when it is found to be in one of the following states: Offline (sleeping, in an evolution process), Online (awake), Busy, Waiting (standby), or Dead.

Attributes: Attributes consist of information describing the agent, its movement history, its resource requirements, and authentication keys

Secured communication protocol

In order to mediate useful tasks, we use a communication model to establish communication between mobile end users and the CyberPark service provider. The agents in the system should be able to understand each other, and they should use the same message transport protocol. Messages are a data oriented communication mechanism, generally used to transfer data between processes Messages are either asynchronous or synchronous.

Roaming in CyberParks

The term "roaming" originates from the context of GSM. Traditional GSM roaming is defined as the ability of a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, through the use of a visited network. Furthermore, roaming refers to the ability to move to a foreign service provider's network. It is, consequently, of particular interest to international tourists and business travelers (international roaming).

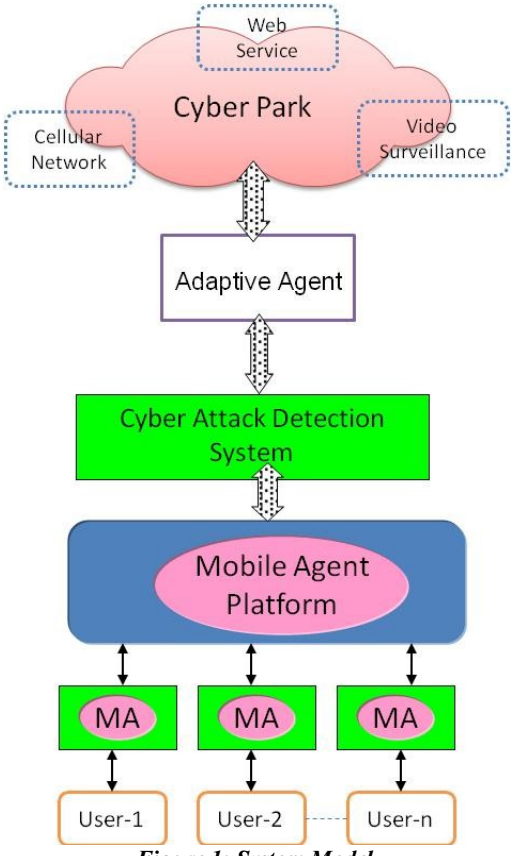

Figure 1: System Model

ISSN 2349-0292
Impact Factor 2.365

Concept of Secured Information

Authentication Form

To increase information security, users need a password to log in. The system starts the identification process and creates a mobile agent for each user, as shown in Figure 2. The mobile agent is responsible for communication security in the system.

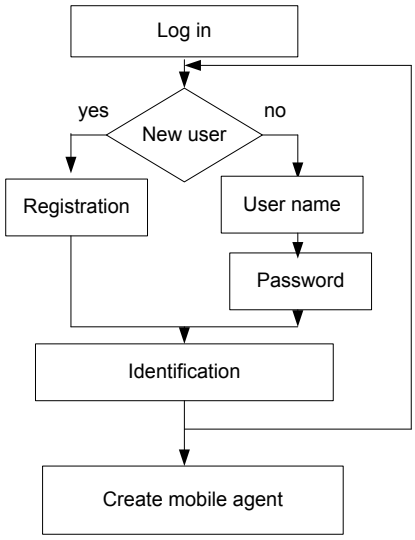

Figure 2: Authentication Process

Establishing a Protocol

Messages are a data oriented communication mechanism [15]. Request/ response message will be used to transfer data between a user end device and a service provider. Two kinds of message are used in the model.

- Inform message: The Inform message includes the mobile device ID and the kind of information requested.
- Re-inform message: The Re-inform message includes information about Cyber Park resources.
- Request message: the request message includes the sender's name, a time stamp that indicates the time the request message was generated, the receiver's name and the requested resource.
- Response message: The response message includes the sender's name, a time stamp, and the requested resource.

Secure Services

CyberParks provide various resources and services. Visitors to CyberPark should be registered in order to manage the CyperPark's resources. Figure 3 illustrates the CyberPark's resources and services. To increase information security communication between the mobile end user and service should be aware. It is necessary to checking the identity of the communication parties before establishing communication and allowing users access to information. Some users will follow a conventional scheme to access secure information; namely, they access CyberPark services with a password. Every user is allocated a mobile agent called a home agent. The home agent creates a new PIN number to access services. The PIN number is a password shared between a user and a system that aims to authenticate the user to the system.

ISSN 2349-0292
Impact Factor 2.365

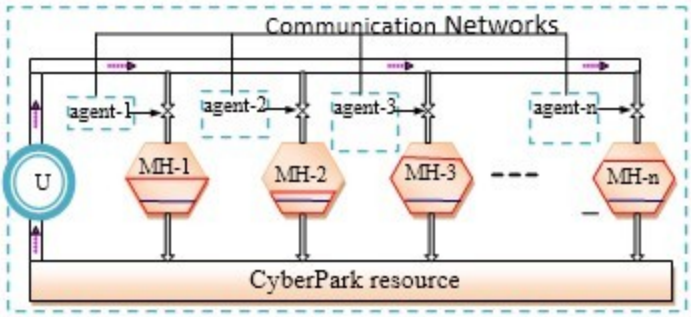

Figure 3: Resource control

Cyber Security And Privacy

It is important for CyberPark visitors to keep their location secret [13]. The privacy approach aims to protect private position information , as shown in Figure 4. The mobile agent works to hide the identity of the user and his or her activity in CyberPark services while the location for the user is visible. This prevents a cyber attacker from detecting the location of users.

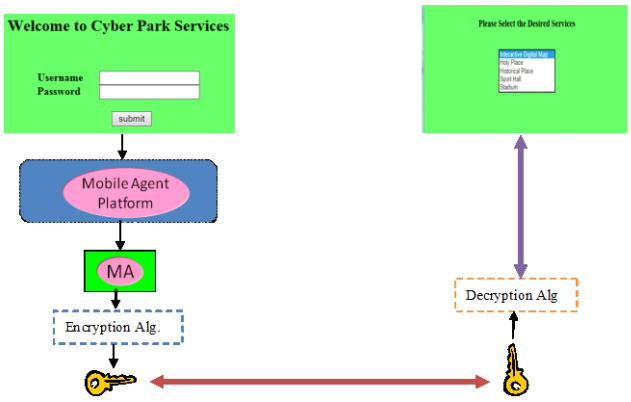

Figure 4: Information Security

Conclusion

It is important for CyberPark visitors to keep their location secret [13]. The privacy approach aims to protect private position information , as shown in Figure 4. The mobile agent works to hide the identity of the user and his or her activity in CyberPark services while the location for the user is visible. This prevents a cyber attacker from detecting the location of users.

.

Acknowledgement

This work was conducted within the framework of TUD COST Action TU1306 "Fostering knowledge about the relationship between information and communication technologies and public spaces supported by strategies to improve their use and attractiveness "(CYBERPARKS).

ISSN 2349-0292
Impact Factor 2.365

Reference

1. E. Bou-Harb, M. Debbabi, and C. Assi: "Cyber Scanning: A Comprehensive Survey", IEEE Communications Survey & Tutorials, Vol. 16, No. 3, Third Quarter, 2014.
2. C. He and C.J.Mitchell: "Security Analysis and Improvements for IEEE 802.11i", In Proceedings of the Network and Distributed System Security Symposium, 2005.
3. H .Changhua and C.J. Mitchell: "Analysis of the 802.11i 4-Way Handshake".
4. K. R. Karthikeyan and A. Indr, "Intrusion Detection Tools and Techniques A survey", International Journal of Computer Theory and Engineering, Vol. 2, No. 6, 2010, 901-906.
5. R. S. Dewar, The "Triptych of Cyber Security": A Classifi cation of Active Cyber Defence, 6th International Conference on Cyber Confl ict, 2014, 7-21
6. J. Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, Vol.8, No.1, 2014, 247-256.
7. S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International of Computer Science and Network Security, Vol. 9, No. 5, 2009, 1-10.
8. S. Patel, Analysis of EAP-SIM Session Key Agreement. Available at https://www.ietf.org/proceedings/57/slides/eap-11.pdf
9. M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification", International Journal of Network Security, vol. 15, no. 6, 2013, 391-397.
10. A. Zarrabi and A. Zarrabi, "Internet Intrusion Detection System Service in a Cloud", International Journal of Computer Science Issues, Vol. 9, issue 5, No. 2, 2013, 308-315.
11. Z.Ynos, R.Ahmad, and M.Yusoff, "Grounding the Component of Cyber Terrorism Framework Using the Grounded Theory", *Science and Information* Conference 2014, August 27-29, 2014, 523-529.
12. R. Von Solms and 1. Van Niekerk, "From information security to cyber security" , Compul. Secur., vol. 38, 2013, 97-102,
13. M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches", Pers Ubiquit Comput, 2014, 18:163–175.
14. S. Garfinkel., PGP: Pretty Good Privacy, O' Reilly & Associates Inc., 1995.
15. J. Raiyn, Development of Resource Allocation Strategies Based on Cognitive Radio, LAMBERT Academic Publishing, Germany, 2014.
16. COST Action TY 1306 CyberParks. Available online: www.cyberparks-projects.eu.
17. J. Raiyn, **"**Using Adaptive Multimedia Mobile Agent in Heterogeneous Wireless Networks", IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (EUROSIM2007), September 9-13. Ljubljana, Slovenia. 2007, 495-501.
18. J. Raiyn, "Toward Developing Real- Time Online Course Based Interactive Technology Tools", *Advances in Internet of Things*, *4*, 2014, 13-19.