Access Control Based on Location and Time

Suresh Limkar[1], Nivedita Kadam[1], and Rakesh Kumar Jha[2]

[1] Department of Computer Engineering, GHRCEM, Pune, India
[2] Department of Electronics and Communication Engineering, SVNIT Surat, India
{sureshlimkar,Jharakesh.45,nivedita.kkadam}@gmail.com

Abstract. We propose an access control model that works like three factor authentication for getting access to our system. This system takes time and location into account to specify access control policies. We also discuss implementation techniques for location and time based policy specifications and the integration of these policies in standalone applications. This model enhances current security applications granting access to sensible information and privileges to execute orders only to entities that are in a trusted location with predefined time. Moreover this system authenticate authorized user but also time and location of the authorized user in both way i.e through GSM & GPS. The declarative nature of the model facilitates the analysis of policies and the evaluation of access requests: we present one case-study for clear understanding. This paper shows how computer and network security can be substantially improved through a new form of authentication based on geodetic location parameter received from GPS/ GSM along with the constraint of time.

Keywords: Cryptography, Encryption, Location based security, GPS, GSM, Biometric.

1 Introduction

We are moving towards an age of ubiquitous computing where location information will be an integral part of many applications. Denning, MacDoran [1] and other researchers [2], [3], [4], [5] have described how the use of location information can make applications more secure. Few examples will help to motivate our work. In a military application, if a computer containing top secret information is placed in a public place, then the computer should automatically become inaccessible. For instance, a user should be able to control or fire a missile from specific high security locations only. Verifying the location information and time parameter in addition to the checks that are performed by traditional methods of authentication and access control will improve the security of the underlying application.In this paper we propose one such formal model that is suitable for military applications. This paper shows how computer and network security can be substantially improved through a new form of authentication based on geodetic location and time. Location-based authentication has the effect of grounding cyberspace in the physical world so that the physical locations of network entities can be reliably determined.We illustrate how

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 102–107, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

location parameter received from GPS (Global Positioning System) and GSM (Global System for Mobile Communication) impacts to enhances current security applications granting access to sensible information and privileges to execute orders only to entities that are in a trusted location with predefined time. Finally, we show how this location information can be used to determine whether a subject has access to a given system or not. The rest of the paper is organized as follows. We describe basic information related to our works in section 2, and introduce the proposed model with its operation and its security analysis in section 3. Then in section 4, we evaluate its efficiency and results in the form of screen shots of working model. We present a case study in 5. Section 6 concludes the paper.

2 Background History

Before moving towards the architecture of the proposed system first try to get the acquaintance with the basic technology that are used in this model.

A.GPS

The Global Positioning System (GPS) is a U.S. space based radio navigation system that provides reliable positioning, navigation, and timing services to civilian users on a continuous worldwide basis freely available to all. For anyone with a GPS receiver, the system will provide location and time. GPS provides accurate location and time information for an unlimited number of people in all weather, day and night, anywhere in the world. The GPS is made up of three parts: satellites orbiting the Earth; control and monitoring stations on Earth; and the GPS receivers owned by users. GPS satellites broadcast signals from space that are picked up and identified by GPS receivers. Each GPS receiver then provides three-dimensional location (latitude, longitude, and altitude) plus the time.

B. GSM

Global System for Mobile Communications, or GSM (originally from Group Special Mobile), is the world's most popular standard for mobile telephone systems. The GSM Association estimates that 80% of the global mobile market uses the standard.[6] GSM is used by over 1.5 billion people [7] across more than 212 countries and territories.[8] This ubiquity means that subscribers can use their phones throughout the world, enabled by international roaming arrangements between mobile network operators. GSM differs from its predecessor technologies in that both signaling and speech channels are digital, and thus GSM is considered a second generation (2G) mobile phone system. This also facilitates the wide-spread implementation of data communication applications into the system.Mobile positioning, which includes location based service that discloses the actual coordinates of a mobile phone bearer, is a technology used by telecommunication companies to approximate where a mobile phone, and thereby also its user (bearer), temporarily resides. The more properly applied term locating refers to the purpose rather than a positioning process. Such service is offered as an option of the class of location-based services (LBS). [9] The technology of locating is based on measuring power levels and antenna patterns and uses the concept that a mobile phone always communicates wirelessly with one of the closest base stations, so if you know which base station the phone communicates with, you know that the phone is close to the respective base station. GSM localization is the use of multilateration to determine the location of GSM mobile phones, usually with the intent to locate the user.

C. Biometric

[10] It consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Here in this model we are using two location based services to get the location of the object i.e. through GSM or GPS. Intention behind using two locations based services just because both have their own advantages and disadvantages.

3 Need of Location Based Security

Information security fundamentally depends on the ability to authenticate users and control access to resources. Existing user authentication mechanisms are based on information the user knows (e.g., password or PIN), possession of a device (e.g., access token or crypto-card), or information derived from a personal characteristic (biometrics). None of these methods are foolproof. Passwords and PINs are often vulnerable to guessing, interception, or brute force search. Devices can be stolen. Cryptographic systems and one-time password schemes can fail even when the algorithms are strong. Typically, their security reduces to that of PINs or passwords, which are used to control access to keys stored in files or activation of hardware tokens. Biometrics can be vulnerable to interception and replay. Geodetic location, as calculated from a location signature, adds a fourth and new dimension to user authentication and access control without changing the existing security mechanism. It can be used to determine whether a person is attempting to log in from an approved location, e.g., a user's office building or home. If a user is mobile, then the set of authorized locations could be a broad geographic region (e.g., city, state, country). In that case, the login location serves to identify the place of login as well as to authenticate it. If unauthorized activity is detected, system will not allow him to access it.Authentication through geodetic location has many benefits. It can be performed continuously so that a connection cannot be hijacked, for example, if a user forgets to logout or leaves the premises without logging out. It can be transparent to the user. Unlike most other types of authentication information, a user's location can serve as a common authenticator for all systems the user accesses.These features make location-based authentication a good technique to use in conjunction with single log-on. A further benefit of geodetic-derived location signatures is that they provide a mechanism for implementing an electronic notary function. The notary could attach a location signature to a document as proof that the document existed at a particular location and instant in time.

4 System Architecture

The scheme aims to develop an architecture that will provide access control system based on location and time obtained by GPS /GSM. The scenario of the proposed approach is presented in fig.1. There are two phases: administrator and end user phase. First, before end user want to get access to the system she has to register herself with the system. Administrator will do the registration. Below are the detailed functions of the administrator and end user.

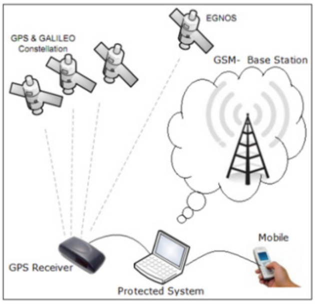

Fig. 1. System Architecture

A. Administrator

First every user needs to register with the administrator by providing its details like username, password, biometric identification, mobile number, and its location from which he would to access this system.

B. End User

One the end user completes its registration, then and only then he can access the system, otherwise he won't. Steps involved in authentication:

1. First end user need to enter his username password.
2. Once the first step is authenticated then next screen appears is to enter biometric credential.
3. Once the biometric credential of the end user is authenticated then next screen appears to enter pass code received on end users mobile. Passcode consist of alphanumeric message that end user need to enter in the text box.
4. Once the passcode is authenticated then it prompts for location check either through GSM or GPS
5. If user selects the GSM then mobile connected with end users system automatically send the users location info in the form of cell area, and get authenticate itself.
6. If user selects the GPS then GPS receiver connected with end user system automatically sends the GPS parameter i.e latitude, longitude, time and authenticates it.
7. While trying to provide location check either through GSM or GPS it automatically authenticate the user time too.

5 Security Analysis

The security analysis of a protocol is complicated as there are no standard metrics to precisely quantify the subject of security. To judge the performance and security of the proposed system, we developed an attack model. An attack model should provide possible failure modes due to the availability of the system. Furthermore, an attack model defines all possible attacks that might threaten the system. Whether a given systems is secure or not can depend dramatically on the attack model is considered.

Proposed system makes two types of errors:

a) FAR: Mistaking the measurements from two different locations to be from the same location, called false accept;
b) FRR: Mistaking the measurements from the same location to be from two different locations, called false reject.

Both false accept rate (FAR) and false reject rate (FRR) depend on the accuracy of the receiver and the grid interval size chosen to quantize the continuous location features.

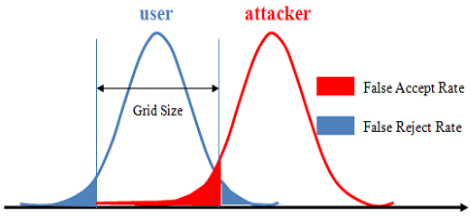

Fig. 2. False Accept and False Reject Ratio

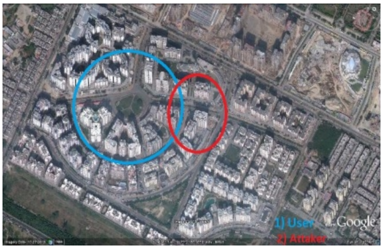

Fig. 3. Pune Based Test Location

These two types of errors can be traded off against each other by varying the grid interval size. Ideally, both low FAR and low FRR are desired. Practically, a more secure system aims for low FAR at the expense of high FRR, while a more convenient system aims for low FRR at the expense of high FAR. The desired interval size is highly dependent on the final application.

6 Conclusion and Future Work

A novel improved access control based on time and location based service model based on GPS and GSM is proposed and implemented to overwhelm the defect of traditional access control model. This scheme enhances current security applications granting access to sensible information and privileges to execute orders only to entities that are in a trusted location. However, the security of our improved scheme has a pre-condition that is the radio frequency signal (GPS signal) is secure, and an adversary could not capture the radio frequency signal. The proposed scheme can be extended to the other application domains, e.g., Employees can access sensitive data only inside a specified geographical area, an email can be decrypted only in predetermined locations, critical operations could be performed only inside a predetermined zone, and managers can analyze in real time the locations from which employees or customers are accessing the enterprise network on a geographical map (if privacy policy allows it), and attestation (proof) of position and contextual data (e.g. time) which could be included in the digital signature of an email, providing information on where and under what conditions the email was written.

References

1. Denning, D.E., MacDoran, P.F.: Location-Based Authentication: Grounding Cyberspace for Better Security. In: Proceedings of the Computer Fraud and Security. Elsevier Science Ltd. (February 1996)
2. Scott, L., Denning, D.: Location Based Encryption Technique and some of its Applications. In: Proceeding of ION NTM 2003 (2003)
3. Jarusombat, S., Kittitornkun, S.: Digital Signature on Mobile Devices based on Location. In: International Symposium on Communications and Information Technologies, ISCIT 2006, APOS, pp. 866–870 (2006)
4. Liao, H.C., Chao, Y.H.: A new data encryption algorithm based on the location of mobile users. Information Technology Journal 7(1) (2008) ISSN 1812-5638
5. Liao, H.C., Lee, P.C., Chao, Y.H., Chen, C.L.: A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. In: The 9th International Conference on Advanced Communication Technology (ICACT 2007), Phoenix Park, Korea, February 12-14, pp. 625–628 (2007)
6. Zhou, J., Alshamsi, A.: GSM World statistics. GSM Association (2010) (retrieved June 08, 2010)
7. GSM Technical Data, Cellular.co.za (retrieved August 30, 2010)
8. Two Billion GSM Customers Worldwide. 3G Americas (June 13, 2006) (retrieved January 08, 2007)
9. Wang, S., Min, J., Yi, B.K.: Location Based Services for Mobiles: Technologies and Standards. In: IEEE International Conference on Communication (ICC), Beijing, China (2008)
10. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634 (2001)
11. Qiu, D.: Security Analysis of Geoencryption: A Case Study Using Loran. In: Proceedings of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS (2007)