© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Website Security using GeoLocation and Behavior Patterns in Cloud Computing

Shri Dilipkumar N. Padhiar, Shri U. L. Patel
Assistant Professor, M. B. Patel Science College, Anand, Gujarat, India
Assistant Professor, C. U. Shah Science College, Ahmadabad, Gujarat, India

ABSTRACT

The purpose of this research paper is to research the use of location and user behavior patterns in authentication and fraud detection. The research paper introduces a new approach of detecting fraud and internet attacks by using geolocation. The new approach is the result of an effort to standardize the ways an information system may use to authenticate a user and detect fraud based on geolocation. Using geolocation as an authentication mechanism poses multiple issues and challenges including that location is not a suitable authentication factor, there are privacy concerns related to tracking user location and user location information can be forged. However, location and user behavior based security is not going to be a replacement for existing authentication and fraud detection mechanisms. It is intended to augment current technologies and make security attacks more difficult and be a deterrent against internet fraudsters.

Keywords : Cloud Computing, NIST, Website Security, SAML

I. INTRODUCTION

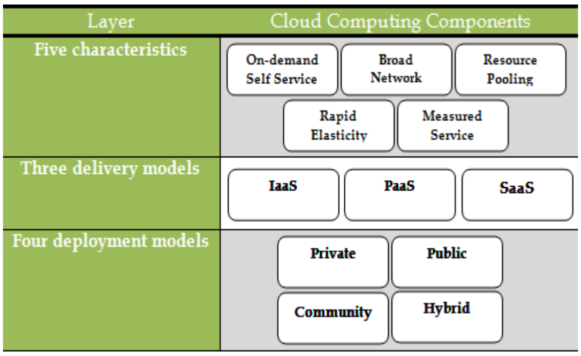
An importance topic in IT security is trust. What can we trust? "In fact, trust is difficult to address and even more difficult to quantify."[i]

- Can we trust that a transaction is performed from the computer specified by the IP included with the transaction? It can be that an attacker is spoofing the IP.
- Can we trust the user and password used to authenticate a user are used by the actual user and they were not stolen?

How we can profile the user behavior and detect when we can trust a user or a transaction by detecting abnormal transaction based on end user behavior and his geolocation. "Geolocation is the ability to determine where online visitors are physically located. With geolocation, merchants can use information they already have to non-intrusively determine where their customers are physically located."[ii] For these abnormal transactions a higher level of security can be enforced. Fraud prevention and Internet application access control is key to any web application. A hacker has a huge number of opportunities that he can exploit to intrude or attack an IT system or network. As soon as one security "hole" is plugged, many more are discovered. The goal of an attack is to plant a "back door" in the system that will allow the hacker to reenter later at will.

II. Cloud Computing

Cloud computing is a relatively new business model in the computing world. In an October 2009 presentation titled "Effectively and Securely Using the Cloud Computing Paradigm,"[iii] by Peter Mell and Tim Grance of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, Cloud computing is defined as follows: "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[iv]



Layer	Cloud Computing Components
Five characteristics	On-demand Self Service Broad Network Resource Pooling Rapid Elasticity Measured Service
Three delivery models	IaaS PaaS SaaS
Four deployment models	Private Public Community Hybrid

Figure 1: Cloud Computing

Five Characteristics:

1. On-demand self service: On-demand self service provides automatic computing capability management to systems, without requiring human interaction.

2. Broad Network: Broad network access allows heterogeneous clients. Such as mobile phones, laptops to connect to Cloud systems over the network

3. Resource Pooling: Resources pooling in Cloud systems is available as pooling resources for multiple consumer which is able to dynamically assign and reassign according to consumer demand.

4. Rapid Elasticity: Rapid elasticity offers rapidly and elastically provision of capabilities. We can grow and shrink our capacity very quickly in minutes or hours.

5. Measured Service: Measure service provides monitoring, controlling & reporting of resources usage.

Three Cloud Service Models:

Infrastructure as a Service: Service provider bears all the cost of servers, networking equipment, storage and backups. We just have to pay to take the computing service. And the users build their own application software's. Amazon EC2 is an example of this type of services.

Platform as a Service: Service provider only provider platform for user. It helps user saving investment on hardware and software. The customer has the freedom to build his own application, which run on the provider's infrastructure, to meet manageability and scalability requirement of the application. PaaS provider offers a predefined combination of OS and application servers. Google Gc engine and force.com are an example of this type of services.

Software as a Service: In this model, a complete application is offered to the customer, as a service on demand. A single instance of the services runs on the Cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. Today SaaS is offered by companies such as Google, salesforce, Microsoft, Zoho, etc.

III. Statement of Purpose

Research is required to authentication mechanisms used in web based systems. The focus is on how fraud attacks are mounted on web applications and access control solutions to prevent such fraud attacks. One component of fraud detection/access control is implementing monitoring tools that look for ***fraudulent behavior and access patterns.*** These monitoring tools should examine information and then compare it to rules, and use an analytic engine to detect geolocation data, device information and behavior patterns that do not fit typical patterns, all signs of fraudulent transactions. If a user tries to access a web applications outside his preferred locations, the new location will be resolved from an IP and the application will respond based on the new location predefined rules. This is an interesting approach to web access control and coupled with personal verification question in high risk scenarios and customizable rules proved to be a very effective fraud prevention mechanism.

There are multiple attributes that determine a user behavior pattern. Ines Brosso, Alessandro La Neve, Graca Bressan and Wilson Vicente Ruggiero define the user behavior by the following attributes like who, where, when what and why.[v]

First, we introduce concepts of how an internet transaction system is architected.

Internet Transactions: A definition of transaction processing is "A type of computer processing in which the computer responds immediately to user requests. Each request is considered to be a transaction."[vi] A web application is interacting with the end user through a web browser that is running on the end user machine. The browser displays the web pages rendered by the internet application that is running on a remote server and it is usually a database. The browser and server are communicating using TCP/IP and HTTP protocols.

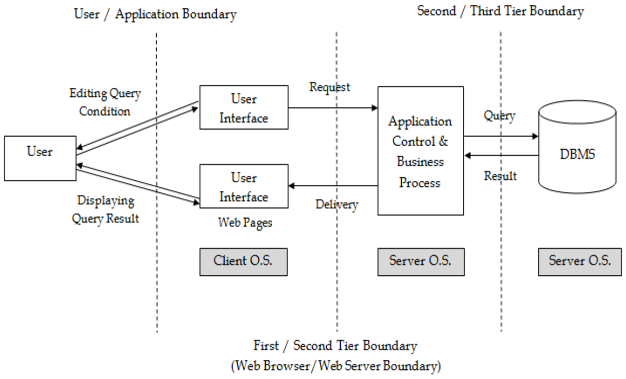

User / Application Boundary
Second / Third Tier Boundary
Editing Query Condition
User
User Interface
Request
Application Control & Business Process
Query
DBMS
Result
User Interface
Displaying Query Result
Delivery
Web Pages
Client O.S.
Server O.S.
Server O.S.
First / Second Tier Boundary (Web Browser/Web Server Boundary)

Figure 2: Internet Application Architecture

IV. Real time Fraud/Authentication

Location based services have one important characteristics which is to establish a user context. The user context has the following information. System properties has all the system properties like IP – Internet Protocol ID and Device MAC – Unique device ID. User information has the user Information. Transaction Information has information about the transaction the user is performing like Time of transaction, Type of transaction and History of transaction. Location Information like Current location and Location history.

In Cloud, A user is using multiple devices, such as, a home or work computer desktop. The IP/location of this home computer is mostly fixed. *A user can also use a laptop or mobile device that can connect from remote location such as airports or restaurants. The IP and location of such devices is dynamic.* Any device has a MAC address that is assigned to the device. This allows having the following sessions.

1. Device Session: The main properties of this session are: MAC Address, IP Address and location. The MAC address is static and IP and location can change for a mobile device.

2. User Session: Once a user is authenticated, it establishes a user session with the remote system. At this time, the device session and user session can be associated.

V. Security Profiling Architecture

The solution intended to detect fraud is using geolocation, transaction monitoring and user behavior to detect anomalies in transaction patterns. The solution uses a SAML based authentication to communicate between the systems involved. The fraud detection system is using a historical data mining to detect if a transaction falls under the user pattern or is anomaly. For public websites, only a device session is required, for secure websites, a user session is required.

The system should use a scoring mechanism that would automatically look at information and analyze that information deviation from the normal state transitions and detect unusual behavior. For example, if you are accessing your computer at home and a few seconds later you connect to a Wi-Fi network in an airport, this can be a clear fraud indicator. This fraud detection mechanism can be even more refined, detecting the user pattern and scoring a fraud situation based on such patterns. These patterns can be created based on user historical data and they can be used trying to predict user behavior and develop scoring models. The diagram modifies the architecture diagram introduced above and adds the following components to this diagram.

1. Geolocation Server
2. Real Time Security Profiler (RTSP Server)
3. Application Security
4. LDAP Server

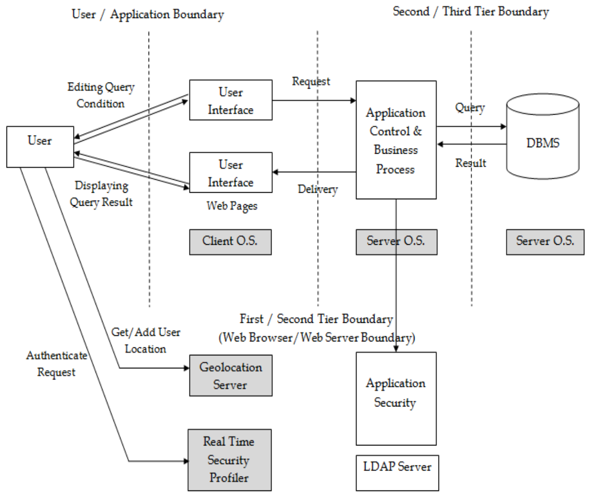


Figure 3 : Architecture of Fraud Detection System

The approach is that each transaction that is processed by the Internet Application is intercepted before processing and *sends to a "Real Time Security Profiler" (RTSP) Server.* Integration between the Internet Application and the new RTSP should be seamless. The application developer should not be required to do any application changes to create this integration point.

It is recommended that RTSP is configured at server or application container. The server or container has mechanisms to intercept the transaction that it is processed by the application. After the transaction is intercepted, a request is send to RTSP to establish that the request is valid. If the request is valid than the transaction is forwarded to the application, if not the transaction is declined and the end user/attacker is going to see an error. Another flow is that the server intercepts the transaction and detects that the transaction should be authenticated/ authorized and instructs the browser to perform the authentication/ authorization. The end-to-end transaction processing/validation flow is based on SAML authentication flow.

The following diagram describes the flow and the interactions between end user, browser, server and the RTSP (Identity Provider).

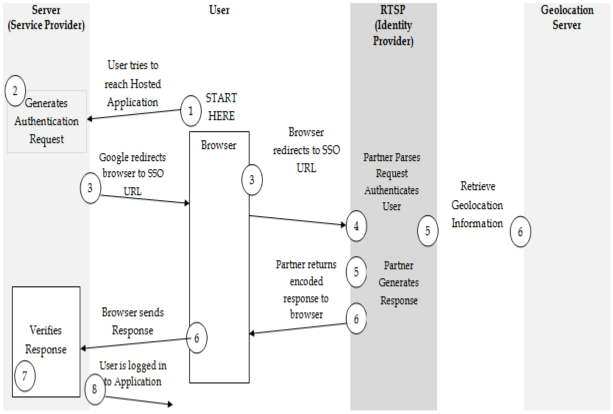

Server (Service Provider)
User
RTSP (Identity Provider)
Geolocation Server
User tries to reach Hosted Application
2
Generates Authentication Request
1
START HERE
Browser
Browser redirects to SSO URL
Google redirects browser to SSO URL
3
3
Partner Parses Request Authenticates User
Retrieve Geolocation Information
4
5
6
Partner returns encoded response to browser
5
Partner Generates Response
6
Browser sends Response
6
Verifies Response
7
User is logged in to Application
8

Figure 4 : Transaction Flow of Fraud Detection

This figure illustrates the following steps.

1. The user attempts to reach an Internet application.
2. The application generates the authentication request. The request is encoded and embedded into the URL for the Identity Provider.

The Internet Application sends a redirect to the user's browser. The redirect URL includes the encoded authentication request that should be submitted to the Identity Provider Service. The authentication request includes additional geolocation attributes like Device IP, Device MAC, Device coordinates, Cell Tower information, Wifi Information.

VI. REFERENCES

[i] Digital Resolve geolocation solution, http://www.digital-resolve.com/solutions/our_solutions.html
[ii] Geolocation, Wikipedia.com, http://en.widkipeida.org/wiki/Geolocation_software
[iii] Csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v25.ppt
[iv] (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)
[v] A Continuous Authentication System Based on User Behavior Analysis, Availability, Reliability and Security" International Conference on pp. 380-385.
[vi] Transaction Processing, Wikipedia.com, http://webopdia.internet.com/term/t/transaction_processing.html