УДК 004

Исследование методов аутентификации пользователей информационных систем по географическому местоположению

Смородин Владимир Александрович
Волжский политехнический институт (филиал) ФГБОУ ВО «Волгоградский государственный технический университет»
Студент

Лясин Дмитрий Николаевич
Волжский политехнический институт (филиал) ФГБОУ ВО «Волгоградский государственный технический университет»
Кандидат технических наук, доцент

Аннотация
В данной статье выполняется анализ метода аутентификации пользователей информационных систем по географическому местоположению
Ключевые слова: аутентификация, географическое местоположение.

The study of methods of authentication of users of information systems by geographical location

Smorodin Vladimir Alexandrovich
Volzhsky Polytechnic Institute (branch) of the Volgograd State Technical University
Student

Lyasin Dmitry Nikolaevich
Volzhsky Polytechnic Institute (branch) of the Volgograd State Technical University
Candidate of Technical Sciences, Associate Professor

Abstract
In this article, an analysis is made of the method of authenticating users of information systems by geographic location
Keywords: authentication, geographic location.

Контроль доступа информационные системы непростая задача. Сложности с паролями и безопасностью возникают как у крупных организаций, так и у частных пользователей. Решить данную проблему пытаются с помощью электронных ключей и прочих аппаратных средств.

Процесс входа в систему можно разделить на три этапа:

- идентификация.
- аутентификация.

- авторизация.

Новым способом аутентификации пользователей информационных систем является доказательство подлинности его личности по географическому местонахождению.

Постановка задачи

Аутентифицироваться в информационных системах пользователь возможно, используя разные методы:

1) **на основе знания**. пароль, PIN-код, секретные и открытые ключи.

2) **на основе обладания**. магнитные карты, смарт-карты, сертификаты, парольные дискеты или флэш-накопители;

3) **на основе каких-либо неотъемлемых характеристик**. Эта категория включает методы, основанные на проверке биометрических характеристик пользователя (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони, подчерк и др.).

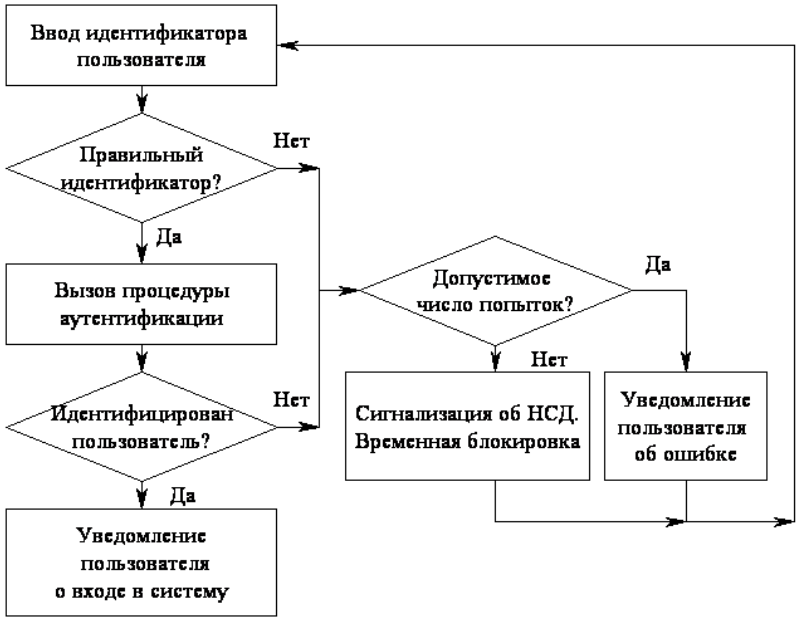

Рисунок 1 –Процедура идентификации и аутентификации

Новым способом доказательства подлинности пользователя является аутентификация по его географическому местонахождению. Данный защитный механизм основан на использовании навигации, типа GPS (Global Positioning System), а также на основе точек подключения к сети интернет.

Пользователь, обладающий оборудованием GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, с высокой точностью определяет географическое местоположение пользователя. Высокую надёжность обеспечивают колебания орбит спутников, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что чрезвычайно сильно затрудняет возможность их перехвата злоумышленниками.

Рисунок 2 –Аутентификация по геолокации

Технология GPS надёжна и проста в использовании, а также относительно недорога. Это позволяет её использовать в случаях, когда авторизованный пользователь должен находиться в необходимом месте.

Другой подвид – это аутентификация, основанная на местоположения выхода в интернет

Данный механизм основан на использовании данных о местоположении серверов, точек доступа беспроводной связи, с помощью которых осуществляется подключение к сети интернет. Крупные организации всё чаще и чаще используют аутентификацию пользователей для улучшения сервиса. В качестве примера можно привести Uber, Google, eBay, Amazon.

Хотелось бы затронуть тему двухфакторной аутентификации. Данный вид аутентификации подразумевает под собой идентификацию пользователя в информационной системе при помощи запроса аутентификационных данных двух разных типов. Такой вид аутентификации используют многие сервисы: вконтакте, яндекс, google, icloud. Все эти сервисы кроме стандартной парольной аутентификации используют ещё и географическое местоположение пользователя. Например социальная сеть «вконтакте» при определении входа в систему из необычного для пользователя места попросит аутентифицироваться не только знаковым паролем, но и дополнительными средствами с помощью электронной почты, SMS или генератора кодов. Данный вид аутентификации увеличивает защиту аккаунта. Злоумышленнику придётся не просто украсть пароль «жертвы», но ещё и его почту или мобильный телефон.

Клиент отправляет на сервер хэш-функцию аутентификатора содержащего географические координаты, логин и пароль.

$k \rightarrow h(A\{x,y,l,p\}) \rightarrow s$

Сервер в свою очередь сверяет аутентификационные данные с базой данных и передаёт ответ пользователю.

$s \rightarrow h(Q)$

где,

k – клиент

s – сервер

A – аутентификатор

h – хэш-функция аутентификатора

x – широта

y – Долгота

l – Логин пользователя

p – Пароль пользователя

Q – Ответ сервера

Возможность геолокации состоит из трех методов объекта navigator.geolocation: getCurrentPosition(), watchPosition() и clearWatch().

Объект navigator — это малая часть JavaScript. Его несколько свойств предоставляют информацию о текущем браузере и его возможностях. Самым полезным является свойство navigator.userAgent, оно предоставляет информационную строку в которой содержатся подробные данные о браузере, его версия, а также операционной системе, в которой он выполняется.

Хочется отметить простоту реализации. Для получения местоположения посетителя вызывается метод getCurrentPosition().При его вызове передается функция завершения (completion function).

В качестве самых популярных инструментов определения географического местоположения можно выделить

1. GPS - определение местоположения выполняется с помощью спутников
2. Cell ID - местоположение определяется с помощью вышек сотовой связи
3. A-GPS (Assisted GPS) – комбинированная информация со спутника и сервера.

В качестве положительных сторон аутентификации по географическому местоположению можно выделить простоту реализации и сложность взлома. Относительная простота взлома состоит в том, что информацию о местоположении, используя аутентификацию основанную на местоположении выхода в интернет, можно изменить, используя прокси-серверы или анонимный доступ.

Библиографический список

1. Агибалов А.В., Горюхина Е.Ю. Автоматизированные системы обработки

экономической информации. Воронеж.: ВГАУ, 2000.
2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях. СПб.: Изд-во СПбГУЭФ, 2010. 267 с.
3. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса "Основы информационной безопасности". Интернет Университет Информационных Технологий, 2010г.
4. Лясин, Д.Н. Объектно-ориентированный анализ и программирование [Электронный ресурс] : учеб. пособие / Д.Н. Лясин, О.Ф. Абрамова; ВПИ (филиал) ВолгГТУ // Учебные пособия : сб. Вып. 1. - 1 электрон. опт. диск (CD-ROM). Волгоград, 2014. 98 с.