Integrating geolocation into electronic finance applications for additional security

Kevin Curran* and Jonathan Orr

Faculty of Computing and Engineering,
School of Computing and Intelligent Systems,
University of Ulster, Northern Ireland, UK
E-mail: kj.curran@ulster.ac.uk
E-mail: orr-j@email.ulster.ac.uk
*Corresponding author

Abstract: People are increasingly using the web to conduct business. It is, therefore, important that users of services such as online banking have confidence in such services. Frameworks such as Google Gears now have the ability to determine the physical location of a person in real time. This geographical information can be very useful in e-finance applications. If we know the geographical location of a computer performing a particular transaction, then we can ascertain whether unusual requests are being performed. This paper presents a prototype Geolocation enabled e-finance prototype to illustrate the benefits of monitoring geographical location of users. The application was developed to block locations with high levels of online fraud.

Keywords: geolocation; enterprise application development; e-finance; pervasive computing.


Biographical notes: Kevin Curran, BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA, is a Reader in Computer Science at the University of Ulster. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. He has published more than 600 published works to date. He is the Editor in Chief of the International Journal of Ambient Computing and Intelligence (IJACI). He is a Fellow of the Higher Education Academy, a Fellow of the British Computer Society and is listed by Marquis in their prestigious Who’s Who in Science and Engineering. He is also listed in the Dictionary of International Biography and by Who’s Who in the World.

Jonathan Orr (BSc) is a Graduate in Computer Science of the University of Ulster. He is presently working in the Northern Ireland Telecommunications industry with Allstate NI. He is employed as a Quality Manager in Infrastructure Services testing voice services. His research interests include distributed systems, low-level protocols and internet technologies.

Copyright © 2011 Inderscience Enterprises Ltd.
1 Introduction

One of the main concerns with e-finance is that of security (Lingfen et al., 2010; Jain and Kohli, 2009). Fraudulent and accidental security breaches are a rare occurrence as banks employ sophisticated procedures and systems to prevent these incidents. As a result, they invest a considerable amount of time and money in developing systems, which will prevent fraud and unauthorised access. The security used in online banking is a combination of technology and user authentication. The bank will use at least a 128-bit Secure Session Layer (SSL) encryption protocol between its server and the user’s browser. The user’s browser will show a padlock when the session is secure. Using SSL can be thought of as preventing eavesdropping. If a hacker were to attempt to listen to the data transmission, they would have to guess the decryption key, which is a 1 in $3.4 \times 10^{-38}$ chances, making it very secure (Carlin and Curran, 2011).

The weakest link of online banking is user authentication (Bapna and Patel, 2010). Typically, a user has to supply a set of answers to questions, which they have previously entered upon registration, as well as a username and password. The banks place the responsibility of keeping these answers secure with the user. If any answer is disclosed and money is stolen, the liability lies solely with the account holder, not the bank. Fraudsters, therefore, target the login details of users through a number of different scams to pose as the registered user and access their accounts, therefore bypassing security measures put in place by banks with ease. Researchers claim that despite the longstanding efforts of banks and the IT security community to warn end users, specifically people using online banking applications, to beware of phishing schemes, many people who open the e-mails and visiting the phony sites, still end up handing over their credentials. Online banking fraud is on the rise, and in the UK alone, there was a 55% rise from 2008. Improving security in terms of online banking is, therefore, a big concern.

Location awareness is becoming a part of web development since the introduction of mobile devices such as smartphones and PDAs (Harkin et al., 2010). Geolocation is the process of automatically identifying a web user’s physical location without that user having to provide any information. Such technology is already being implemented on the web to determine how a user arrives at country-specific websites for example. A user’s location can be very useful information as a host of services can be centred on a user’s location. The social networking site Twitter, for example, has recently incorporated geolocation. A Twitter user can now find what people are posting from the place where an important event is happening, or what people are saying about a specific restaurant or store.

Gears (formerly Google Gears) is software offered by Google that enables more powerful web applications by adding new features to your web browser. One of the features of Gears is the Geolocation API; this enables a web application to obtain a user’s geographical position. Gears is a set of JavaScript APIs that can be integrated into a browser. Our paper demonstrates us using the geolocation aspect of Gear in a prototype to show how it can be used to improve security of online banking by integrating the Gears API with an e-finance prototype.
2  Electronic finance and fraud

E-finance allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.4 Most large banks now offer online banking and therefore security to go with it. Banks spend years building up relationships with their customers and thereby a level of trust. For banks to convert people to banking online, they have to ensure that their customers will be safe and secure. After all, banking online benefits both the banks and its customers in general. Customers can bank from the comfort of their home and the banks save money on costly paper handling and teller interactions.

Many banks ask the user to enter their login details by selecting information from drop-down menus. Simply using menus rather than the keyboard stops keyloggers from quickly capturing passwords. Keylogging software is blamed for online banking fraud more than doubling in 2008. It soared to £52.5 m last year in the UK, up from £22.6 m in 2007 according to the UK Payments Administration.5 Some UK banks also offer users anti-virus software such as the Kaspersky Internet Security Suite to help stop viruses and Trojans.

However, anti-virus software and firewalls only go so far, most banks offer a free software solution known as ‘Rapport’ for safer online banking. Rapport is a software solution from Trusteer that secures communication from keyboard to website; many banks now offer this software for you to download as added protection against fraud whilst banking online. It detects and prevents Man-in-the-Browser, Man-in-the-middle, phishing and other attacks launched directly against the user. When users browse to sensitive websites such as online banking, the Rapport plug-in immediately locks down the browser and prevents any unauthorised access to web pages and sensitive information that flow through the browser. This browser lockdown is achieved through a combination of access control, encryption and verification technologies that take place in the background, completely transparent to the user. The purpose of the browser lockdown is to prevent malware known as Man-in-the-Browser from accessing the browser itself, as well as keystrokes typed into the browser, and communication that enters and leaves the browser. While the browser is locked down, malware cannot read the content of web pages or information entered into these websites. Malware cannot tamper with web pages or web communication. In addition to locking down the browser, Rapport also locks down communication with the website. It authenticates the website, and forces end-to-end secure communication with the website. This communication lockdown prevents both Man-in-the-middle and phishing attacks and prevents criminals from accessing sensitive web communication. Unauthorised attempts to access the browser or its communication are automatically reported to the Trusteer cloud-based fraud analysis service. The Trusteer team of fraud analysts works 24 × 7 analysing this information from customers all over the world to identify new attack patterns. Institutions registered for the Trusteer service receive immediate reports and actionable alerts of new attacks and can learn of attacks as they happen, instead of days, weeks and sometimes months later.6

Deceiving a user to steal their login information is the most common attack on users banking online. Two well-known examples of these attacks are phishing and pharming. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.7 What this means is, if you bank
Integrating geolocation into electronic finance applications

275

You could receive an e-mail claiming to be from your bank asking you to ‘update’ or ‘verify’ information regarding your account. You will then be asked to click on a link that will direct you to another website to do so, this will be a fake website set up by the fraudster, and any information entered on this site will be captured by the fraudster and, therefore, be manipulated by them (Petzold et al., 2006).

Banks will never contact a customer via e-mail to ask them to enter a password or any other sensitive information by clicking on a link and visiting a website. SPAM e-mails are sent out at random in the hope of reaching a live e-mail address of a customer with an account at the bank being targeted. Other approaches are:

- **Pharming** is a hacker’s attack aiming to redirect a website’s traffic to another, fake website. Pharming can be conducted either by changing the hosts file on a victim’s computer or by exploitation of a vulnerability in DNS server software.

- **Trojan Horses** are a type of computer virus that can be installed on your computer without you realising. Trojans can be capable of installing a ‘keylogger’ on your computer that captures all the keystrokes entered on your keyboard. The keylogger can then be used to capture passwords for certain websites. Trojans can even be used to take screen shots of websites you visit. This information is then sent to the fraudster over the internet. Like phishing, e-mails are sent out at random asking users to click on a link that will direct them to a fake/malicious website where vulnerabilities in the web browser are used to install the Trojan.

- **Money Mules**, most of these scams are conducted by fraudsters overseas, if a fraudster is successful in hacking your account, it is, however, impossible for the fraudster to make a cross-border transfer from your account to one overseas outside of the UK, this is where ‘Money Mules’ come in. Money Mules basically launder the funds obtained from Phishing and Trojan scams. They are recruited online by fraudsters and receive funds in their accounts; these funds are then withdrawn and sent overseas using a wire transfer service. The fraudster receives his money and the mule a commission for his or her services.

Table 1 shows that online banking fraud loses rose by 60% in 2010. The rise is mainly due to fraudsters employing more sophisticated methods and choosing to target customers of banks rather than the banks themselves, which are more difficult to attack. In general, it is very difficult for someone to gain access to your login details as long as you take the right precautions. Fraudsters mainly gain access to these details by tricking the user into providing them. If someone does gain access to your details, it is then easy for them to use them.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Financial fraud action UK bank Losses 2006–2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online bank fraud loses</td>
<td>£22.4 m</td>
</tr>
</tbody>
</table>

Countries or regions that are regarded as having high-risk online fraud include Africa, Amsterdam in Holland, Belgium, Bulgaria, China, Eastern Europe, Egypt, Ghana,
Malaysia, Russia, Malmö in Sweden, Nigeria, Pakistan, Palestine, Romania, Indonesia, Israel, Lithuania, Southwest Asia, Turkey, Ukraine and Yugoslavia.\textsuperscript{11}

Nigeria remains one of the largest fraud and scam operations centre in the world. New tactics by criminals in Nigeria are increasingly sophisticated, and victims range from individuals, to investors, to multi-national corporations. New system technology allows Nigerian criminals to hide their true location, masking their IP address and using non-Nigeria phone numbers and mailing addresses.

Cyber criminals have created sophisticated Trojan viruses that steal online banking log-in details from infected computers. The Clampi virus, which is spreading rapidly across hundreds of thousands of computers in UK and the USA, infects computers when users visit websites that host a malicious code. Once on the computer, the virus sits unnoticed until the user logs on to bank, credit card or other financial websites. It then captures log-in and password information and sends it to a server run by the attackers. They can then tell the compromised computer to send money to accounts that they control, or they can buy goods with the stolen credit card details. The Trojan has a list of more than 4500 finance-related websites that it monitors, including British high street banks. Security experts warned that it was one of the stealthiest and most pervasive threats to computers using the Microsoft Windows operating systems.\textsuperscript{12}

3 Geolocation

Geolocation is the identification of the real-world geographic location of an internet-connected computer, mobile device, website visitor or other. IP address geolocation data can include information such as country, region, city, postal/zip code, latitude, longitude and time zone (Lassabe, 2009). Geolocation may refer to the practice of assessing the location, to the actual assessed location or to the locational data.\textsuperscript{13}

Geolocation is increasingly being implemented to ensure web users around the world are successfully being navigated to content that has been localised for them. Due to the ‘.com’ dilemma, most companies are finding that more than half of the visitors to their global (.com) homepages are based outside of their home markets. The majority of these users do not find the country site that has been developed for them. Companies such as Amazon have introduced geolocation as a method of dealing with this problem (Brewster and Dunlop, 2002). Amazon uses geolocation to ensure that its customers shop from the most relevant websites. If for instance a UK user browses to amazon.com, they will be greeted with a country-specific homepage such as Figure 1.

Figure 1  Amazon application (see online version for colours)

Notice the ‘Shopping from the UK?’ banner, Amazon knows that the visitor is searching from a UK IP address and therefore directs them to the Amazon UK site. This is
beneficial to the user as the content of the US website (amazon.com) will vary to that of the UK site. Currency and region restrictions on DVDs and video games are examples of this.

The foundation for geolocation is the Internet Protocol (IP) address, a numeric string assigned to every device attached to the internet. When you surf the web, your computer sends out this IP address to every website you visit. IP addresses are not like mailing addresses. That is, most are not fixed to a specific geographic location. And knowing that a particular Internet Service Provider (ISP) is based in a particular city is no guarantee that you will know where its customers are located (Furey et al., 2008). That is where geolocation service providers come in. Geolocation service providers build massive databases that link each IP address to a specific location. Some geolocation databases are available for sale, and some can also be searched for free online. As the IP system is in a constant state of flux, many providers update their databases on a daily or weekly basis. Some geolocation vendors report a 510% change in IP addresses locations each week.

Geolocation can provide much more than a geographic location. Many geolocation providers supply up to 30 data fields for each IP address that can help to further determine if users really are where they say they are. These may include country, region, state, city, ZIP code, area code; latitude/longitude; time zone; network connection type and domain name and type (i.e., .com or .edu). Not every IP address accurately represents the location of the web user. For example, some multinational companies route internet traffic from their many international offices through a few IP addresses, which may create the impression that some Internet users are in, say, the UK when they are actually based in France. If someone is using a dial-up connection from Ireland back to their ISP provider in the France, it will appear like they are in the France. There are also proxy services that allow web users to cloak their identities online, a few geolocation providers, however, have introduced technology that can look past these proxy servers to access the user’s true location. In addition, some providers can now locate, down to a city-street level, people connecting to the Internet via mobile phones or public Wi-Fi networks. This is accomplished through cell tower and Wi-Fi access point triangulation (Curran and Furey, 2008).

4 Google gears

Gears is an open source set of java script API’s that can be added to a browser and called from web applications. Gears is cross platform and works on browsers such as Firefox, Safari, Internet Explorer in addition to a number of mobile devices. The overall aim of Gears is to make web applications just as powerful as desktop applications. The Geolocation API enables a web application to obtain a user’s geographical position. The Geolocation API enables a web application to retrieve a user’s current position, using the getCurrentPosition method. It allows you to watch the user’s position as it changes over time, using the watchPosition method and obtain the user’s last known position, using the lastPosition property. The Geolocation API provides the best estimate of the user’s position using a number of sources called location providers (Deak et al., 2011). For instance, each Wi-Fi access point and cell tower has a unique ID, this information along with GPS and IP addresses are sent to a location server and used to give the most accurate position possible. The information you receive back can include latitude/longitude, altitude, horizontal/vertical accuracy and time stamp (when the
The user’s position is then returned, in this example, city, region, country, latitude and longitude of the user’s location is returned. It is even possible to return accurate information such as the number/name of the street regarding the user’s position. This is possible through the getCurrentPosition method. The getCurrentPosition provides a previously cached position if available and repeatedly obtains a new position.

The Geolocation API is an abstraction for various location APIs that currently exist on mobile platforms (GPS-based, network/cell id-based). Geolocation implementations could be straightforward mappings to native APIs or have a more complex design that combines several location providers and returns the location from the most accurate provider at any given time. The Gears implementation chooses the location provider to invoke subject to the criteria specified with PositionOptions. When location data is requested, the first result that satisfies the criteria is returned via the PositionCallback function. Subsequent invocations will always use the most accurate location data available. This caters for the common case where a less accurate fix from a network-based location provider can be obtained quickly followed by a more accurate GPS fix later.

The Geolocation API can be used to retrieve the geographic location of a hosting device. In almost all cases, this information also discloses the location of the user of the device, thereby potentially compromising the user’s privacy. A conforming...
implementation of the API must, therefore, provide a mechanism that protects the user’s privacy and this mechanism should ensure that no location information is made available without the user’s express permission. User agents must not send location information to websites without the express permission of the user. User agents must acquire permission through a user interface, unless they have prearranged trust relationships with users, as described below. The user interface must include the URI of the document origin. Those permissions that are acquired through the user interface and that are preserved beyond the current browsing session must be revocable and user agents must respect revoked permissions. Some user agents will have prearranged trust relationships that do not require such user interfaces. For example, while a web browser will present a user interface when a website performs a geolocation request, a VOIP telephone may not present any user interface when using location information to perform an emergency 999 function.

Recipients must only request location information when necessary. Recipients must only use the location information for the task for which it was provided to them. Recipients must dispose of location information once that task is completed, unless expressly permitted to retain it by the user. Recipients must also take measures to protect this information against unauthorised access. If location information is stored, users should be allowed to update and delete this information. The recipient of location information must not retransmit the location information without the user’s express permission. Care should be taken when retransmitting and use of encryption is encouraged. Recipients must clearly and conspicuously disclose the fact that they are collecting location data, the purpose for the collection, how long the data is retained, how the data is secured, how the data is shared if it is shared, how users may access, update and delete the data and any other choices that users have with respect to the data.

Wi-Fi-based positioning means that you can deliver web applications for laptop users that are automatically customised to your user’s exact position. Lastminute.com has developed a ‘radar’ application using the Gears Geolocation API for viewing hotels a location automatically. ITN have also developed an application that allows users to view news stories local to their position graphically on a map, using the Geolocation API, plus if you have the Google Earth plug-in installed, the results are shown Google Earth. A service known as ‘Rummble’, a form of social networking application that allows its users to build up trust networks by creating and sending ‘Rumbles’ to one another also implements Gears and the Geolocation API by automatically centring its search of nearby Rumbles on the user’s position.

5 Geolocation prototype

The application will present the user with a login screen. Once the user enters and submits a username and password, Gears is initialised and checks the users system to see if Gears is present. If Gears is not present on the users system, the user is directed to an installation page where Gears can be downloaded and installed. Users will not be allowed to progress in the login process until Gears has been successfully installed on their system. When Gears is present on the users system the user will be prompted with a security warning, notifying the user that Gears is about to access information regarding the user’s location. For users to proceed, they will have to allow Gears to do so. User’s
who deny Gears of the permission to retrieve their location information will be notified that they cannot progress until Gears is granted such permission. When Gears is allowed to retrieve the user’s location, the Geolocation API is called and the user’s location retrieved. The location of the user is then compared against a database containing locations that have a history of online fraud, if the user’s location corresponds with one on the database then the user’s login details are not processed and the user is refused access to the account. A record of the attempted login is then generated and stored in a separate database. When and only when the location of the user is valid are the user’s login details processed. When the user’s login details are submitted they are verified and if correct then the user is granted access to the account, otherwise the user will be denied access. When a user loads the login page for the first time, a Gears security warning is displayed to the user (see Figure 3).

Figure 3  Gears security warning (see online version for colours)

This is important as disclosing information regarding a user’s location is potentially compromising the user’s privacy (Furey et al., 2010). The warning states that Gears is going to retrieve information regarding the user’s location. The user must allow Gears to retrieve such information. To do so the user must check the box and click on the ‘Allow’ button. The login page will then load. The user is only required to agree to this warning once. The next time the user loads the login page it will load without displaying the warning. If the user loads the login page again from another terminal, the warning will appear again on the first attempt.

Now that the user has agreed to share their location, the login page loads and an alert box appears stating the country that the user is trying to access the account from (see Figure 4). This is to illustrate that the application knows the location of the user. The user must click ‘OK’ to close the alert. If a user clicks ‘Deny’ on the security warning, the login page will still load but the user’s location will not be retrieved, in this event the user is not able to login into the account.

Now that the login page has been loaded and the users location retrieved, the user can now attempt to login to the account. To do so, the user must enter the username and password and click submit. When the user clicks submit, the user’s location is verified. If the user’s location is not valid, an error message is displayed. If the user is logging in from a valid location, the username and password are verified and access to the account is granted. If the username and password is incorrect, the user is asked to submit
them again. Accessing the site from a browser that does not have the Gears plug-in installed will result in the user being redirected to the Gears installation page. Once Gears is installed the login page will load. When a user accesses the login page, the application checks to see if the user has Gears installed on his or her browser. For the user’s location to be retrieved, Gears needs to be installed. If Gears is not installed, the user is redirected to the Gears installation page. The user can now click on the ‘Install Gears’ button to start the installation process. The user will then be prompted to agree to the terms of service and privacy policy. Once the user agrees the installation file can be downloaded. The user can then open the downloaded file and click ‘Run’, Gears will then be installed automatically. The user’s browser must then be restarted so that it can recognise Gears. The user will be prompted to do so. Once the browser has been restarted, the user is directed back to the login page and in another tab the Gears installation page where an installation confirmation message is shown. Now that Gears has been successfully installed in the user’s browser, the user can attempt to login to the system.

Figure 4 Login screen (see online version for colours)

To manipulate the Gears Geolocation API, the ‘gear_init.js’ needed to be downloaded from http://code.google.com/apis/gears/tools.html#gears_init. This file is needed to initialise the Gears library. The library is reference in the application code. Global variables defined include geo, which holds a reference to a newly created Geolocation object; locationFound which is set to true once a location is found; lat and lon hold latitude/longitude coordinates and addr holds a string of the country. When finding a location using Gears, two functions are needed. One that will be called if a location can be found; the other called if there was an error. The updatePosition function is called when a location is successfully found.

The lat and lon variables are set to the found latitude and longitude positions. The addr variable is then set using the country that was found. In a case that a country cannot be found it is first checked to see if it is null, locationFound is then set to true. Country value returned in the addr variable is used to prompt the user of his or her location. In the event that a user’s location could not be found, an error message is shown.

The getCurrentPosition function is called to actually find the users location. The updatePosition and handleError functions are supplied as callbacks. The third parameter in the getCurrentPosition function is a PositionOptions object. Here, a high accuracy request (enableHighAccuracy: true) has been made and requested that the country be
found (gearsRequestAddress: true) supplies the information required to populate the addr variable.

Figure 5 depicts the checkCountry() function. The user’s location is validated using this function. The addr variable is compared against three other countries. These countries were outlined earlier in the report as countries with a high online fraud rate and therefore used in my application. If a user from any of these countries tries to login to the account, the access is denied. Any other country is granted access. In the event that the user’s location is not retrieved, the user is denied access. This is done by checking to see if the addr variable is null.

```javascript
function checkCountry()
{
    if (addr == "Russia")
    {
        alert('Access to this account is not permitted from: ' + addr);
        invalid();
    }
    else if (addr == "Nigeria")
    {
        alert('Access to this account is not permitted from: ' + addr);
        invalid();
    }
    else if (addr == "China")
    {
        alert('Access to this account is not permitted from: ' + addr);
        invalid();
    }
    else if (addr == null)
    {
        alert('ACCESS DENIED!');
        invalid();
    }
    else
    {
        validate(loginForm.text2.value, "name", loginForm.text1.value, "pass");
    }
}
```

If each comparison is proved false then the validate function is called. This is to ensure that the user’s login details are not processed until the location has been verified. The username is set to ‘name’ and the password set to ‘pass’. These values are then checked using the validate function.

To test if the real-world location of a user can be identified, the retrieve location component was invoked using the getCurrentPosition and updatePosition functions and a marker displaying the location on the map was the result. The country stored within the ‘addr’ variable was displayed with the latitude and longitude coordinates of the location in an info bubble to illustrate the accuracy of the information retrieved (Figure 6).

As the latitude and longitude coordinates are retrieved by the Geolocation API, the exact location can be pinpointed on the map. The country is displayed to illustrate that it can be used to check a location against another; this will become apparent in the integration testing. Testing the retrieve location component of the application demonstrated that the real world location of a user can be identified using Gears. By using a map to display the location retrieved by Gears, you are able to see the accuracy of the location retrieved. As the latitude and longitude of a user’s location is retrieved, it is possible to retrieve the user’s exact address if required. However, a country is of a larger scale and even if a user’s exact location is not retrieved, it is more than likely the country will be and therefore more practical to validate a country.
The application could be used to check a location based on a certain region within a country if necessary.

**Figure 6** Retrieve location test (see online version for colours)

---

### 6 Conclusion

To demonstrate how Gears could be integrated into an online banking account and used as a form of added security, a simple yet functional login screen was designed and implemented. The application was developed to block locations with high levels of online fraud (Yogarajah et al., 2011). This was to demonstrate how access to such accounts could be blocked even with the correct account details. Many accounts are hacked by fraudsters abroad by obtaining account details. This therefore demonstrated that these details could become meaningless to the fraudster as even though they are correct, access would not be granted due to their location. Geolocation can be a powerful tool and when implemented as a form of security, many web applications can benefit. With mobile devices becoming more sophisticated and used to carry out tasks that would normally have been done on a desktop such as banking, then Geolocation can only help improve how securely they work.

However, there are some limitations concerning Gears. For instance, if this application was to be integrated in online accounts, Gears would need to be installed in each customer’s browser therefore each user would be forced to go through the install process each time they access their account from a different computer. The install process can become tiresome as the user is also receiving prompts and having to restart their browser each time they are required to install the plug-in.

With the introduction of HTML5 however, Gears can be implemented as well as other browser plug-ins without the need to install. HTML5 is the proposed next standard for HTML 4.01, XHTML 1.0 and DOM Level 2 HTML. The aim is to reduce the number of plug-ins needed to be installed by users such as Gears. HTML5, therefore, comes with Gears pre-installed across all browsers and its functions called without having to go through the install process each time. This would prove to be of great advantage when implementing an application like the one developed throughout here. With Gears available in all major browsers due to HTML5, web developers can implement Gears as a form of security for free and for a variety of applications and reasons.
References


Websites

1 http://securitywatch.eweek.com/phishing_and_fraud/online_banking_users_still_hooked_on_phishing.html
4 http://en.wikipedia.org/wiki/Online_banking
5 http://www.which.co.uk/news/2009/08/online-banking-security-risks-revealed-183544.jsp
6 http://www.trusteer.com/product-0
7 http://en.wikipedia.org/wiki/Phishing
8 http://en.wikipedia.org/wiki/Pharming
9 http://www.banksafeonline.org.uk/trojans_explained.html
Integrating geolocation into electronic finance applications

10http://www.banksafeonline.org.uk/
11http://www.onlinefraudguide.com/risk-countries-fraud/
12http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article6841779.ece
14http://code.google.com/apis/gears/api_geolocation.html
15http://code.google.com/apis/gears/geolocation_network_protocol.html