NetSecure:
A context aware based online security framework

Conrad Deighan, Kevin Curran, Tom Lunney and Paul Mc Kevitt

School of Computing and Intelligent Systems
Faculty of Computing and Engineering University of Ulster, Magee
BT48 7JL, Derry/Londonderry, Northern Ireland
Email: deighan-c1@email.ulster.ac.uk

Abstract- **Location and Context Aware Computing are playing an important role within the field of networks and telecommunications. Consequently, the ability to determine the exact location of a device on the Internet can not only optimise the shipment of data from end-to-end, but additionally lead to innovative location based services. Such services include increased security of online banking application, e-commerce applications, and the ability to deny user access to a network infrastructure from predefined locations. At present, the majority of such systems do not have adequate security mechanisms in place to deal with malicious/potential attacks on data and fraud. In addition, the ability to perform such attacks has increased with the rapid growth of the network and telecommunications technology, as users can perform such actions from the comfort of their own home. This work proposes the use of a location determination system, such as GPS and context data from Personal Area Networks (PAN) to build a 'profile' of incoming requests to an online service. The NetSecure framework will provide a programming API to enable it to be accessed by any Internet applications requiring enhanced security. The adaption of location-awareness and the ability to 'profile' people and environments via PAN's will enhance the security aspects of applications through the added location awareness capability.**

Keywords: Location Aware Computing (LAC), Context Aware Computing (CAC), Location-aware security, internet application security, location determination, smart places, smart environments, Personal Area Network (PAN). NetSecure

I. INTRODUCTION

The advent of the Internet has not only facilitated millions of people to communicate freely over the past thirty years but additionally has opened up the potential for online applications such as Internet Banking and e-Commerce. However, it is not just major retail chains or supermarkets that can participate in online commerce. Any person with a computer and an Internet connection can provide such a service. These new opportunities present a set of associated problems such as, security, client-vendor trust and privacy. This is one of the main reasons why consumers are skeptical in regards to online transactions [1]. Many online vendors are only concerned with the security of a transaction and therefore rely solely on secure transactions protocols, namely SSL (Secure Socket Layer) and TLS (Transport Layer Security). This being said, many online applications do not have appropriate security mechanisms put into practice [2], as the majority of vendors ignore client-server security.

With no clear disconnection between location and user identity on the Internet [3] an Internet Protocol (IP) address and login credentials cannot be used solely to authenticate a user to a secure online environment. This is why the significance of context-aware computing (CAC) services has grown rapidly throughout the last decade as it enables developers to offer more 'aware' applications. The main objective of CAC services is to provide applications with contextual information such as, user activity, location, target machine credentials, time, landmarks or weather conditions [4]. However, the most important factor that can be extracted from this is location [5]. Furthermore, if some aspects of context, e.g., location, environment, time, user activity or unique device data can be integrated into Internet applications it can provide a more secure and intelligent environment.

The aim of this research is the integration of geographically accurate location information from both an indoor and outdoor positioning system in conjunction with unique personal data from personal mobile devices, cell phones, Bluetooth devices or PC's. For example, the Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, local time and cell phone number from the named devices could be potentially utilised. Therefore, based on predefined rules, different levels of access will be granted to a user based on the profile information retrieved from the current context. The GPS data could be utilised to ascertain accurate estimates of router location, resulting in the application 'knowing' the source of the request and the ability to compare the location of the router and PAN devices. Furthermore, unique data from the user's context could be extracted to further the authentication process.

ISBN: 978-1-902560-22-9

The objectives of this research are as follows:

- Determine router location from GPS enabled devices.
- Profile person and environment by utilising context from Personal Area Networks.
- Develop a framework to enable further development of secure online applications.
- Intelligently access risk from incoming requests.
- Determine personal access rights based on risk assessment.
- Deploy the NetSecure application in different benchmarking scenarios.

II. RELATED WORK

If an application can become context-aware, in particular, location-aware, then developers can offer more powerful and dynamic applications to the end user. Some of these functionalities are: selecting the appropriate language to display the content of a web page, restricting users from non pre-set locations from accessing secure services such as Internet Banking Systems, and in peer-peer networks unnecessary high latency hops can be avoided. This can subsequently optimise security, privacy and routing efficiency [6]. Sripanidkulchai [7], review multimedia delivery systems such as Content Distribution Networks (CDNs) and state that they benefit vastly from an understanding the location of their clients. Such benefits include the identification of servers that are in proximity and the dynamic adaption of multimedia content based on the clients location.

Vendors of Internet applications such as online banking and e-commerce should use effective and proven mechanisms for the successful authentication to their services. The authentication mechanisms implemented within the online applications must be appropriate to the risk coupled with the services which are being offered. There are various types of risks associated with online banking and e-commerce such as, identity theft, account fraud and money laundering. This is often as a result of a single-factor authentication process, e.g., user name and password. Risk assessments signify that the sole use of a single-factor authentication is insufficient for unrestricted access to an online financial or retail service. This is where vendors should merge multi-factor authentication into their applications, such as multiple uses of, user name, passwords, personal identification numbers (PIN), one-time passwords (OTP) and/or digital certificates [8]. Correctly designed and implemented multi-factor authentication process has proven to be a more reliable fraud deterrent [8]. A successful authentication process is not only depended upon the technology employed, but additionally is depended upon various factors such as customer approval, reliability, policies, scalability and interoperability.

A. Security of Internet applications

The Secure Socket Layer (SSL) protocol, one of the most widely known and used protocols [16] was implemented to protect the shipment of data from end-to-end. SSL incorporates all network services that utilise TCP/IP which supports the communication and secure delivery between the client-server paradigm. Netscape, the original developers of the SSL protocol put this protocol into practice to ensure data was routed securely through HTTP, LDAP, IMAP4 and POP3 application layers. SSL can be used for the secure transmission of any related networks service. However it is mostly used in HTTP client-server applications. A wide range of HTTP servers support SSL sessions and additionally Microsoft and Netscape provide integrated SSL software for their browsers [17]. The Transport Layer Security (TLS) protocol, seen as an enhancement to its predecessor SSL [9] is used for the secure and reliable delivery of data within TCP/IP networks, for example, the Internet. TLS ensures that the privacy of information when applications communicate over the Internet. Whenever the client-server has an established connection, the TLS protocol ensures that there is no 'sniffing' or tampering with packets when they are in transit. The TLS protocol comprises two different layers, the record protocol and the handshake protocol. The record protocol facilitates a secure connection together with encryption method such as Data Encryption Standard (DES). Additionally, the handshake protocol enables the client-server to authenticate and decide which encryption algorithm and cryptography keys are used before the exchange of data [9].

B. Geo-Location Awareness

The integration of geographical awareness mechanisms with such location based services (LBS) and applications have various advantages over non-geographical aware LBS and applications. Such advantages include: increased security for online applications and network infrastructures, the ability to deny access to systems from predefined locations and IP addresses associated with known fraudulent transactions, and additionally, the mechanisms to optimise IP routing and the shipment of data from end-to-end. Consequently, developers have seen the potential for the integration of geographical information to such applications and services. Companies such as Quova [10] and NASDAQ [11] have introduced geographical data to their applications where security of data is critical.

C. Positioning Systems

Since the arrival of GPS, developers have used it extensively by incorporating its functionality into various applications such as tracking, navigation, logistics, GeoTagging and current location information. This global

navigation satellite system (GNSS) is one of the most common methods for locating a device provided that a GPS receiver is being utilised to capture and calculate location. On average, GPS receivers are capable of pinpointing their current location 95% of the time within 10 meters of a known location. However, they can often offer even greater accuracy, but in some scenarios offer much less [12]. Unlike some positioning systems, the data can be captured and utilized by any person with the technology to-do so. Although GPS seems to have great advantages and even greater accuracy, satellite signals can be easily blocked by buildings.

The accuracy of a mobile station's location is the key requirement for the effective delivery of location based services over mobile networks. Consequently, the development of such cellular positioning methodologies has been a significant research focus with various localisation algorithms being proposed. Some of the technologies that can be used are, CellID, Time of Arrival (TOA), Angle of Arrival (AOA), Time Difference of Arrival (TDOA), Observed Time Difference (E-OTD), Timing Advance (TA), triangulation and fingerprinting [18]. The GSM cellular network is divided into cells that overlap to enable seamless hand-over techniques when roaming from one mobile station to the other.

RADAR was the first Wi-Fi signal-strength positioning system intended for indoor use. By exploiting radio frequency (RF) fingerprinting and profiling of the environment, e.g., W-LAN hardware, location of user and machines can be determined inside buildings. Thus, facilitating an indoor location determination system. Tthis provides location-awareness for both applications and services. Bahl and Padmanabhan [13] describe RADAR as "Indoor-GPS".

The Ekahau Real Time Location System (RTLS) is a pure software solution for real-time tracking dependent upon already deployed Wi-Fi network infrastructures. Two-way Wi-Fi tags are used to obtain the full accuracy and functionality potential that Ekahau offers. However, accuracy is depended upon some additional factors as Ekahau interoperates over existing Wi-Fi infrastructures. A graphical user interface (GUI) is integrated into the software with the intention that full visibility is offered across geographically-dispersed areas. As a result there is no requirement for hardware or software to be installed at remote locations.

D. Personal Area Networks (PAN)

A Personal Area Network (PAN) is a type of computer network that has the ability to communicate between various devices, such as cell phones, Bluetooth devices and PDA's that are in proximity to one person [14]. However, a device within one person's PAN has the possibility of belonging to another person. Depending on the technologies employed to contribute to the PAN's infrastructure their coverage can range from a few meters, to at best, a few hundred meters. Interpersonal communication can take place between connected PAN devices and at higher network levels such as Local Area Network (LAN) or the Internet. PAN's are normally hardwired connections, although when the IEEE 802.15 standard was released this opened the potential for Wireless Personal Area Networks (WPAN). Wireless enabled Bluetooth devices are capable of creating WPAN which are sometimes referred to as piconets [19]. Bluetooth is digital communication technology with a short wireless range, ideal for sending and receiving data between mobile phones, computer to mouse, keyboard and printer. The main principle behind this would be to remove unnecessary wires. Internet access is possible when making use of the WPAN as the capability of expansion is possible to include AP's [15]. In addition, WPAN can consist of various other technologies such as Infra-Red (IrDA) and radio frequency connections such as Ultra-Wideband (UWB) and Z-Wave.

Bluetooth WPAN's can normally be composed of a maximum of eight simultaneous devices in a master-slave setup where the first device is usually the master. These interconnected devices are unique within a person's personal workspace. Consequently when the WPAN is active, data can be extracted to build a unique context profile of a person and their environment. When a person is attempting to logon to a secure environment, the use of a multi-factor authentication gives added security to the system [8]. As an alternative to solely using user names and passwords, the archived context data could be used to aid in the secure authentication of a person. The context profile is forwarded to the master device, which would then be uplinked to the server where the person is attempting to connect. However, if the master device does not have sufficient Internet access, the use of an Ambient Network would be required to intelligently change network types.

III. DESIGN OF NETSECURE

The previous section has reviewed a wide range of various protocols, methods and mechanisms that have the potential to enhance security aspects of Internet applications. However, none of them offer a complete solution to what is deemed a secure online environment for both, client and vendor. It has become apparent that the security of online applications is not as secure as one would like them to be. This being said, developers cannot rely on 20th century technologies in the 21st century, e.g., single factor logins, user names and passwords. This section will discuss various aspects of NetSecure together with the potential tools that will be employed to formulate the new framework. The NetSecure framework will comprise of several integrated technologies together to enable the development process to take place. Additionally, this section provides an overview of the proposed solution together with the technical

documentation required in order to develop the NetSecure framework. As previously stated, NetSecure will comprise several different technologies in order to develop a complete location aware security framework for online applications. These include geographically aware routers, Personal Area Networks (PAN's) and a web server.

To enable routers to become geographically aware, they will be updated in the bootstrap phase by GPS devices in proximity. The router would sequentially search for these devices and probe the GPS coordinates from each device. Furthermore, these coordinates will then be used to determine the location of the router, which will then be stored within the routing table. Figure 1, shows how the above information is extracted and the routing table is updated.

Figure 1: GPS Devices updating Router

The PAN setup will vary from person-to person. However, the most common devices will be Bluetooth enabled laptops and persons computers, cellular telephones, and personal digital assistants (PDA's). The web server will be used to host the applications developed by utilizing NetSecure. Each potential developer will have different needs in terms of security, incoming countries to be scrutinised in greater detail, and devices of the PAN that need to be probed. Additionally, testing of the proposed NetSecure framework will consist of developing an online banking application. Figure 2 shows the online banking systems application infrastructure.

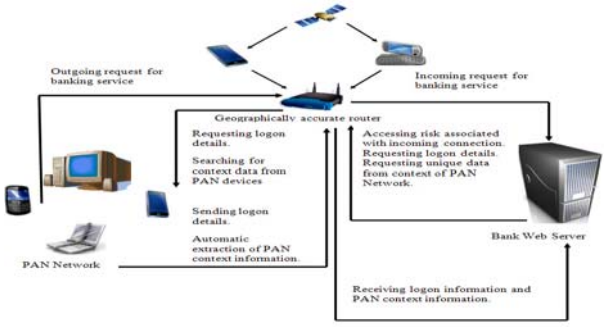

Figure 2: NetSecure applied to online banking

Upon receiving the user's logon credentials, the web application will automatically seek for a connected PAN to confirm if the user is actually who they say they are. The system will attempt to extract unique data such as the MAC address of each device, IMEI numbers of the cell phone and PDA, GPS coordinates of GPS enabled devices, and the current time of day from each device. Together, this data can be exploited to subsequently determine the identity of the user. Figure 3 shows how the NetSecure banking application determines which access level a user will be granted, which is intelligently coordinated across the banking application.

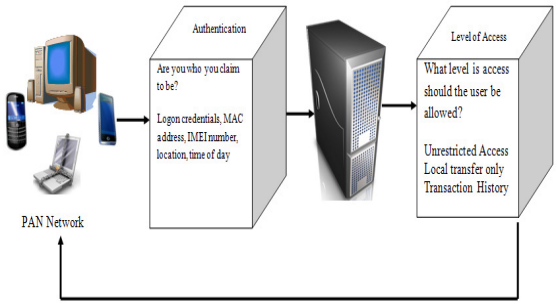

Figure 3: Determining access level

NetSecure will be developed by utilising a range of tools both hardware and software. In order to ascertain router location, a C++ network level program will be developed to extract GPS coordinates from GPS enabled mobile devices in proximity to the router. Additionally, the main application will be developed with Microsoft Visual Studio, which includes several programming languages and database technology.

IV. CONCLUSION

This research focuses on the development of more secure and intelligent online systems where user data and privacy are key. We have reviewed several technologies that enhance security aspects of Internet applications, and various location determination systems that could play a key role for enhancing security aspects. However, none of them offer a complete location aware security solution, sufficient to deter fraudulent and malicious attacks on confidential data. In addition to location playing a key role for enhanced security, context aware computing has opened up new boundaries for computing applications as it can take advantage of the local environment to uniquely identify people and places. The proposed frameworks overall aim is to incorporate such unique data from Personal Area Networks to improve security aspects of online systems.

V. REFERENCES

[1] Foresight., (1998). E-commerce sets new rules, Systems Relationships. Marketing, on behalf of Datatec Ltd, 1998 November;1(3).

[2] Junnarkar., S. (2002). http://news.zdnet.co.uk/internet/0,1000000097,2109660,00.htm

[3] Kumar, S., (2006) Geographic addressing in WANs to simplify routing and enable new services http://www.arl.wustl.edu/~jst/reInventTheNet/?p=154.

[4] Chen, G., and Kotz, D. (2000). A survey of context-aware mobile computing research. Technical Report TR2000- 381, Dept. of Computer Science, Dartmouth College.

[5] Araujo, F., and Rodrigues, L. (2004) GeoPeer: A Location-Aware Peer-to-Peer. Network Computing and Applications (NCA). Proceedings Third IEEE International Symposium Page(s):39 – 46.

[6] Ratnasamy, S., Handley, M., Karp, R., Shenker, S. (2002): Topologically-aware overlay construction and serverselection. In: Proc. of the IEEE INFOCOM'2002, New York, NY, USA.

[7] Sripanidkulchai, K., Maggs, B., and Zhang, H. (2003): Efficient content location using interest based locality in peer-to-peer systems. In: Proc. of the IEEE INFOCOM'2003, San Francisco, CA, USA.

[8] FFIEC 2001 - Federal Financial Institutions Examination Council - 3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov Authentication in an Internet Banking Environment.

[9] TechNet – (2003) – What is TLS/SSL - http://technet.microsoft.com/en-us/library/cc784450.aspx.

[10] Quova :- http://www.quova.com/.

[11] NASDAQ:- http://findarticles.com/p/articles/mi_pwwi/is_200806/ai_n25480305/.

[12] Hulbert, I. A. R. & French, J. (2001) 'The accuracy of GPS for wildlife telemetry and habitat mapping', Journal of Applied Ecology, vol. 38, pp. 869-878.

[13] Bahl., P and Padmanabhan., V. (2000) RADAR: An in-building RF-based user location and tracking system. Proc. of IEEE INFOCOM, Tel-Aviv, Israel.

[14] D.M. Bakker and Diane McMichael Gilster, Ron Gilster, series editor, Bluetooth End to End, Hungry Minds, Inc. New York, 2002.

[15] Bluetooth Performance Analysis in Personal Area Network (PAN)Rozeha A. Rashid and Rohaiza Yusof Department of Telematic and Optic, Faculty of Electrical Engineering, University of TechnologyMalaysia, 81310 UTM Skudai, Johor, MALAYSIA.

[16] Maj, A., (2005) - http://www.securityfocus.com/infocus/1818.

[17] TechNet., (2003) SSL/TLS in details - http://technet.microsoft.com/en-us/library/cc785811.aspx.

[18] Lakmali, B., and Dias, D.. (2009) Database Correlation for GSM Location in Outdoor & Indoor Environments. Dialog-University of Moratuwa Mobile Communications Research Laboratory, University of Moratuwa, Moratuwa, 10400, Sri Lanka.

[19] Belqasmi, F., Glitho, R., Dssouli, R., Network, IEEE Volume 22, Issue 4, July-Aug. 2008 Page(s):6 - 12 Digital Object NetSecure.