Web 2.0 Mashup Spatial Web Service Architecture Agile Modeled Privacy Design – Case Study Evaluations and Validations extended to Cloud Big Data and IOT

Dr.D.Shravani
Rayalaseema University, Kurnool, A.P, India

Abstract
This research paper deals with Web 2.0 Mashup Spatial Web Service Architecture Agile Modeled Privacy Design with case studies evaluations and validations extended to Cloud Big Data and IOT..

Keywords - *Security Engineering, Security Architectures, Web Services, Cloud Computing, Big Data, IOT*

I. INTRODUCTION

In this paper, a methodology on a case study of Web 2.0 Mashup Spatial Web Services Applications, case study is carried out using Agilr Modeled Web 2.0 Services Security for Privacy Management.

A. Web 2.0 Mashup Security

Mashup is an application that combines data or services from multiple web sites into one user experiences. A lot of great functionality in mashups comes from using tools from multiple sources. The problem is that when the website creator embeds code written by a third party on his site, the same –origin policy no longer offers any protection, and the embedded code likely has access to information stored on the creator’s site. Web 2.0 technologies are being used as a tool for cybercrimes. With web 2.0, following Attack trends came into scenario:

- Web site vulnerabilities open the door to compromise.
- Threats spread far and wide among the most popular websites.
- Popular social networking sites became hot targets.
- Web advertising is a vehicle for delivering malware.
- Insecure web 2.0 widgets and gadgets are on the rise and being exploited.
- Malware hide under the legitimate web 2.0 applications
- Spam replacing text content with URLs.
- The URLs becoming more varied phishing sites are increasingly dynamic.
- Botnets and spam are interdependent and this co-perpetuating relationship between botnets and spam is a notable trend.
- Spammers adopting more targeted and more aggressive attack tactics like highly targeted spam using social engineering as a vehicle for targeted spam, spam attacks on antispam infrastructure etc.

B. Introduction to Spatial Web Services

A lot of research has been developed for integrating the analysis functionality that is available in both analytic and geographic processing systems [Alastair Airchison]. The main goal is to provide users with a system capable of processing both geographic and multidimensional data by abstracting the complexity of separately querying and analyzing these data in a decision making process. However, this integration may not be fully achieved yet or may be built by using proprietary technologies. A service integration model had been already built, for supporting and/or geographic requests over the web. This model had been implemented by a Web Service, named GMLA WS, which is strongly based on standardized technologies such as Web Services, Java and XML. The GMLA WS query results are displayed in a Web browser as maps and/or tables for helping users in their decision making.

1) GEO_RBAC for Spatial Web Services

The widespread deployment of location based services and mobile applications as well as the increased concern for the management and sharing of geographical information in strategic applications like environmental protection and homeland security, have resulted in a strong demand for spatially aware access control systems [Jim Gray]. These application domains impose interesting requirements on access control systems. In particular, the permissions assigned to users depend on their position in a reference space; users often belong to well-defined categories; objects to which permissions must be granted are located in that space; and access control policies must grant permissions based on object locations and user positions.

As an example, consider a mobile application for the personnel and patients of a health care organization. Individuals are given a location-aware terminal with which they can request information services provided by an application server. The organization consists of individuals who have different functional roles, e.g. Nurse, doctor and patient. We note that, depending on the organizational context, the services available to users may differ based on the functional roles of users. For example, the services available to nurses may be different from those available to doctors, not simply because of the individual preferences, but mainly because of organizational and functional reasons. Further, the availability of the services may depend on the position of the requester. For example, a nurse may be allowed to request the record of a patient only when the patient is located in the department to which she has been assigned [Michael S Kirkpatrick].

To deal with the requirements listed above, an access control model with spatial capabilities is needed. Since in location-aware applications users are often grouped in distinct categories, such as nurse and doctor, RBAC represents a reasonable choice for the underlying access control framework. However, conventional RBAC does not suffice to support such applications, and needs to be extended with suitable location constraints, that is, expressed as coordinates in the reference space, or logical, that is, expressed in terms of spatial objects (such as the city of Milan or the West Valley Hospital) that have a semantics relevant to the specific application domains. When dealing with location-based applications, it is also important to take into account relevant standards for the representation of spatial objects; one such standard is by the OGC.

GEO_RBAC is a recently developed model that directly supports such location constrains. It is based on the notion of a spatial role that is a geographically bounded organizational function. The boundary of a role is defined as a geographical feature, such as a road, a city, or a hospital, and specifies the spatial range in which the user has to be located in order to use the role. Besides being assigned a physical position, obtained from a given mobile terminal such as a GPS based vehicle tracking device or a cellular phone, users are also assigned a logical and device independent position, representing the feature in which the user is located. Logical positions can be computed from real positions by using specific mapping functions, and can be represented at different granularities depending on the spatial role played by the user. If the user is located inside the spatial boundary of the role that has specify the type of spatial boundary of the role and granularity of the logical position, GEO RBAC has introduced the concept of spatial role schema. Spatial roles are thus specified as instances of role schemas.

Like RBAC, GEO-RBAC encompasses a family of models:

- Core GEO-RBAC includes the basic concepts of the model, and thus the notions of spatial role, role schema, real or logical position, and activated or enabled role.
- Hierarchical GEO-RBAC extends the conventional hierarchical RBAC by introducing two distinct hierarchies, one over role schemas and one over role instances.
- Constrained GEO-RBAC supports the specification of separation of duty (SoD) constraints for spatial roles and role schemas. Since exclusive role constraints are important to support the definition and maintenance of access control policies in mobile contexts, SoD constraints are extended to account for different granularities, dimensions and verification times (static, dynamic activation, dynamic at enabling). The resulting set of constrains developed for GEO-RBAC represents the first comprehensive class of constraints for spatially aware applications.

2) *Problems with Location-Based Mobile Applications*

Integrating location information into an application may possibly be the most exiting possibility for mobile applications [Michael Juntao Yuan]. Location information offers a whole new realm of applications. The biggest single problem with location information is not in the technology, but in the use of it: privacy. Whereas knowing the location of the mobile user can be very handy in offering very useful services, it can also violate basic privacy rights of a user. So, the users are often faced with a choice whether to “opt-in” or “opt-out”; participating in the program means signing a form that basically gives up a great deal of privacy, but not signing results in a lack of access to the desired services. Currently, there are no technologies that allow for “opting-in” or “opting-out” of sharing ones location on a granular interactive basis. In other words, there is no easy way for the user to specify when, where and how his or her location should be known and when, where and how his or her location should not be known. The second and third biggest problems with today’s location systems are price and power use. Good GPS-based systems are still fairly expensive and if we want to add GIS information to that to get value-added services such as finding restaurants etc. we are looking at subscription fees. Also, most location devices are considerable drain on the batteries, though this is an area of focus in the location industry and should be addressed with in the near future.

3) *Security and Privacy of Mobile Location Information:*

Security and Privacy are of utmost importance to location-based services. Without providing proper security and privacy, few users are willing to use a system that can reveal their current location or history of locations to third parties. Examples of problems that may arise if proper security is not implemented for location services are unwanted marketing, invasion of privacy by governmental or commercial entities, and identity theft or other criminal activities [Patrick Stuedi]. There are several aspects to security and privacy of location information, the most important are the following:

1. Access Security: There must be a proper authentication and authorization mechanism in place for those systems that access the location of a given device. Any systems that can obtain location information must in turn provide secure access to any related data through proper authentication and authorization.
2. Data Security: Any system used to cross-reference any information that identifies the user associated with a device through profiles; billing etc. must be completely secured. The content that specifies the location of the device must be transmitted through a secure mechanism (e.g. encryption)
3. User Control: The user must have control in specifying whether the location of his or her device is shared with any secondary systems within or outside of the primary wireless network.

Some of the key features of a system that offers location-based service and the clients to such a system must be the following:

1. The system must allow the users to configure policies regarding where and when their location information may be obtained and/or shared.
2. The system must allow the users to specify with whom their location information may be shared.
3. The system must automatically remove all historical data about a user's location unless otherwise allowed by the user.
4. The location-based service must not expose specific information to its client systems on why the location of a particular user may not be available. For example, the client system must not be able to request whether the user has specified to be unavailable to that particular client or during a particular time window.
5. The error margin in the exact location of the user must not be provided unless specified by the user.
6. The client system must specify a reason for which the location is obtained. Only trusted systems should be able to obtain location information.

4) *Mobile XML and Web Services*

XML (eXtensible Markup Language) has already become the de facto standard for exchange of human-readable data. Whether such will be the case for machine-to-machine communication is questionable; nevertheless, such applications exist and their popularity is increasing. A variety of XML-based technologies for Mobile applications have been evolved. RDF (Resource Description Framework), a part of the Semantic Web that is becoming pervasively more crucial to mobile applications. CC/PP Composite Capabilities / Preference Profiles and UAProf (User Agent Profile) are applications of RDF and XML for mobile applications, and even XML can be mapped to UML. (Unified Modeling Language) at the architectural level. The significance of XML to mobile applications is twofold. First, it offers well-formed and deterministically modifiable format for human-readable data, and second, it offers interoperability. Building mobile applications now always uses XML as one of the core pieces in their infrastructure.

5) *Cell Phone Security*

One of the most widely deployed cellular networks is the Global System for Mobile Communications (GSM). The designers of GSM or 2G (second-generation cellular networks) had several goals in mind. Better quality for voice, higher speeds for data, and other non-voice application and international roaming were some of the goals. From a security viewpoint, it was also designed to protect against charge fraud and eavesdropping.

The successor to GSM is Universal Mobile Telecommunications Systems (UMTS) or simple 3G. It promised advanced services such as Mobile Internet, multimedia messaging, videoconferencing, etc. UMTS standards were defined by an international consortium/standardization organization called 3GPP (Third generation Partnership Research implementation). The security provided in GSM is a quantum leap over that provided in first generation cellular networks. Still, there are several lacunae in 2G that have been plugged in 3G networks.

C. *Implementations and Validations.*

1) *Case 1. Safe Passwords in mobile phone*

Safe passwords in mobile phone: These days, anyone who is on the web needs too many passwords, and it's impossible to remember them all. Generally if we have too many passwords to remember we will be writing them all down on a piece of research implementation and hide it somewhere. We designed password safe application as another solution. It's a small program that encrypts all of your passwords using one paraphrase. The program is very easy to use, and isn't bogged down by unnecessary features. This application provides security through simplicity.

This is an end–user java application that stores sensitive information like passwords on mobile phones with strong encryption. This uses SHA encryption technique to secure the information. The application requires Java Micro Edition (J2ME) with MIDP-1.0, which is available on most current phones.

Modules involved: Security Module, Password Storage Module, and Password Retrieval Module.

a) *Security Module:* In this module we use the SHA algorithm to encrypt and decrypt the password which is required to enter into the application.
b) *Password Storage Module:* In this module the user can store his passwords into the application.
c) *Password Retrieval Module:* In this module user can view his passwords by login in to the application. The

Figure 6.1 consists of sequence diagram of the safe passwords in mobile phone application.
The Figure 6.2. consists of the class diagram of the safe passwords in mobile phone application

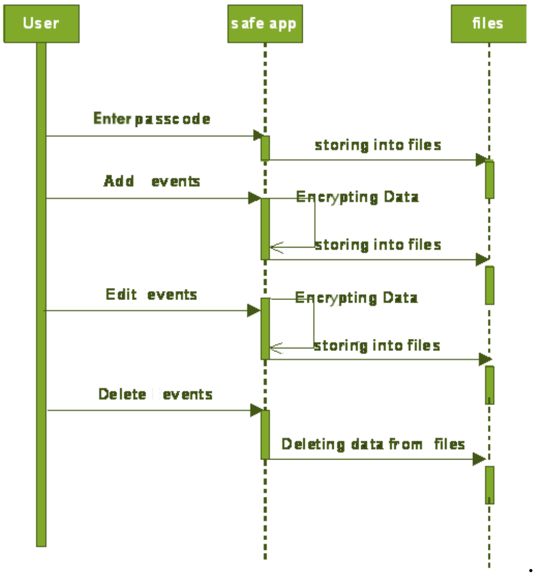


Figure 6.1. Sequence Diagram of the Safe Passwords In Mobile Phone

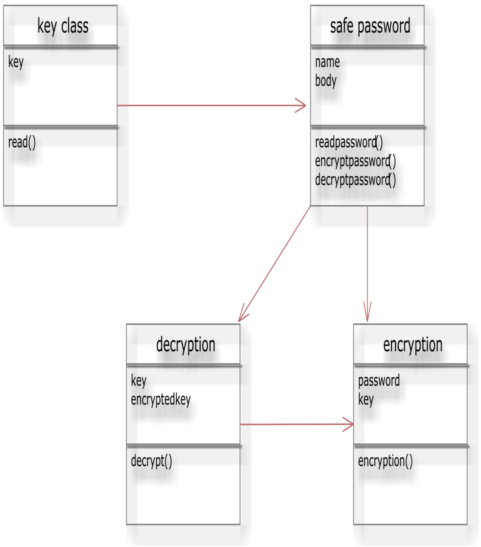
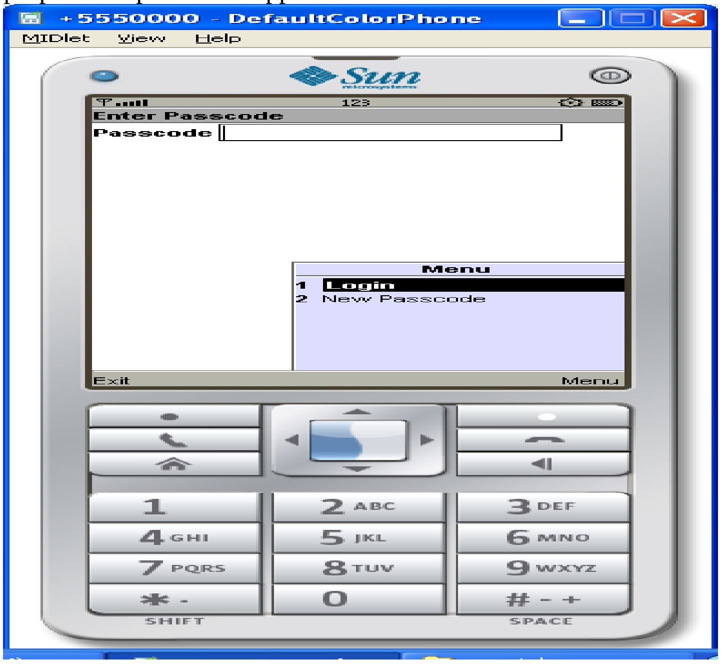


Figure 6.2 Class Diagram of the Safe Passwords in Mobile Phone

Figure 6.3 consists of the execution screen shot of the proposed implemented application



Enter Passcode

Passcode

Figure 6.3 Execution Screen Shot of the Mobile Phone Application

2) ***Case 2 Spatial Mobile Privacy Web Service Application***

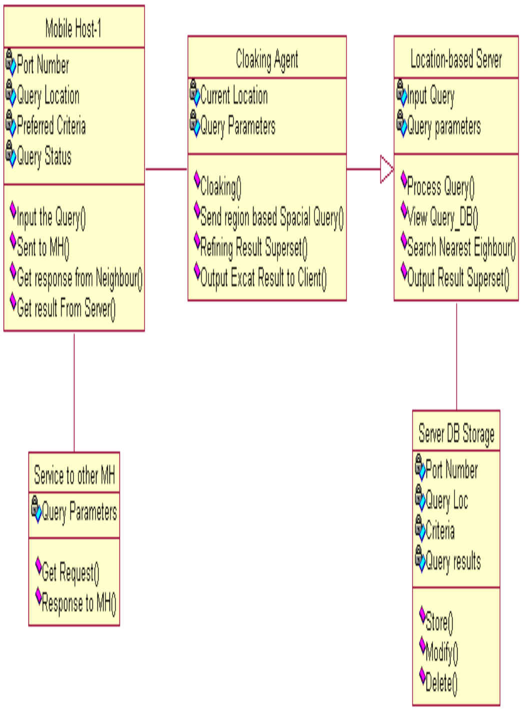
This case study discusses about privacy issues and implementations of Spatial Web Services Security Architectures. Role-Based Access Control (RBAC) Model is a widely deployed model in commercial systems and for which a standard has been developed. The widespread deployment of location-based services and mobile applications, as well as the increased concern for the management and sharing of geographical information in strategic applications like environmental protection and homeland security has resulted in a strong demand for spatially aware access control systems. These application domains impose interesting requirements on access control systems. In particular, the permissions assigned to users depend on their position in a reference space; users often belong to well-defined categories; objects to which permissions must be granted are located in that space; and access control policies must grant permissions based on locations and user positions. In this implementation, we want to review various strategies for Geo-RBAC and its future research work for grid computing, virtualized environments and cloud Spatial computing.

In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it also raises concerns over potential intrusion into user location privacy. To protect location privacy, one typical approach is to cloak user locations into spatial regions based on user-specified privacy requirements, and to transform location-based queries into region-based queries. We study the representation of cloaking regions and show that a circular region generally leads to a small result size for region based queries. Moreover, the progressive query processing mode achieves a shorter response time than the bulk mode by parallelizing the query evaluation and result transmission.

The Disruptive Cloud Cloud computing is a service consumption and delivery model that can help improving business performance, control costs and ultimately transform business models. Cloud computing can bring opportunities to many, ranging from businesses that consume IT infrastructure, to providers of such infrastructure, general users and government as well [Hiren Bhatt].

The Figures. 6.4, 6.5, 6.6 below provides the class diagram, sequence diagram, and execution screen shot respectively of the spatial mobile privacy web service application

Figure 6.4 Class Diagram of Spatial Mobile Privacy Web Service Application



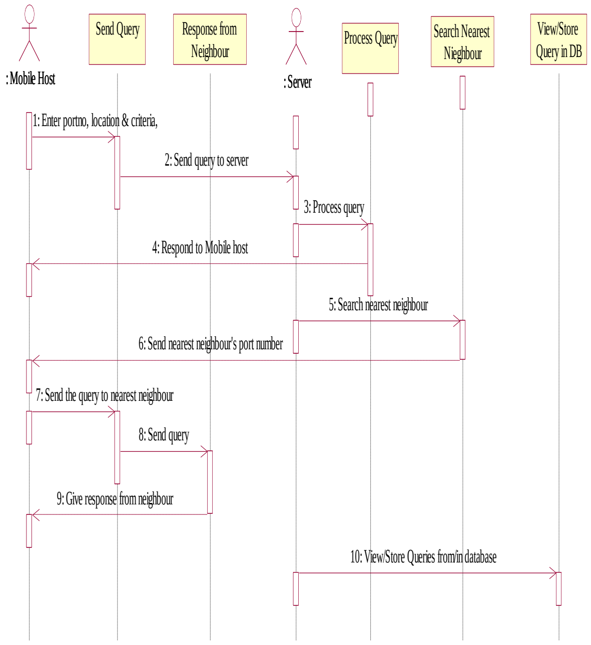

: Mobile Host
Send Query
Response from Neighbour
: Server
Process Query
Search Nearest Neighbour
View/Store Query in DB
1: Enter portno, location & criteria,
2: Send query to server
3: Process query
4: Respond to Mobile host
5: Search nearest neighbour
6: Send nearest neighbour's port number
7: Send the query to nearest neighbour
8: Send query
9: Give response from neighbour
10: View/Store Queries from/in database

Figure 6.5 Sequence Diagram of Spatial Mobile Privacy Web Service Application

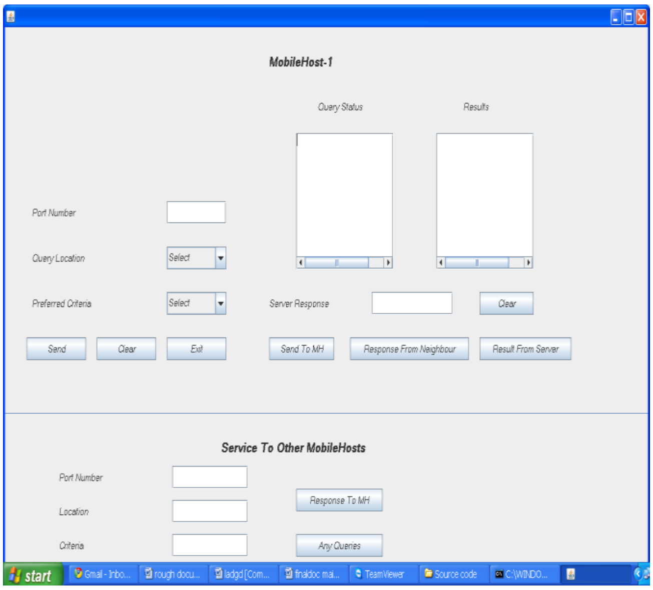


Figure 6.6 Execution Screen Shot of Spatial Mobile Privacy Web Service Application

3) *Case 3 Spatial Secure Design of CRM Web Services Application*

The purpose of the implementation is to develop a Report in which we can track the customer's location, the details and the driving directions to the customer's location. Today there are several web-based maps available on market. Companies like Google, Microsoft and Yahoo provide their own Application Programming Interface (API) for integration web-based maps in applications.

The CRM Application is designed to allow users to track customers and potential customers based on the usage of web service Interfaces. In this implementation we use Google search API to retrieve the details of the customers and MapPoint API is used to generate the map and driving directions to that particular location.

Features:

It enables the user to add, update, and delete contact information for a specified contact. It allows the user to navigate among the contact records. It displays the web pages with the given information. It retrieves a map of the contact's city and state/region. It also retrieves the driving directions to the customer's location. The geographic location and distribution of customers is a critical piece of information that is usually missing from customer relationship marketing and data mining applications.

People tend to shop where it is convenient, which usually means close to home or work, hence travel time is important for retail response to promotion. Hence we illustrate the use of spatial modeling and analysis for understanding customer loyalty, assessing competitive threat, identifying customers likely to defect, and targeted print media promotion choices.

WEB APIS Web APIs are a set of application programming interfaces that can be called over standard Internet protocols. Web APIs generally allow remote computers on different platforms to talk to each other using methods that were previously very difficult.

Representational State Transfer(REST) uses HTTP-GET to retrieve data. Similarly HTTP-POST is used to retrieve data as well as updates.

Simple Object Access Protocol(SOAP) is used for communication in between the client and the server.

We integrate features from the Google API and the Microsoft MapPoint API into the CRM Application to further extend its capabilities.

The application uses the Google API to retrieve the first five sites that mention the customer.

The Microsoft MapPoint API retrieves directions to the customer's location.

Google API

The Google API is currently available using SOAP with the HTTP protocol. Google has made several of its popular features available in an API to developers to use in their own applications.

The Google API supports search requests, retrieving pages from the Google cache, and spelling suggestions. Five Creative Ways to Use the Google API:

1—Build a Google Search Feature
2—Return Random Pages
3—Save the Results of a Google Search to a File
4—Use Google to Check Spelling
5—Use the Google Cache to Retrieved Web Site That Is No Longer Available

MapPoint API

The MapPoint API is implemented as an XML Web service that can be called using the SOAP protocol. MapPoint supports various features such as finding addresses, finding non-addressable places, reverse geocoding, address parsing, finding nearby places, custom locations, routing, map rendering, and Points of Interest (POI).

Five Creative Ways to Use the MapPoint API:
1—Obtain Driving Directions
2—Retrieve a Map
3—Perform a Geocode Lookup
4—Find Nearby Places
5—Obtain Information on Points of Interests

We believe firmly that the true Enterprise Portal is what is beyond CRM -A highly functional, customizable, low-cost, high ROI interface through which the organization can transact with the world. Enterprise portals require different thinking however from the software in a box concept. The starting point for any enterprise portal implementation is to redefine the word "Customer" – in essence to reclaim it from the Customer Relationship Management acronym of CRM. You see, a customer of an enterprise portal is anyone who uses it: staff, management, executives, existing customers, new customers, stakeholders, suppliers…it can be a long list. And for each customer there needs to be a secure role and permissions based access mechanism. These roles and permissions need to extend into the heart of the enterprise software systems so that a supplier accessing the portal gains a completely different experience from a member of staff.

The Figures 6.7, 6.8, 6.9 below, provides the class diagram, sequence diagram and execution screen shot of Spatial Secure Design of CRM Web Services Application respectively

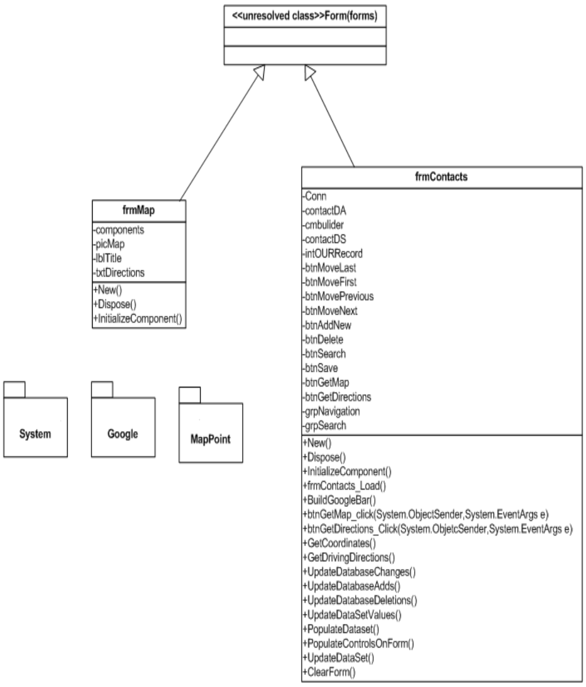


Figure 6.7 Class Diagram of the Secure CRM Application

II. PAGE LAYOUT

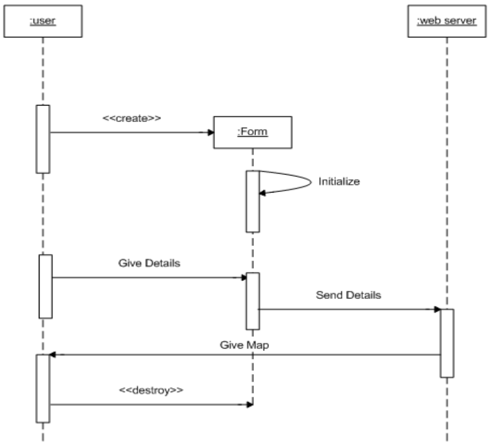
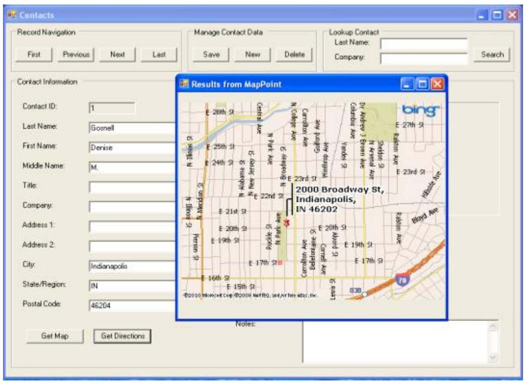


Figure 6.8 Sequence Diagram of the Secure CRM Application Case Study



Last Name:
Company:

Contact ID: 1
Last Name: Gosnell
First Name: Denise
Middle Name: M.
Title:
Company:
Address 1:
Address 2:
City: Indianapolis
State/Region: IN
Postal Code: 46204

2000 Broadway St, Indianapolis, IN 46202

Figure 6.9 Execution Screen Shot of the Secure CRM Application Case Study

III. CONCLUSION

In this paper we discussed about security design for web 2.0 Mashup spatial application privacy using agile modeling using with various case studies.

REFERENCES

[1] Nina Godbole [2009], “Information Systems: Security Management, Metrics, Frameworks and Best Practices”, Wiley India Publishers, Preface pp. 1 – 14.

[2] Nils Agne Narbotten [2009] , “XML and Web Services Security Standards”, IEEE Communications Survey and tutorials, Vol 11, No 3, Third Quarter, pp. 4 – 21

[3] Ozgur Erol et al, [2009], “A Framework for Enterprise Resilience using Service Oriented Architecture approach”, IEEE Sys Con 2009, 3 rd annual IEEE International Conference March 23 – 26.

[4] Patrick Stuedi, Iqbal Mohammed, Doug Terry, [2010], “Where Store: Location-based Data Storage for Mobile devices Interacting with the Cloud”, MCS 10, ,San Francisco USA, ACM 2010 , (Microsoft Research) , June 15, 2010 , pp. 1 – 10.

[5] Rafuel Accorsi, Claus Wonnemann: Indico. “Information flow analysis of Business Processes for confidentiality requirements”, pp. 1-16

[6] Reza B’Far [2005], “Mobile Computing Principals – Designing and Developing Mobile Applications with UML and XML”, Cambridge University Press, ISBN: 0-521-69623-2, pp. 146 – 198.

[7] Ross Anderson, 2003, “Security Engineering: A guide to building Dependable Distributed Systems”, Wiley publishers, pp. 1 – 19.

[8] Sami Baydeda, Matthias Book, Volker Gruhn (Eds.) [2005], “Model-Driven Software Development”, © Springer-Verlag Berlin Heidelberg, pp. 18-22.

[9] Sandeep Chatterjee [2004], “Developing Enterprises Web Services An Architects Guide”, Pearson, pp. 67 – 98.

[10] Sasikanth Avancha [2008], “A Framework for Trustworthy Service Oriented Computing”, ICISS 2008, pp. 124 – 132.

[11] Sarah Spiekermann, Lorrie Cranor [2009], “Engineering Privacy”, IEEE Transactions on Software Engineering”, Vol 35 No 1 January February 2009 pp. 67 – 82

[12] Satoshi Makino, Takeshi Imamura, Yuichi Nakamura [2004], “Implementation and Performance of WS-Security”, International Journal of Web Services Research, Jan-March 2004, Idea Group Publishing, pp. 58-72.

[13] Sebastian Hohn, Lutz Lowis, Rafael Accorsi, Albert-Ludwig [2009], “Identification of Vulnerability Effects in Web Services using Model-Based Security” IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch001, pp. 1 – 32.

[14] Soumya Simanta, Ed Morris, Sriram Balasubramaniam, Jeff Davenport and Dennis B.Smith [2009], “Information Assurance Challenges and Strategies for Securing SOA Environments and Web Services”, IEEE SysCon 2009—3 rd Annual IEEE International Systems Conference, Vancouver, Canada, March 23 – 26, pp 1 – 4.

[15] Spyvain Halle, Roger Villemaire, Omar Cherkaoui [2009], “Specifying and Validating Data-Aware Temporal Web Services properties”, IEEE Transactions J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.