Identification of Security Challenges and Security Issues in Social Oriented Architecture

Ami Shaileshkumar Desai
Assistant Professor Of Vivekanand College, Surat

Dr. Sanjay Buch
Assistant Vice President Of Reliance Industries Ltd., Naroda

Abstract: Nowadays social networking/service sites are our daily habits and necessity. About 80% of transaction done through online web services, but it is not safe or reliable. Because People may unaware have fraud and crime happened online or they have less command on English language. So, threats are increasing day by day. SOA (service oriented architecture) provides based to online servicing, social interactions and communications without human interaction, but it is raises privacy and security concerns in web services. Generally Web services managed by more than one stake holders. In this proposal we discuss the security testing issues of web services. Development based on SOA is still required for providing the unique security or proper testing.

Keywords: SOA, WSDL, Black box testing, White box testing, Gray box testing

I. INTRODUCTION

With today's many people are attached with each other using web technology. Many service providers deliver facilities to exchange of ideas, information, videos, pictures, and graphics based on SOA. It also allows easy sharing and distribution of existing content to others so that professional work can be shared through networks.
Using Social networking web sites maximum people are share or transfer images, video clips, text and personal details without any precautions and bothered about fraud. People also doing on-line transaction without any security check because of many people do not have awareness about on-line fraud and cyber crime. Thus hackers can easily hack and misuse of their information. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats. There are certain issues regarding on-line fraud occurs with people are describe as below,

A. Hacking:

This is a type of crime in which a person's computer is become out of order so that his/her personal or sensitive information can be accessed by other unauthorized person. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his/her computer is being accessed from a remote location by hacker.

B. Theft:

This crime occurs when a person break copyrights laws by downloading music, movies, games and software. Generally, license version software is costly hence culprit person crack this license software and use for profit. To use cracked software, company's logo, domain name and idea of good name websites for misguide people is crime.

C. Cyber Stalking:

This is a kind of online harassment wherein the victim is subjected to a bombardment of online messages and emails. Typically, these stalkers know their victims and instead of alternative to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more depressed.

D. Identity Theft:

This has become a major problem when people use the Internet for money transactions and online banking services. In this cyber crime, a criminal accesses data of a person like bank account, credit & debit cards details, Social security and other sensitive information to draw off money or to buy things online on the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history also.

E. *Malicious Software:*

These are Internet-based software or programs that are used to disturb a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

While surfing such web sites these malicious software pop up and ask to download. By downloading such software cause start damaging your network and system.

F. Child soliciting and Abuse:

In this type of cyber crime wherein criminals solicit minors through chat rooms for the purpose of child pornography. Many Investigating companies or agencies has been spending a lot of time to monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

II. EXAMPLE OF FRAUD ON WEB SERVICES

Lack of proper testing, methods, model and technology fraud occurs and it will increase day by day which is provides negative impact of online services. Some cases are as explain bellow,

Case 1:

How online transaction of information and currency pass through generally as bellow

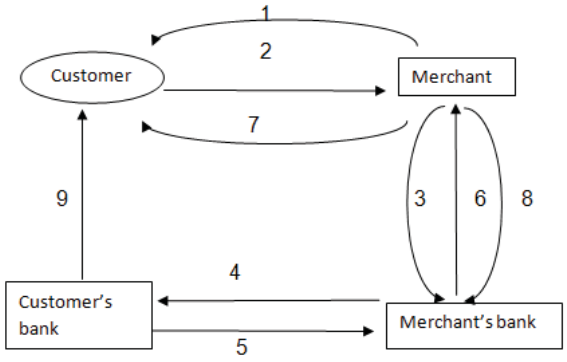


Fig.1 Online shopping system

Fraud Cases in above system are as bellow,

Maximum fraud is occurred in step 1, 2 & 3 when customer sends their bank details and credit or debit card information.

- In first step fraud web services which specially develop for attract and collecting personal data, who have no online transaction authorization certificates. So, they develop their own facility for gathering information without knowledge of customer.
- In second step customer send detail to merchant which may be redirect through hackers web services and data hacks
- In third step when merchant forward payment information through PayPal, Paytm, etc to bank, but in between customer data redirect directly to hackers websites

Case 2:

How insurance, service provider, matrimonial site etc

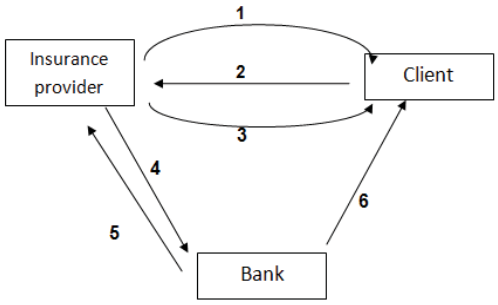


Fig.2 Online insurance payment system

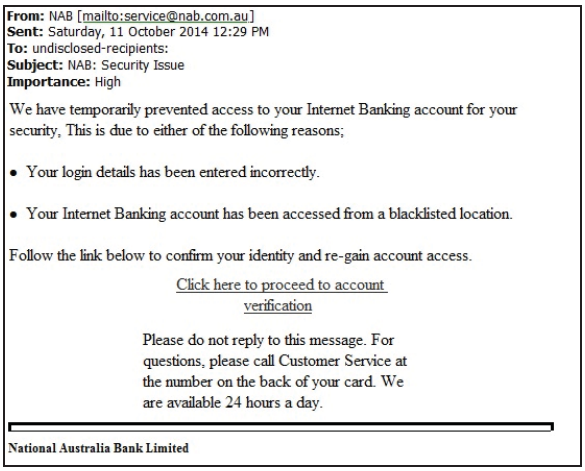
Fraud Cases in above system are as bellow

In step 1 & 3 fraud is occurs after banking fraud

- In first step fraud web services which specially develop for attract and collecting person's data. They send spam messages, request for help, bogus offers, winner emails etc to miss guide customer.

- In third step customer send detail to insurance company which may be redirect through hacker's web sites and data hacks. May be that web site is fraud. For example a customer wanted car issuance. For registration customer send all information about car like owner name, address, car number, chassis number, engine number etc and miss use it
- Bank fraud may be occurs its already discussed in above case

Case 3:
The email states customers have incorrectly entered their Internet Banking details, or have accessed their accounts from blacklisted locations.
The email asks customers to validate their details by clicking on a link.
This link leads to a fake website, requesting credit card details and personal information.



From: NAB [mailto:service@nab.com.au]
Sent: Saturday, 11 October 2014 12:29 PM
To: undisclosed-recipients:
Subject: NAB: Security Issue
Importance: High

We have temporarily prevented access to your Internet Banking account for your security, This is due to either of the following reasons;

- Your login details has been entered incorrectly.
- Your Internet Banking account has been accessed from a blacklisted location.

Follow the link below to confirm your identity and re-gain account access.

Click here to proceed to account verification

Please do not reply to this message. For questions, please call Customer Service at the number on the back of your card. We are available 24 hours a day.

National Australia Bank Limited

Fig.3 Online fraud email example

According to Fig.3
These frauds are occurs because of some lacking in software designing, software coding, hardware, software, security protocols, methodology, network, web standards, Architecture, tools and technology. As per study and review major problems occurs due to proper testing model for the web services.

Generally for protection, all web site developers are testing their web sites using white box testing, black box testing and gray box testing. After web hosting some web automated tools are provided in SOA for automation performance, load and security testing like Soap, Apache jmeter, Curl, Jconsole, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET, SSL(Social security layer) etc.

According to R. S. Pressman, Testing have own pros and cons.

According to Naik & Shivalingaiah (2008), Nowadays All service oriented web services based on web 2.0 standards and SOA. SOA is the architectural style that supports loosely coupled services to enable business flexibility in an interoperable, technology-agnostic manner. SOA consists of a composite set of business-aligned services that support a flexible and dynamically re-configurable end-to-end business processes realization using interface-based service descriptions.

According to Torry Harris, SOA divide into layers and all types of testing are done in these layers (which testing through customer, developer and provide view). Here testing is done on all layers but fraud occurs when multi stake holders web services, distributed data, different languages, multi ownership or anything else but still it is difficult to identify so below challenges are remain.

III. CHALLENGES OF WEB SERVICES

A. Functionality

- According to Asankav (2014), it is different from traditional software testing because in traditional testing GUIs, number of user, types of requirements and inputs are fixed. Mainly problem occurs for multiple types of GUIs and huge amount of various types of data.

- This multi functions are also managed by different service providers e.g. In Nokia token machine website some web pages or facilities are managed by other services providers/developers. So it is difficult for testing without testing rights and source code.

B. Publish, Find, and Bind

- According to Asankav (2014), before publishing and developing of web sites they needs to think as customer, developer, service provider and stakeholder point of view.
- It is also a major and important problem for binding and transportation because web services are manage by multi or distributed server and some time services are provides by third party like online payment services done by third party bank or PayPal.

C. *Security*

- Dolvara Gunatilaka mention that there are many types of SOA related issues from customer side like Privacy issues, Identity theft issues, Span issues, Malware issues, Physical issues, etc. because of improper architecture, technology or security method of SOA.
- As per report by US government (2013), online services provider collects many personal and bank information of customers. But it may be not secure because provider sells our private data to other provider for marketing without any intimation of customer which increased spamming, phishing, etc.
- Fake and same domain name (with minor change in domain name) also misguide the victim. Many web sites developed for collecting victim's personal information. These information will further use for fraud like spamming, spoofing, phishing etc by culprit.

D. *Performance*

- Asankav (2014) pointed that It is also a big challenge or nearly impossible to develop user friendly and error or bugs free system because after implementation it is difficult to do testing. Recently web sites data are managed in distributed server or third party server. These stored data also access by multi languages from multi platform. So, Huge and variety of data is difficult to manage load and performance testing. It needs automation needs to be done through programmatic interfaces.

IV. WORK IS DONE

- Guided by Gaurish Hattangadi (2011): SOA testing model is divide in four steps: service level testing, process testing, end-to–end testing and regression testing. It is difficult to implement in inaccessible system and repetitive steps for login and logout per use. Challenges SOA testing need development verification tool or testing methodology.
- As defined by Torry Harris(2007): According to Torry governance provide rules and policy all over the system development life cycle like security, performance, transaction, backup, access but it is not properly work on individual level. So challenges are like services that do not have a user interface, Data driven business logic with in services, performance, scalability, stress, load, performance, etc problems in SOA
- As per studied by Shivani Acharya & Vidhi Pandya, they discuss how black box, white box and gray box testing methods are applied to validate critical software system. There are testing problems using white box and black box testing in distributed network and system because source code is not available. So testing is done by Gray box testing through WSDL(Web Services Definition Language). They compare these three methods with examples and conclude that gray box testing is well suited for web site testing.
- Sahida Sultana *et al.* (2014) are mentioned that Need of testing. Type of testing and compare of testing techniques. Advantages and disadvantages of testing techniques. They develop method for selection of testing techniques using AHP (ANALYTIC HIERARCHY PROCESS). Proposed method is a four step process, namely, (I) identify the criteria, (II) construct the hierarchical structure of Software Testing Techniques, (III) construct the decision matrix, and (IV) the selection of a technique. Proposed method selects the agile methods for the testing of the project. There is a need to improve the agile methods by intertwining of decision making approaches for the selection and prioritization of requirements. But it is work when requirement, environment, language etc are fixed.
- Symantec Netmarcom (2009) stated that in this paper they explain how online bank system protects from Trojan affected PC fraud. In this, during the fraud transaction detection system verify users authentication through 2FA(two factor authentication) means first verify by username & password and then check by automatic SMS (one time password) / voice call before transaction.
- A Review by Ajeet Singh *et al.*(2012), In this research paper they specify which necessary and important security are require for online payment system like authentication, access control, data confidentiality (security), data integrity, non reputation. Attack on online payment system is basically done by network attack or cryptographic. They also specify some approach for security to payment system like SSL, SET, 3D secure, cyber cash, tunnel. But still there is some security model is needed to secure information transaction.

- As per comparative review of Dancho Danchev (2013), in this article he discussed anti-phishing facilities provided by internet browser. Still Opera, Internet Explorer, Google chrome, Apple Safari and Mozilla fire fox provide detection rate of the phishing URLs used in the test are 94.2%, 82%, 72.4%, 65.6% and 54.8% respectively.
- G. Zayaraz and Poonkavithai Kalamegam (2013) were presented CPN (*Colored Petri Nets*) model basically made for combine test of web services for control flow and data flow testing. It generates test sequences and for verifies design correctness of web service? It also check common path to decide reused code and redundancy testing which reduce cost and time for testing but it work when whole site is maintained by one developer.
- According to Michael Fire, Roy Goldschmidt and Yuval Elovici (2014) , There are main four types of threads occurs using online transaction like classical threat, modern threat, combination threat and threat targeting children which again classify in phishing, spamming, cross-site scripting, clickjacking, identity cloning, information and location leakage etc. They provide variety of security and privacy solutions for prevention & protection. Which divide in main five level first level prevent unwelcome intruders from entering and viewing OSN users' personal posts and details. Second level is use to prevent malicious users from collecting OSN users' personal posts and details. Third level is to protect both young children and teenagers by enabling parents to monitor online activity primarily via various monitoring software. Fourth level uses wisdom of the crowd to pinpoint malicious users. Fifth level which parallels the functionality of a *police force* includes authentication mechanisms which are responsible for making sure that only real people can log. But still prevention and protection method is required against threats done on on-line social networking.
- As per survey by Shih-Chien Chou(2015), He specifies maximum data was leaked during the execution of net services. He developed NetIFC (net information control flow) for controlling leakage of information. NetIFC is not embedded with net services it is execute parallel with different web sites. NetIFC uses groups to prevent exchanging incomparable information and security levels to prevent information leakage. Since our research excludes virus and worms, only output information may be leaked. NetIFC thus strictly controls output statements but allows others.
- As per the comprehensive study of Karumanchi and Squicciarini (2015), Develop proxy based solution. A novel simple taxonomy to classify Web Services vulnerabilities. Within the provided classification, they stated that web services are classified the services into 6 types based on their provisioned service: Business (eg., quote retrieval), Location (eg., weather), Communication and Entertainment (eg., email, travel, holiday), Scientific/Security (eg., gene variations, encryption), Search (eg., search for university data), and Others. They discussed various vulnerabilities associated with Web Services. They provide comprehensive solution to prevent the exploitation of these vulnerabilities. We suggest the adoption of a proxy-based solution to counter these vulnerabilities. As part of the future work, they plan to complete the deployment and testing of the proposed proxy-based solution. It provide security between client and server system but it not workable in multi stake holder or multi environment system
- Poster presentation by Tan Phan *et al.* (2010), to provide end to end collaborative partner services in properly protecting each other's data. In this modify the message handling mechanisms of Web Service engines to dynamically gather protection requirements for a given outgoing message by aggregating requirements from original owners of message data. They encrypt data using binding method, encrypted algorithm and length of the key. It broad cast input and output data with protection. Provide approach for collaborative service partners to protect data in transit according to the requirements of parties who created and processed that data. But approach ensures that data is not under protected
- As per Choudhary, Aaseri, & Roberts (2013), They develop Web service security model based on HTTPI protocol over SOAP, with the security goal: client/server authentication and integrity on message, without confidentiality. They use
    - Username/Password Tokens
    - Binary Authentication Tokens (X.509 certificates) for Authentication
    - XML Digital Signature for Message Integrity

    To secure the communication between two web services. The secured web services based on HTTPI can be used in non-confidential open applications (like: Social Networking, Blogging and News sites) in future.
- As Per Mamoon Yunus (2012), SOA testing done by IT professional using automated tools for check. Functional testing, first transport protocol for transferring services or communication on internet by http/https protocol. Public key infrastructure is managed by SSL and HTTP for secure functional testing. Services require client authentication and authorization for before the request is accepted and a response is returned through identity token in encrypted form Performance testing is testing by SOA tool by calculating time stamps, latency time, and transaction per second. Security testing for data base security SQL injection, SOAP and XML protect database information. It also protected from virus and malware. But SOA testing

require demanding domain skill, tools and processes for simple web sites. SOA lifecycle testing framework is crucial for ensuring a successful SOA deployment.

V. DISCUSSION

At this movement according to literature review of tools, technology, mechanism, testing methods for web services testing have some gap the problems are as bellow.

- Basically web services are chained and depended on each other because of different languages and platform.
  .
- Web services are managed by multi stakeholder. Some time a stake holder makes changes in web services without giving prior notice to other stake holders. At that time dependent stakeholders may face problem due to certain changes.

VI. CONCLUSIONS

Generally developer provides user-friendly and secure web services but due to lack of proper testing model some bugs are there.

Web Services based on SOA plays an important role in facilitating the integration of different applications from various departments or trading partners and thus increasing business productivity. This web service security testing is still big problem which need any model/method of security testing for prevention from fraud at the time of online transactions without considering the rights of stakeholders.

REFERENCES

[1] Acharya, S., & Pandya, V. Bridge between Black Box and White Box – Gray Box Testing Technique. *International Journal of Electronics and Computer Science Engineering , 2*, 175-184.

[2] Ajeet, S., Singh, K., & Shahazad. (2012). A Review: Secure Payment System for Electonic Transaction. *IJARCSSE , 2* (3).

[3] Asankav.wso2.com. (2014, 4 11). How to Efficiently Test Service Oriented Architecture. *WSO2*

[4] Chou, S.-C. (2015, Feb). Controlling Information Flows in Net Services with Low Runtime Overhead. *I.J. Computer Network and Information Security* , 1-9.

[5] Choudhary, P., Aaseri, R., & Roberts, N. (2013). HTTPI BASED WEB SERVICE SECURITY OVER SOAP. *IJNSA , 5* (3).

[6] Danchev, D. (2013). *Comparative review: Opera leads in browser anti-phishing protection*. Retrieved from http://www.zdnet.com/article/comparative-review-opera-leads-in-browser-anti-phishing-protection/

[7] Fire, M., Goldschmidt, R., & Elovici, Y. (FOURTH QUARTER 2014). Online Social Networks: Threats and Solutions. *IEEE COMMUNICATION SURVEYS & TUTORIALS, , 16* (4), 2019-2036.

[8] gunatilaka, D. (n.d.). *A survey of privacy and security issues in social networks*. Retrieved from http://www.cse.wustly.edu/~jain/cse571-11/ftp/social/index.html

[9] Hattangadi, G. (2011, july). Modern SOA testing.

[10] (2013). *Information resellers.* the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate. United States: Government office.

[11] Karumanchi, S., & Squicciarini, A. (2015). A Large Scale Study of Web Service Vulnerabilities. *Internet Services and Information Security , 5* (1), 53-69.

[12] Naik, U., & Shivalingaiah, D. (2008, March). Comparative Study of web 1.0,web 2.0 and web 3.0. *International CALIBER* , 499-502.

[13] Netmarcom, S. (2009). - *WHITE PAPER: DEFEND YOUR INSTITUTION AGAINST TROJAN-AIDED FRAUD* . SYMANTEC.

[14] Pressman, R. S. (2001). *Software Engineering* (Vol. 1). New york: McGraw-Hill.

[15] Sultana, S., Sadiq, M., & Ahmad, W. (2014). A Tool To Automate The Test Cases Of Software Using Gray Box Testing Approach. *International Journal of Advanced Research in Computer and Communication Engineering , 3* (8), 7689-7695.

[16] Tan Phan, J. H. (2010, april). Protecting Data in Multi-Stakeholder Web Service. *(978-1-60558-799)* . ACM.

[17] Torry, H. (2007). SOA Test Methodology. 10.

[18] Yunus, M. (2012, Feb). Fundamentals of SOA Security Testing. *Service Technology Magazine* (LIX), pp. 1-6.

[19] Zayaraz, G., & Kalamegam, P. (April 2013). A Test Framework based on CPN Model for Functional Testing of Web Service Composition. *International Journal of Advanced Science and Technology* , 135-150.