Abstract—Business process modelling is very crucial for enterprises because it gives an idea how the business would be operated in the real world and it is important for every stakeholder. Along with increased connectivity in SOA environment, security risks rise exponentially. MDS frameworks are presented to systematically developed security enabled SOA based software applications, where security is modelled along with the business process model. However; there is an information gap that exists between business process expert (business analyst) and security expert (technical people) on the notion of security during business process modelling, while defining security requirements for SOA based application. This progress work paper is aim to bridge the information gap between the two experts. This will be done by presenting a framework which will facilitate the business process expert in modelling the security requirements along with the business process modelling. This security annotated business process model will facilitate the security expert to specify concrete security implementation. We apply approach for a typical on-line student information system business process.

Keywords—Model Driven Software Development (MDSD), Model Driven Security (MDS), Service Oriented Architecture (SOA), Business Process Modelling

I. INTRODUCTION

Service Oriented Architecture (SOA) facilitates the merging of Business and Information Technology (IT) domain. Application development is becoming easy with the emergence of Web Services technology and SOA paradigm. In SOA environment; a Web Service, which serve as an application components, can be coupled over the internet or via the Internet to form business applications. Which result in a complex distributed, heterogeneous and loosely-coupled architecture. This architecture is composed of complicated topologies, firewalls and intermediary servers where organizational assets and resources are exposed by business services [1, 2]. Web services located in various businesses are connected to form an application and these businesses have their own security infrastructure which makes security a difficult task [1]. However realistic connection between business values and security cost is neglected in existing methodologies for IT security, which result in integrating security into business process life cycle [3].

Security must be unified with the software engineering process but in practise it is implemented in ad-hoc manner [4]. Security is left on to the developer and added when the functional requirements are met or at the time of integration of distributed applications, which is not a realistic approach [1]. During the past few years, several security protocols, access control models and security implementations are emerged to enforce the security goals [1, 2] however focus of the SOA security standards and protocols are towards technological level; which do not provide low level of abstraction and mastering them is also a daunting task [5, 6]. Business process modelling for SOA based applications are normally performed in a modelling language such as Unified Modelling Language (UML) or Business Process Modelling Notation (BPMN), it is not possible to specify security requirements during business process modelling [7]. Some security extensions are presented in these modelling languages by different authors to annotate the business process model with security goals [8, 9] and work is still in progress.

Model Driven Software Development (MDSD) provides a systematic way of software development. The basic building block of MDSD paradigm is a model; which in further stepwise refined and transformed into executable software [10]. Model Driven Security (MDS) and automatically developed software having security configuration has been a topic of interest among the research community. Different research groups across the globe are trying to solve the security problems for SOA based applications by presenting MDS Frameworks [1, 2, 7-9, 11, 12]. In our previous work [13], we have highlighted the different SOA security problems and study of different MDS frameworks was presented to address the security problems.

In MDS; business process expert and IT security expert must work collaboratively at Platform Independent Model (PIM) level of abstraction while designing the SOA application, must define their security goals on a common abstract level i.e. during business process modelling. Each domain expert is responsible for his domain specific activities and communication is take place over a common process model [2]. It is evident that business domain expert must define the security requirements at business process model [14]. In our current work we have presented a MDS framework at PIM level of abstraction.
to integrate security goals in a business process model. Our aim is to facilitate business process expert to add security goals while performing business process modelling. Security annotative business process model will facilitate the security expert while defining concrete security implementation. BPMN is used as a modelling language for our work; which is an industry standard for business modelling [4].

II. CURRENT MDS APPROACHES FOR SOA

MDS specializes MDSD towards information security [15]. Here security concepts are modelled side by side with the business process modelling using modelling notations like UML, BPMN; at the PIM level of abstraction and step-wise refined to further level of abstraction i.e. Platform Specific Model (PSM) and Implementation Specific Model (ISM) [2, 6, 15].

As seen in the figure 1, security configuration can be generated automatically through MDS by adding security objectives to business model. During MDS configuration process, security objectives are defined by the business analyst during Business Requirement Analysis. Afterwards a Service Design is created by software architect by adding security intents. This security annotated model is still at PIM Level. Later on assembler executes the model transformation process and security intents are transformed into concrete security configuration i.e. PSM. Platform configuration and service deployment is done by the developer. [16].

Figure 1: MDS Configuration [16]

Many MDS security frameworks are presented by different research groups. Main idea of these MDS frameworks is to incorporate security requirements during business process modelling. Security goals are expressed graphically at the time of business process modelling and security annotated business process model is developed. This model is transformed to corresponding security policies and access controls during the next levels of abstractions. Among these MDS frameworks, following three are discussed. Working of these frameworks is: PIM is created which would be transformed to PSM and PSM will be transformed to ISM. However these frameworks differ in the number of security objective they are focusing and their working style.

Michal Hafner et al. in [11] presented a framework for the model driven development and management of security critical workflow for Web Services based SOA systems known as SECTEC. Security objectives for SECTEC framework are Access rights i.e. Authentication and Authorization through Role Based Access Control (RBAC). Working is almost same as of MDA approach presented by Object Management Group (OMG) i.e. security annotated model is developed at PIM level of abstraction which is transformed to PSM level of abstraction and PSM is transformed to ISM.

SECTTISSIMO framework is an extension of the SECTECT framework [12] presented by Memon M. et al. In SECTTISSIMO have many more security goals then SECTECT framework covering access rights, non-repudiation, right delegation, single sign-on privacy and auditing. In SECTTISSIMO, after PIM level of abstraction; a new layer is added naming Abstract Security Service Model to further elaborate the security requirement. This layer is still PIM which is transformed into PSM; and PSM is further transformed to ISM.

Wolter C. et al. in [2] have provided a very detailed discussion about the different abstract security aspects i.e. Confidentiality, Integrity, Authentication, Authorization, Traceability, Auditing and Availability and developed a security policy model based on these security requirements. This model describes the secure interaction of different objects and the necessary information to be stored about these interactions. This policy model will serve as security model for their MDS framework. In their framework, they have introduced a new level of abstraction called Computational Independent Model (CIM). Security expert and business process expert work side by side to prepare CIM which is transformed to PIM; which is further transformed to PSM.

III. PROBLEMS IN THE CURRENT MDS APPROACHES FOR SOA

Information gathered during modeling of the business process are not sufficient to generate enforceable security configuration, expert knowledge for each field must required for successful implementation because multiple solutions for a security goal might exist [7]. In MDS frameworks, presented in the previous section; at PIM level of abstraction, security experts and developer (technical people) at one side and business domain expert (business analyst) at other side, have differences on notion of security. Business analyst defines security goals at a very abstract level in the context of business application to fulfill some business goal. Whereas technical people want to achieve security through some technical means i.e. algorithm, protocol or implementation [15]. For
example business analyst defines a security goal “authorization” for accessing a service. Technical people have different options for implementing authorization i.e. a certificate based authorization mechanism or four-eyes-principle or break-glass policy [15]. Same is the case for the security goal “confidentiality”, which can be implemented by securing part of a Simple Object Access Protocol (SOAP) messages or through Secure Socket Layer (SSL) channel [7]. Implementing a particular solution for a security goal might have different implications or it can re-organize the whole business process [15].

IV. PROPOSED MDS FRAMEWORK FOR SOA

Business process expert will define the security goals along with the business process modelling. These security information, modelled in the business process model, would be sufficient enough so that security expert may be able to i) model security solution (security mechanisms, security protocols, access control models) for the system, ii) perform some tool-supported transformation to generate the executable artefacts. Business process model will be prepared at PIM level of abstraction. Along with the business process model, security requirements will be transformed to PSM and PSM will be transform to ISM.

![Proposed MDS Framework](image)

**Figure 2: Proposed MDS Framework**

**Security Goals of our MDS Framework**

Security is an abstract concept which can be defined by specifying a set of security goals. These security goals can be further subdivided, specialized or combined [14]. During our work we mainly focus security measures to encounter the threats related to: use of identity information and associated rights i.e. authentication authorization (Confidentiality), information in different forms i.e. stored, transferred or processed (confidentiality and integrity) and service function (availability and integrity of a system) [5].

Different research groups are focusing different security goals for their work [1, 4, 14, 15, 17]. We believe security goals defined by Michal Hafner et al. in [15] fulfil the requirement of a business process model which is defined at high level of abstraction. The security goals are **confidentiality, integrity and availability**. Confidentiality is achieved through access control which itself is achieved through authentication and authorization. Integrity ensures the integrity of data (properness of information) as well as integrity of origin. In SOA environment availability is used in the meaning of non-repudiation[15].

V. CASE STUDY

To demonstrate the work, a case study of “Online Student Information System” is presented. It describes the web services based interaction between the participants and enables them to work through the Internet. The whole process has to be realised in a peer-to-peer fashion and should integrate security requirements.

A. Business Scenario

Pakistani universities normally have semester based education system, and normally have two semesters in a year. During the whole working of the system, normally interaction takes place between three stakeholders naming Student, University Administration and Teacher. Normally university administration is composed of three departments naming registration, accounts and examination. A student has to register for each semester by filling the registration form and submit it to the registration department, which verify three things: first; student’s dues information from accounts department, which calculate the dues of the student for the semester after consulting his/her accounting information and send it to student as well as registration office. Second; previous result of the students are verified from examination department, which prepare the student result. Third; university rules for registration are consulted and ensured. After getting verified from these three things, registration department informed student about his/her registration status and registered students lists for the offered courses are prepared. Faculty member who is teaching the course get the list of registered student for a particular course. He is responsible for the student’s evaluation and assigning him/her marks and grads. Whenever a teacher evaluates a student, he enters his/her marks in the student result file which is maintained at examination department. At the end of the semester student is notify about his result information by exam department.

B. Security Requirements of the System

In Online Student Information System, a student needs to perform different tasks i.e. filling the registration form, viewing registration status and result information. Necessary permissions are assigned to student on different objects to perform his/her tasks i.e. student require update permission on registration form and read permission on registration status and result information. These are personal information of a student therefore confidentiality is required i.e. proper access
control mechanism with authentication and authorization is required to access these information.

Furthermore student has to submit the registration form to the registration department. Student must sign the submitted form with his/her signature so he/she may not be able to deny that he/she has not submitted the registration form. Availability (Non-repudiation) is required in this use-case between the student and registration department. As this registration form is submitted online, therefore secure information flow i.e. integrity is required to successfully perform this use-case. These three security requirements i.e. Confidentiality, Availability, and Integrity can be identified and modelled for other users of the case-study like teacher and clerks from different departments i.e. registration, accounts and examination.

Figure 3 describe the security annotated business process model which is modelled by the business process expert. It will facilitate the security expert in defining the concrete security requirements for the software application because now he/she has understanding what security

Figure 3: Online Student Information System
intension business analyst has for the system. Which will improve the security of the Information System.

VI. CONCLUSION

Incorporating security requirements into early stages of software development will improve the important aspect “Security” of SOA based Information Systems. Problem of the misunderstanding on the notion of security between the two experts i.e. business process expert and security expert; is presented; if it left unmanaged then it may cause serious consequences. A MDS framework is presented for defining the security requirements for Web Services based SOA applications, while performing Business Process Modelling using Model Driven approach at PIM level of abstraction. We believe our effort is a contribution towards stressing to incorporate security requirements during business process modelling for SOA applications.

We are working to present a Domain Specific Language (DSL) for our MDS framework to facilitate business process expert to efficiently model security goals along with business process modelling for SOA based applications. We are trying to present lightweight DSL covering essential security objectives so that it would be easily understandable and useable by a common business process expert.

REFERENCES