Extensão de um *framework* de processo para adaptação à segurança em aplicações Web

Rosana Wagner
PPGI – Programa de Pós Graduação em Informática
Universidade Federal de Santa Maria
Santa Maria – RS – Brasil
rosanawagner@gmail.com

Lisandra Manzoni Fontoura
PPGI – Programa de Pós Graduação em Informática
Universidade Federal de Santa Maria
Santa Maria – RS – Brasil
lisandramf@gmail.com

Raul Ceretta Nunes
PPGI – Programa de Pós Graduação em Informática
Universidade Federal de Santa Maria
Santa Maria – RS – Brasil
raul.cerettanunes@gmail.com

RESUMO

Este artigo descreve uma proposta de extensão do Rational Unified Process (RUP) para contemplar as práticas preconizadas pelo System Security Engineering Capability Maturity Model (SSE-CMM). Inicialmente foi realizada uma avaliação, onde verificou-se que várias áreas de processo propostas pelo SSE-CMM não são contempladas pelo RUP. A incorporação de segurança, baseada no SSE-CMM, ao RUP é considerada importante, visto que a cada dia são necessários novos mecanismos de segurança para proteção dos sistemas de informação. Neste sentido, esse artigo propõe a inclusão de uma nova disciplina no RUP visando satisfazer requisitos de segurança, conforme descrito pelo modelo SSE-CMM (norma ISO/IEC 21827), de forma que a segurança esteja integrada em todas as fases do desenvolvimento de software.

ABSTRACT

This paper describes a proposal to extend the Rational Unified Process (RUP) to include the practices recommended by the System Security Engineering Capability Maturity Model (SSE-CMM). Initially, an assessment that found that several areas of process proposed by the SSE-CMM are not covered by the RUP. The incorporation of security, based on SSE-CMM, the RUP is considered important, since every day is a need for new security mechanisms for protection of information systems. In this sense, this paper proposes the inclusion of a new discipline in the RUP in order to satisfy security requirements, as described by the model SSE-CMM (ISO / IEC 21827), so that security is integrated into all phases of software development.

General Terms Reliability, Security, Experimentation

Keywords Security, RUP, SSE-CMM

1. INTRODUÇÃO

Ameaças à segurança das informações dos negócios, de propriedade intelectual e à privacidade das informações pessoais estão aumentando. Assim, a necessidade de se conter tais ameaças faz com que o gerenciamento da segurança de informações ganhe mais importância nas empresas. De acordo com um estudo realizado por [1], o roubo de dados e violações de crimes cibernéticos pode ter custado para as empresas em 2008 mais que $ 1 trilhão em razão da perda de propriedade intelectual e dos gastos com a reparação dos prejuízos. Esses dados são preocupantes e se pudessem ter sido previstos, provavelmente, seriam evitados através da implementação de alguns modelos e normas de segurança como: ISO 27001, ISO 27002, SSE-CMM, entre outros [2].

Na tentativa de reduzir tais números e melhorar constantemente a segurança nas organizações, neste artigo é descrito o modelo de SSE-CMM, que está centrado nos requisitos para implementações de segurança em sistemas que estão relacionados com o domínio da Tecnologia da Segurança da Informação. Dentro desse domínio, o modelo SSE-CMM [3] está focado nos processos utilizados para alcançar a Segurança da Informação, mais especificamente na maturidade desses processos. O modelo SSE-CMM resultou da investigação sobre a necessidade de um modelo de maturidade de capacidade (*Capability Maturity Model* - CMM) especializado para tratar de engenharia de segurança.

O Rational Unified Process(RUP) é um processo de engenharia de software. Ele fornece uma abordagem disciplinada para atribuir tarefas e responsabilidades dentro de uma organização de desenvolvimento. Seu objetivo é garantir a produção de software de alta qualidade que satisfaça às necessidades de seus usuários finais, dentro de um cronograma e um orçamento previsíveis [4]. O RUP não propõe atividades específicas para tratar de questões de segurança, limita-se a descrever que na atividade "Detalhar Requisitos" é necessário considerar como requisitos não-funcionais os requisitos de segurança do sistema e que na atividade "Revisar Arquitetura" é necessário avaliar se a arquitetura contempla os requisitos de segurança.

Considerando que, não é objetivo do modelo SSE-CMM especificar um processo específico para ser usado pela organização, a intenção é que a organização possa usar seus processos adaptando-os às recomendações do SSE-CMM, e que o Processo Unificado da Rational é um dos modelos de processo de software mais utilizados atualmente, neste artigo é proposta uma extensão do RUP para satisfazer as práticas de segurança do SSE-CMM, adequando-o para o desenvolvimento de software seguro, de acordo com um modelo de segurança já utilizado com sucesso em várias organizações.

A adaptação do RUP consiste na inserção de uma nova disciplina de suporte chamada de “Segurança de Sistemas” que descreve uma série de atividades, tarefas, artefatos e papéis, definidos de acordo com a especificação do Modelo SSE-CMM [3].

O artigo está descrito da seguinte forma: a seção 2 descrevem como o Processo Unificado da Rational (RUP) foi estendido para tratar das atividades de segurança do modelo SSE-CMM. A seção 3 mostra o estudo de caso realizado para validar a extensão realizada, a seção 4 apresenta trabalhos relacionados. Por fim na seção 6 são descritas as considerações finais e trabalhos futuros.

2. ESTENDENDO O RUP PARA ATENDER AO MODELO SSE-CMM

O RUP é largamente utilizado em grandes projetos, podendo ser adaptado também a pequenos e médios, além de estar em constante atualização pela sua equipe de desenvolvimento [5].

A segurança é um requisito de qualidade em um sistema e deve ser considerada em todo o ciclo de desenvolvimento. Assim, este trabalho utiliza o SSE-CMM para adaptar o RUP de acordo com as recomendações de segurança deste modelo.

Considerando que, o Modelo SSE-CMM descreve várias recomendações que devem ser seguidas para o desenvolvimento de software seguro, e que disciplinas no RUP visam agrupar coleções de atividades relacionadas a uma área de concentração, identifica-se que a melhor solução é agrupar as atividades propostas para adicionar segurança ao RUP em uma única disciplina chamada de “Segurança de Sistemas”, conforme a Figura 1. Essa disciplina foi elaborada de acordo com as orientações para adaptação do RUP [4], e deverá ser executada em todas as fases, porém, com mais intensidade na fase de iniciação e elaboração. Essa disciplina é uma disciplina de suporte porque se preocupa com gerenciamento de segurança dentro do projeto.

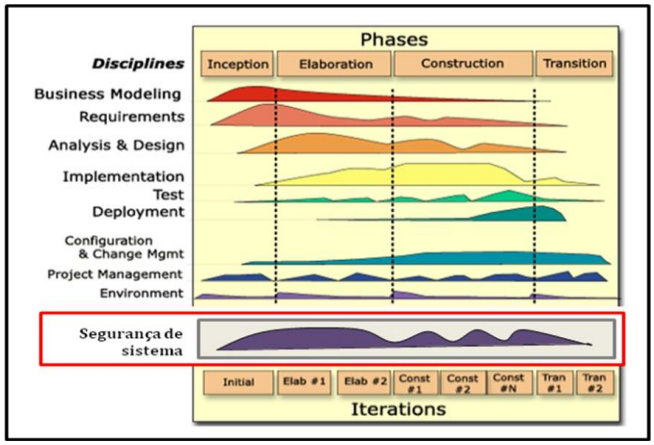

Figura 1. RUP adaptado com a disciplina de segurança

Após uma análise detalhada do Modelo SSE-CMM foi definido um conjunto de atividades com o propósito de contemplar a segurança conforme esse modelo. Essas atividades são organizadas em um diagrama de atividade UML mostrado na Figura 2.

Considerando que no RUP as atividades se referem a um agrupamento de tarefas. Cada atividade deste diagrama é descrita, em diagramas separados, como um conjunto de tarefas que a compõe, os papéis responsáveis por executar cada tarefa e os artefatos de entrada e saída da tarefa. Esse formato de descrição é o padrão adotado pelo RUP.

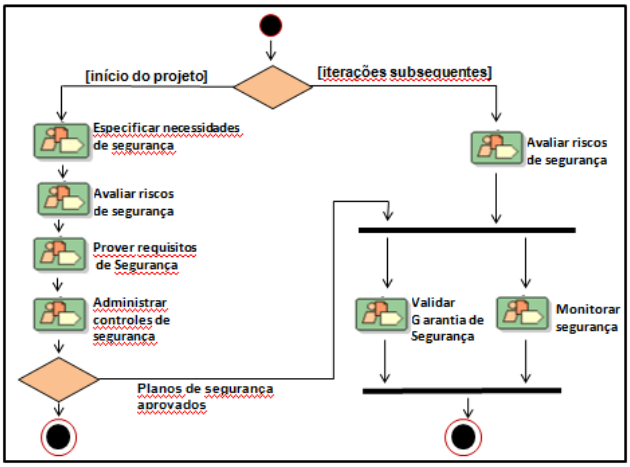

Figura 2. Diagrama de atividade UML com as atividades de segurança

Este trabalho limita-se a demonstração do diagrama de atividades UML pela questão de espaço, porém um detalhamento claro de cada atividade com suas respectivas tarefas, papéis e artefatos foram criadas e podem ser obtidas através da dissertação de mestrado em elaboração com base neste trabalho.

3. ESTUDO DE CASO

Para descrever como deve ser utilizado o modelo RUP adaptado para contemplar a segurança do SSE-CMM será adotado um sistema de cadastro de dados pessoais de clientes para realização do Imposto de Renda anual em uma empresa de contabilidade.

Durante o cadastro dos dados será necessário o uso do bom senso e a ética do profissional, mas uma vez que os dados estão no sistema e a empresa tem acesso a todas as contas, valores, folha de pagamento e notas fiscais de seus clientes a responsabilidade passa a ser do sistema da empresa.

Neste sistema além de serem cadastrados, também são enviados os dados ao governo. No momento do envio dos dados através de transações *web* é que a segurança indicada para o desenvolvimento deve entrar em ação.

Durante a operação de transferência das informações podem ocorrer várias falhas de segurança causadas por vulnerabilidades no sistema, conforme Robertson [6] afirma no resumo de sua tese, a *World Wide Web* envolve desde um serviço para sistemas interconectados tais como documentos estáticos aos quais existe uma plataforma de serviço poderoso, versátil, e amplamente democrático até a entrega de aplicações e disseminação da informação. Infelizmente, com o explosivo crescimento da *web* veio um também um grande crescimento do

número de impactos e incidentes de segurança. Esta magnitude do problema aumentou muito o interesse com que a comunidade de segurança desenvolve esses mecanismos de pesquisa.

Neste sentido, a disciplina de segurança de sistemas proposta neste artigo consiste na realização de uma série de atividades, mostradas na Figura 2, que visam evitar falhas de segurança. A seguir, uma breve descrição da atividade em relação ao estudo de caso específico.

A atividade nomeada "Especificar necessidades de segurança", consiste em identificar as possíveis ameaças que podem vir a acontecer, verificar problemas já ocorridos anteriormente em relação à segurança neste tipo de sistema. Leva-se em conta o fato de que a informação é o ativo mais importante e deve-se assegurar a confidencialidade, disponibilidade, integridade, autenticidade e não repúdio dos usuários destes serviços. Para o sistema de Imposto de Renda pode-se citar ataques de *hackers* à servidores da Receita Federal, o que pode colocar em risco dados de clientes. Recentemente, os servidores da Google foram atacados e o sistema de senha da empresa foi violado [7]. Após identificar os requisitos de segurança, estes são documentados e posteriormente revisados para garantir que satisfazem as necessidades de todos os *stakeholders*. Chega-se a um acordo sobre uma série de definições de segurança baseadas em padrões como são propostas na Norma ISO/IEC 27001.

A atividade "Avaliar riscos de segurança" consiste em identificar ameaças, vulnerabilidades, impactos e riscos que podem vir a ocorrer neste tipo de sistema. Exemplos de riscos de segurança associados ao Sistema de Imposto de Renda incluem: *Cross-site scripting (XSS)* estão entre os ataques mais prevalentes entre as aplicações web [8]*; Cross-site request forgery (CSRF)* [9]; *HTTP header injection* é uma classe de vulnerabilidade que engloba diversas variações [6]; *SQL injection* não é um tipo de ataque específico para a web [9]. Robertson [6] em sua tese afirma que clientes e servidores *Web* têm sido vulneráveis a ataques de injeção de comando. Em particular, as aplicações web que executam programas externos durante o processamento do pedido sem checar corretamente os argumentos do cliente fornecido provaram ser vetores de ataques populares. Essas vulnerabilidades são consideradas graves, já que ações arbitrárias podem ser executadas.

A atividade "Prover requisitos de segurança", consiste em alterar os artefatos "Documento de Arquitetura de Software" e "Especificação de Requisitos de Software" para incorporar os requisitos de segurança identificados para o projeto. Exemplos de requisitos de segurança que podem ser incorporados ao projeto do Sistema da Receita Federal incluem: verificar permissões de acesso as opções do sistema de acordo com o *login* do usuário; verificar se a conexão foi estabelecida no servidor correto no momento de transmissão de dados, verificar se o computador com acesso a *web* que fará o envio para o servidor da receita está seguro, etc.. Em [10], após analisar casos de mal uso, foram identificadas vários tipos possíveis de ameaças, como: revelação de informação sem autorização; alteração de dados sem autorização; Indisponibilidade não autorizada de informações; *Phishing*.

A atividade "Administrar controles de segurança", estabelece as responsabilidades para a realização das atividades relacionadas à segurança, bem como identifica as necessidades de treinamento de acordo com as responsabilidades, e prevê a elaboração de um plano para gerenciamento de configuração de segurança. Para o Sistema do Imposto de Renda, devem ser criados esses artefatos de acordo com o contexto organizacional.

A atividade "Validar garantia de segurança, consiste na elaboração e priorização de atividades que devem ser realizadas para validar os mecanismos de segurança implementados. Estes requisitos de garantia podem ser obtidos através do EAL (*Evaluation Assurance Level*) estabelecido de acordo com as partes interessadas, os *stakeholders*. No caso do Sistema de Imposto Renda, pode-se contratar "hackers", pessoas que não conheçam o sistema para tentar burlá-lo, identificando vulnerabilidades, para que estas possam ser corrigidas antes do sistema ser implantado.

A atividade "Monitorar segurança", consiste em analisar através de *logs* que estão disponíveis as tentativas de violações que ocorreram e responder de forma adequada a esses ataques. Neste caso devem ser levados em consideração os *logs* de tentativas de fraudes que foram realizados e verificar se nenhuma dessas tentativas poderá realmente resultar em um futuro acesso indevido ao sistema.

Por se tratar de um processo iterativo e incremental, serão realizadas várias iterações até se desenvolver o software completo, no início de cada iteração é necessário verificar se as necessidades de segurança continuam válidas para iteração atual e se nenhuma outra necessidade é identificada. Melhorias em relação ao processo utilizado na iteração anterior podem também ocorrer como resultado da avaliação ao final da iteração.

Ao desenvolver o sistema de transferência de dados do Imposto de Renda da Receita Federal é necessário considerar atividades, tarefas e papeis, ou seja, todo o contexto preconizado pelo RUP. A meta principal do desenvolvimento visa realizar a implementação de um sistema que tenha requisitos de segurança. Porém, a utilização do modelo RUP não trata em nenhum momento da segurança como referenciamos através da bibliografia existente, isso faz com que a segurança seja tratada por entremeios das demais disciplinas e fases que o modelos apresenta. Já no RUP adaptado verifica-se a segurança como questão principal da mesma maneira como são tratadas as demais disciplinas.

Entendemos que o nosso estudo de caso é bastante limitado e que esta parte é importante e precisa de elaboração, no entanto, para sermos conclusivo, sabemos que um ou dois estudos de caso não serão suficientes para a validação do modelo, mas sim muitos estudos de caso com o desenvolvimento em diferentes tamanhos de equipes devem ser considerados.

4. TRABALHOS RELACIONADOS

Alguns trabalhos propõem extensões ao RUP para satisfazer requisitos de segurança. Cita-se em especial dois trabalhos.

Paes e Hirata [11] propõem uma extensão ao RUP para contemplar segurança. Esses autores também propõem uma extensão ao RUP para contemplar tolerância a falhas [12].

Em [13] os autores descrevem uma análise realizada de como os processos de gestão COBIT e ITIL, e o modelo de segurança SSE-CMM, podem contribuir para o desenvolvimento de software seguro, destacando também aspectos de sobreposição entre esses modelos em relação à segurança de software.

Os trabalhos citados estão relacionados com segurança, porém não estão baseados em um modelo de segurança como o presente trabalho. Considera-se importante que normas e modelos já consagrados sejam utilizados para a elaboração de processos que visam desenvolver software seguro.

Considerando que a segurança, se proposta através de um modelo consistente, terá resultados mais objetivos e focados no modelo proposto. O usuário terá conhecimento de qual o nível de segurança que estará contemplado no sistema. As tarefas propostas por esse trabalho satisfazem o nível dois do SSE-CMM, pois focam nos problemas de definição, planejamento e desempenho em nível de projeto**.**

5. CONCLUSÃO E TRABALHOS FUTUROS

A segurança na qual é baseado o desenvolvimento de sistemas tem se mostrado cada vez mais importante para a organização, para os desenvolvedores e para seus usuários.

O RUP não descreve atividades, papéis e artefatos para implementação de segurança de forma satisfatória. Sendo assim, esse trabalho visa contribuir, por meio da definição de um processo, para o desenvolvimento de softwares mais seguros, seguindo práticas preconizadas por um modelo bastante utilizado pelas organizações.

Neste sentido o presente trabalho apresenta um modelo do RUP adaptado com uma disciplina extra que contempla a segurança, segundo o modelo SSE-CMM. É muito importante que a segurança seja integrada desde o início do projeto, passando pelas fases de iniciação, elaboração, construção e transição.

A disciplina proposta para contemplar os requisitos de segurança no modelo RUP, foi descrita por meio de um diagrama de atividades que proporciona um entendimento mais amplo e após foram descritos papéis, tarefas e artefatos para atender a segurança demandada pelo modelo SSE-CMM, de acordo com cada atividade a ser realizada.

O processo proposto é útil para empresas que utilizam o RUP e que desejam melhorar seus processos inserindo práticas relacionadas à segurança das informações, para que a incorporação dos requisitos de segurança aos sistemas seja realizada durante o desenvolvimento do mesmo. Empresas que possuem seus próprios processos de software e objetivam o desenvolvimento de software confiável, podem tomar como base as atividades propostas nesse trabalho incorporando-as ao processo organizacional.

Trabalhos futuros incluem a elaboração de uma metodologia para adaptação de processos com base em padrões de segurança e de acordo com requisitos específicos de cada projeto, e a execução dos processos adaptados usando ferramentas de gerência de *workflow*

6. REFERÊNCIAS

[1] Mcafee. (2009) "*Cybercrime cost $1 trillion last year, study"*. Em: ZDNet News & Blogs/Technology News. Disponível em: <http://news.zdnet.com/2100-9595_22-264762.html 1>1 Acesso em nov. 2009.

[2] Ernst & Young. (2008) . "Global Information Security Survey" Em: Ernest & Young Disponível em: <http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf> Acesso em dez. de 2009.

[3] SSE-CMM. (2003) "Systems Security Engineering-Capability Maturity Model Group (SSE-CMM) – Model Description Document". Version 3.0, International Systems Security Engineering Association. Disponível em: <http://www.sse-cmm.org/docs/ssecmmv3final.pdf > Acesso em nov. de 2009.

[4] IBM Corporation. (2007) "IBM Rational Unified Process" v7.0.

[5] Shuja, A. (2008) "Welcome to the IBM Rational Unified Process and Certification". Em: IBM Rational Software. Disponível em: <http://www.ibmpressbooks.com/bookstore/product.asp?isbn=0131562924 > Acesso em jan. de 2010.

[6] Robertson K., W., "Detecting and Preventing Attacks Against Web Applications". Tese de doutorado. Universidade da Califórnia, Santa Barbara (2009).

[7] Gorman S. and Vascellaro J.E. Google Attack Linked To Asian Hackers (2010) Disponível em: http://online.wsj.com/article/SB10001424052748704751304575080362745174130.html

[8] Kiezun A., Guo P., Jayaraman K., Ernst M., (2009) "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks" Em: IEEE Transactions on Software Engineering. University of Washington. EUA.

[9] Alexenko T., Jenne M., Deb Roy S., Zeng W., (2010) "Cross-Site Request Forgery: Attack and Defense" Em: IEEE Transactions on Software Engineering. Universidade de Missouri. Colombia.

[10]Mellado D., Fernández-Medina E., Piattini M., "Un Proceso de Ingeniería de Requisitos de Seguridad en la Práctica" Em: IEEE Transactions on Software Engineering. Universidad de Castilla La-Mancha. Espanha (2007).

[11] Paes, C. E. B. and Hirata, C. M. (2007) "RUP *extension for the development of secure systems"*. Em: ACM Symposium On Applied Computing , Pontifícia Universidade Católica de São Paulo - Instituto Tecnológico de Aeronáutica – São Paulo, Brasil.

[12] Paes, C. E. B., Hirata, C. M. and Yano, E. T. (2008) "*Extending RUP to Develop Fault Tolerant Software"*. Em: Portal ACM. Pontifícia Universidade Católica de São Paulo - Instituto Tecnológico de Aeronáutica – São Paulo, Brasil.

[13] Tovar, E., Carrillo J., Veja V. and Gasca G. (2006) **"***Desarrollo de productos de Software seguros en sintonía con los Modelos SSE-CMM, COBIT e ITIL*". Em: Revista de Procesos y Métricas de las tecnologías de la información. Universidad Católica del Norte - Universidad Politécnica de Madrid. Madrid.