REQUISITOS DE SEGURANÇA EM UM AMBIENTE DE ENSINO A DISTÁNCIA

Cláudia Eliane da Matta[1,2], Denise Nunes Rotondi Azevedo[2]

[1]Instituto Tecnológico de Aeronáutica/Divisão de Ciência da Computação, CTA, Praça Marechal Eduardo Gomes, 50, 12228-900, São José dos Campos, SP[2]Centro Universitário Salesiano de São Paulo – Unidade de Lorena
Rua: Dom Bosco, 184, Centro, Lorena, SP
{claudia,denise.nunes}@lo.unisal.br

Resumo- Este artigo propõe uma especificação para desenvolvimento de ambientes de ensino a distância que levem em conta o quesito segurança. Foram identificados bens a serem protegidos e os agentes de ataque potenciais desse ambiente e aplicada a norma ISO 15408 (*Common Criteria*) visando definir os requisitos de segurança do sistema. O *Common Criteria* pode ser utilizado para desenvolver um sistema seguro ou avaliar a segurança de um sistema já existente; esta última opção foi utilizada neste artigo. A metodologia aplicada levou em consideração as seguintes classes de funcionalidades: proteção de dados de usuários; auditoria; identificação e atenticação; acessos ao sistema suporte para criptografia; repúdio; proteção das funções de segurança; privacidade; gestão de segurança; e utilização de recursos.

Palavras-chave: Segurança, Ensino a Distância

Área do Conhecimento: Ciências Exatas e da Terra

Introdução

No contexto das sociedades contemporâneas, o ensino a distância (EAD) aparece como uma modalidade de educação extremamente adequada e desejável para atender às novas demandas educacionais decorrentes das mudanças na nova ordem mundial.

O EAD vem sendo adotado em diversas instituições nacionais e internacionais, por se tratar de uma forma de ensino mais flexível em relação a horário e local, e um meio de fácil acesso, já que possui um grande alcance, além de ser uma maneira mais rápida de disponibilizar o conteúdo do curso para os alunos, de qualquer lugar do mundo.

Como meio de disseminação do EAD vem sendo utilizada a Internet que, de acordo com Oeiras (1998), quando utilizada em um curso a distância pode tornar mais eficiente a comunicação entre o professor e o aluno e entre os alunos, se comparados com os outros métodos convencionais, como, por exemplo, o correio comum.

Criar um curso a distância pela Internet requer garantia de segurança da informação que envolvem o conteúdo do curso e dados dos alunos.

Existem diversos ambientes de ensino a distância que auxiliam e disponibilizam cursos na Internet, conhecidos por ferramentas de autoria, que além de incluir ferramentas para o desenvolvimento do curso, possuem ferramentas de comunicação, administração e de acompanhamento do aluno durante o curso.

Neste artigo propõe-se realizar uma análise de segurança dessas ferramentas de autoria. A justificativa para realizar esta análise é verificar possíveis falhas e ameaças de segurança e fornecer uma contribuição com sugestões para melhoria do sistema no que se refere ao aspecto de segurança.

Materiais e Métodos

Utilizou-se o ambiente de ensino a distância TelEduc para realizar a identificação dos bens e dos agentes do sistema.

Inicialmente definiram-se os bens, mostrados na Tabela 1. Os bens são informações importantes do sistema, que possuem valor e que podem ser do interesse do agente para leitura, alteração ou destruição.

Tabela 1: Identificação dos Bens e Valores

Bem	Valor
Disponibilidade do Sistema	Impossibilita o bom andamento do curso e do negócio. Impede acesso a *chats* agendados, leituras, execução de provas, atividades, etc.
Integridade do Site (páginas Web)	Impossibilita o bom andamento do curso, através da divulgação de falsas informações (datas de entrega de trabalhos, provas, etc.) ou indisponibilidade de

	determinados serviços.
Integridade do Banco de Dados	Idoneidade e credibilidade dos cursos.
Confidencialidade do Banco de Dados	Dados úteis para concorrentes.
Integridade na tabela Usuário	Passo para outros ataques (captura de senhas). Acesso a dados indevidos, através da mudança de privilégio.
Curso	Parte mais importante do negócio. Direitos autorais.
Informações do curso: Dinâmica do Curso, Agenda, Leituras, Perg. freqüentes, Parada Obrigatória, Mural, Correio, Grupos, Diário de Bordo	Idoneidade e credibilidade dos cursos. Informações falsas ou de valor duvidoso podem ser passadas para os alunos.
Confidencialidade das Notas	Imagem do curso perante o mercado. As notas dos alunos não podem ser visualizadas por pessoas que não participem do curso.
Avaliações (Alteração de Notas)	Informações falsas ou de valor duvidoso podem ser passadas para o coordenador do curso. A empresa fornece a certificação do curso baseada em dados alterados.
Atividades (Material do Curso)	Impossibilita o funcionamento do curso. Nas atividades estão todos os direcionamentos do curso. Dados úteis para concorrentes. Informações falsas ou de valor duvidoso podem ser passadas para os alunos. Direitos autorais.
Material de Apoio (Material do Curso)	Impossibilita a execução do curso. Dados úteis para concorrentes. Informações falsas ou de valor duvidoso podem ser passadas para os alunos. Direitos autorais.
Perda de Comunicação	Impossibilidade de comunicação com os demais alunos do curso.
Privacidade da Comunicação	Acompanhamento indevido de *chats*, de troca de mensagens e de participação aos fóruns.
Perfil do Aluno	Dados úteis para concorrentes. Exposição do e-mail do aluno a e-mails *spam*, caso a tabela que contém o e-mail dos alunos seja acessada.
Portfólio (Material do aluno)	"Cola eletrônica". Direitos autorais.
Acessos (quantidade de acessos do usuário aluno ao sistema)	Informações falsas ou de valor duvidoso podem ser passadas para o coordenador do curso (item pode ser utilizado como uma das formas de avaliação).

A seguir, foram identificados os potenciais agentes de ataque, conforme tabela 2. Entre os agentes de ataque estão também identificados os usuários do sistema descritos pelos seus respectivos perfis.

Tabela 2: Identificação dos Agentes

Categoria	**Descrição**
Usuário Aluno	Utilizam todas as ferramentas disponibilizadas para este perfil.
Usuário Coordenador	Criador do curso, tem acesso a todas as ferramentas disponíveis no ambiente, pode ou não disponibilizar determinadas ferramentas a usuários de outros tipos, moldando seu curso à suas necessidades.
Administrador do Sistema	Total acesso à operação e administração do sistema; responsável pela autorização para criação do curso e envio da senha para o coordenador do curso.
Equipe Desenvolvimento	Desenvolve os códigos, define o esquema de configuração; terá acesso a estas informações.
Concorrente	Sem acesso ao sistema
Hacker	Sem acesso ao sistema

Depois foram identificadas as ameaças ao sistema, mostradas na tabela 3.

Tabela 3: Identificação das Ameaças

Ameaças	**Alvos**
01. Obtenção de Credenciais de Autenticação do Aluno	Privacidade da Comunicação Confidencialidade das Notas Material de Apoio (Material do Curso) Perfil do Aluno Portfólio (Material do aluno)
02. Obtenção de Credenciais de Autenticação do Formador e/ou coordenador do curso	Privacidade da Comunicação. Confidencialidade das Notas Material de Apoio (Material do Curso) Perfil do Aluno Portfólio (Material do aluno) Informações do curso: Dinâmica do Curso, Agenda, Leituras, Perguntas freqüentes, Parada Obrigatória, Mural, Correio,

	Grupos, Diário de Bordo Avaliações (Alteração de Notas) Atividades (Material do Curso)
03. Obtenção de Credenciais de Autenticação do Administrador do Sistema TelEduc	Privacidade da Comunicação. Confidencialidade das Notas Material de Apoio (Material do Curso) Perfil do Aluno Portifólio (Material do aluno) Informações do curso: Dinâmica do Curso, Agenda, Leituras, Perguntas freqüentes, Parada Obrigatória, Mural, Correio, Grupos, Diário de Bordo Avaliações (Alteração de Notas) Atividades (Material do Curso) Base de Dados de Cursos
04. Alteração das permissões do usuário	Confidencialidade das Notas Material de Apoio (Material do Curso) Perfil do Aluno Portifólio (Material do aluno) Informações do curso: Dinâmica do Curso, Agenda, Leituras, Perguntas freqüentes, Parada Obrigatória, Mural, Correio, Grupos, Diário de Bordo Avaliações (Alteração de Notas) Atividades (Material do Curso) Curso
05. Acesso ao Banco de Dados (Cópia do banco de dados, Aquisição da Tabela de Senhas, Alteração das permissões dos usuários, Exclusão de Dados, Inserção de Dados (indevidos)	Disponibilidade do Sistema Integridade do Site (páginas Web) Integridade do banco de dados Integridade na tabela Usuário Curso Informações do curso: Dinâmica do Curso, Agenda, Leituras, Perguntas freqüentes, Parada Obrigatória, Mural, Correio, Grupos, Diário de Bordo Confidencialidade das Notas Avaliações (Alteração de Notas) Atividades (Material do Curso) Material de Apoio (Material do Curso) Perda de Comunicação (correio, fórum, Chat) Privacidade da Comunicação Perfil do Aluno Portifólio (Material do aluno) Acessos (quantidade de acessos ao sistema)
06. Alteração do site de acesso ao curso	Disponibilidade do Sistema Integridade do Site (páginas Web) Curso
07. Quebra de algoritmo	Disponibilidade do Sistema Integridade do Site (páginas Web) Curso Banco de Dados
08. Ataques ao servidor	Disponibilidade do Sistema Integridade do Site (páginas Web) Curso Banco de Dados
09. Indisponibilizar serviços	Disponibilidade do Sistema Curso Banco de Dados
10. Varreduras na rede	Disponibilidade do Sistema Integridade do Site (páginas Web) Curso Banco de Dados
11. Acidentes físicos	Disponibilidade do Sistema Curso Banco de Dados

A criação de uma tabela de ameaças auxilia na identificação das diversas explorações que podem ser usadas em um ataque.

O processo de análise de ameaças é utilizado para determinar os ataques que podem ser esperados e, assim, desenvolver formas de defesa contra esses ataques, embora seja impossível se preparar contra todos os ataques é necessário se precaver contra os mais prováveis.

Resultados

Feitas as identificações dos bens, agentes e ameaças utilizou-se a norma ISO 15408, conhecida como *Common Criteria* (CC) para fornecer um conjunto de critérios que permitem especificar a segurança de uma aplicação utilizada como ambiente de ensino a distância, a partir de características deste ambiente e para definir formas de garantir a segurança da aplicação para o cliente final.

O *Common Criteria* que em português significa Critério Comum para Avaliação de Segurança de Tecnologia da Informação, segundo Albuquerque (2002), pode ser utilizado para desenvolver um sistema seguro ou avaliar a segurança de um sistema já existente.

A seguir são descritos os resultados obtidos desta análise de ameaças e descritas as classes de funcionalidade de segurança que foram utilizadas neste trabalho:

- Proteção de dados de usuários (FDP): deve garantir a política de controle de acesso com base nos privilégios dos usuários;
- Auditoria (FAU): deve ser capaz de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque;
- Identificação e Autenticação (FIA): deve ser capaz de garantir que um usuário, sistema ou informação é mesmo quem alega ser.
- Acessos ao sistema (FTA): deve ser capazes de limitar o acesso a dados de configuração com base em: tipo de conexão;

endereço de conexão;tipo do usuário; hora do dia.

- Suporte para criptografia (FSC): deve realizar operações de criptografia, decriptografia, assinatura eletrônica e verificação de assinatura eletrônica utilizando o protocolo RSA com chave de criptografia de tamanho 1024;
- Repúdio (FC0): deve ser capaz de provar que um usuário executou determinada ação no sistema.
- Proteção das funções de segurança (FPT): além de proteger os dados dos usuários é necessário proteger as funções de segurança; ser capaz de entrar em modo de manutenção quando a recuperação automática após uma falha ou descontinuidade de serviço não seja possível; para falhas ou instalação de novos módulos, ser capaz de garantir o retorno do sistema a um estado seguro, utilizando procedimentos seguros;prover aos usuários autorizados a capacidade de verificar a integridade dos dados daquelas funções; deve fornecer a capacidade para determinar se a violação ocorreu nos dispositivos ou nos elementos das funções de segurança; deve monitorar todos os dispositivos internos da máquina e avisar ao administrador do sistema através de e-mail qualquer alteração efetuada;
- Privacidade (FPR): deve ser capaz de manter incógnito um usuário, impossibilitando a ligação direta da identidade deste com as ações por ele realizadas.
- Gestão de segurança (FMT): deve restringir a habilidade de alterar e remover os dados da trilha de auditoria apenas ao administrador de auditoria; restringir a habilidade de restaurar os dados de configuração de segurança apenas ao administrador de auditoria; especificar um prazo de expiração para as contas cadastradas no sistema de acordo com uma definição feita pelo administrador; ser capaz de encerrar as suas sessões correntes e impedir novos logins após a expiração ter ocorrido.
- Utilização de recursos (FRU): deve garantir o funcionamento dos mecanismos de controle de acesso e registro de trilha de auditoria quando ocorrer uma das seguintes falhas: perda de conexão do servidor, falhas na comunicação, falha no cabeamento; deve garantir o funcionamento de todas as suas funcionalidades quando ocorrer uma das seguintes falhas:falha no aplicativo,perda da integridade nos dados de configuração na memória,perda da integridade dos dados de configuração no disco.

Discussão

Segurança é um requisito básico no desenvolvimento de sistemas. O uso da Internet traz como vantagens a interconexão entre os computadores de todos os portes, o que traz enormes ganhos, mais exige uma segurança muito maior, pois facilita o acesso de *hackers*.

Focalizou-se, neste artigo, os aspectos de segurança para sistemas de EAD que utilizam a Internet, pois a interconexão de redes públicas e privadas e o compartilhamento de recursos, aumenta consideravelmente a probabilidade de ataques aos sistemas para conseguir informações ou para deixar o sistema indisponível.

Os benefícios da realização de uma análise de segurança são: o conhecimento da real situação do sistema e a identificação das medidas de segurança apropriadas.

Conclusão

Este trabalho buscou analisar o sistema de ensino a distância no que se refere aos aspectos de segurança. Foi realizado um trabalho de definição do sistema em questão e de identificação de: ameaças, riscos, agentes de ataque potenciais e bens a serem protegidos. A partir destas identificações foram traçados os objetivos de segurança e foi aplicada ao mesmo a norma ISO 15408 visando definir os requisitos de segurança do sistema.

A partir dos objetivos e requisitos apontados, é possível projetar e implementar tais requisitos de segurança para um sistema de ensino a distância.

Referências

ALBUQUERQUE, Ricardo; Bruno, Ribeiro. Segurança no Desenvolvimento de Software: como garantir a segurança do sistema para seu cliente usando a ISSO/IEC. Rio de Janeiro: Campus, 2002.

MICROSOFT. Modelagem de Ameaças. Disponível em: http://www.microsoft.com/brasil - Acesso em 1 mai. 2006.

OEIRAS, Janne Yukiko Yoshikawa. ACEL: Ambiente Computacional Auxiliar ao Ensino/Aprendizagem a Distância de Línguas. Dissertação de Mestrado. Instituto de Computação. Universidade Estadual de Campinas, 1998.

SCHETINA, Erik; Green, Ken; Carlson, Jacob. Sites seguros: aprenda a desenvolver e construir. Rio de Janeiro: Campus, 2002.