

## Uma ferramenta de Formação a Distância em Segurança de Sistemas da WWW

**Assunto:** Educação a Distância e Segurança em Sistemas da WWW

**Área Temática:** “La formación a distancia y el teleaprendizaje en el sector empresarial”

**Autores:**

Luciano Freire

Regina Borges de Araújo

Departamento de Computação

Universidade Federal de São Carlos - Brasil

A Web e a Internet têm facilitado o fluxo de informações e a interação entre consumidores, empresas e parceiros de negócios. Através de *sites* que realizam transações de comércio eletrônico as pessoas podem adquirir os mais variados produtos nas mais diversas localidades. Utilizando Intranets as empresas têm facilitado o fluxo de informações entre seus funcionários e a automação de processos. Empresas parceiras têm interligado seus sistemas através de Extranets visando facilitar a realização de transações e a troca de informações entre as empresas. Entretanto, o uso destas tecnologias tem aumentado a exposição dos sistemas das empresas ao acesso público, através da Internet e, com isso, aumentado a vulnerabilidade dos seus sistemas de computação e de redes. Assim, uma falha na segurança pode possibilitar o acesso não autorizado de funcionários, parceiros e invasores em geral a informações confidenciais, possibilitando, por exemplo, roubo ou destruição de informações, o que, conseqüentemente, pode levar a prejuízos financeiros. O treinamento de administradores de segurança de sistemas e de redes é hoje um grande desafio, pois a capacitação nesta área exige o domínio de uma vasta e detalhada quantidade de informações que normalmente são dispersas, não relacionadas e dinâmicas, além de demandar experimentação prática.

Neste contexto, o ambiente de ensino aqui proposto provê, além de um conjunto abrangente de informações fundamentais de segurança, um ambiente de experimentação, onde o aluno pode especificar a estrutura desejada de seu ambiente de comércio eletrônico, bem como suas características e componentes, para que o sistema possa avaliar, em tempo-real, através de uma base de regras de validação, as possíveis vulnerabilidades presentes no ambiente além de indicar *checklists* de segurança para cada tipo de componente do ambiente. Desta forma, o aluno pode refletir no ambiente de experimentação o seu próprio ambiente na web, e ter os conhecimentos adquiridos no ambiente do curso avaliados, sob a forma de testes interativos. O treinamento pode ser direcionado, através da especificação de cenários que ampliam a interação do usuário com o ambiente de ensino, melhorando assim o engajamento do aluno no curso.

O ambiente de ensino de segurança de sistemas de comércio eletrônico sendo desenvolvido, possui cinco módulos principais:

- Módulo de provimento de informações fundamentais, que oferece ao administrador uma idéia global dos principais elementos envolvidos na segurança de sistemas;
- Módulo de orientação para a elaboração e implementação de políticas de segurança;
- Cenários ilustrativos de ambientes WWW e os principais pontos sensíveis a ataques e respectivas medidas de proteção;
- Módulo de Avaliação de Cenários Pré-definidos;

- Módulo de Criação de Cenários Personalizados (Ambiente de Experimentação).

O módulo de provimento de informações fundamentais é composto por um conjunto de tópicos contendo informações sobre os seguintes itens: aspectos básicos da segurança (como por exemplo, a definição de conceitos chaves do tipo: ataques, vulnerabilidades e suas origens, auditoria, etc.), vulnerabilidades em sistemas operacionais, softwares, linguagens de programação e protocolos de comunicação; ferramentas e tecnologias de segurança (como *firewalls*, sistemas de detecção de intrusos, criptografia etc.) e informações sobre segurança em sistemas da WWW (*World Wide Web*).

O segundo módulo da ferramenta trata do desenvolvimento de políticas de segurança. Este tem por objetivo orientar o desenvolvimento de políticas de segurança voltadas para ambientes de comércio eletrônico.

Os ambientes de comércio eletrônico são tratados no terceiro módulo (“Cenários ilustrativos de Ambientes WWW”). Este módulo apresenta os componentes específicos de ambientes de comércio eletrônico como, por exemplo, servidores do tipo: *web*, *ftp*, banco de dados, aplicações, etc., além dos principais problemas de segurança que esses sistemas apresentam, através de cenários variados. O objetivo destes cenários é apresentar quais componentes de sistemas de informação na WWW devem ser protegidos e como.

No módulo de avaliação de cenários pré-definidos, cenários variados de sistemas WWW são oferecidos aos alunos que são convidados a responder uma série de perguntas, avaliadas em tempo-real, visando revisar o conhecimento adquirido no curso. Através destas avaliações pode-se direcionar os alunos para determinados tópicos do curso para os quais o aluno não tenha conseguido obter um aprendizado satisfatório.

O módulo de criação de cenários personalizados é composto de uma ferramenta que permitirá ao usuário a especificação de um determinado cenário para que possa ser treinado para atender os requisitos de segurança deste. O módulo é composto dos seguintes componentes:

- Interface Gráfica:** responsável pela interação entre o aluno e a ferramenta. A interface gráfica foi desenvolvida como um *applet* Java e é composta por uma barra de componentes, um painel onde estes componentes podem ser inseridos, além de outro painel (*frame* de uma página *web*) onde será possível ao aluno especificar as propriedades dos componentes e receber informações (relação de vulnerabilidades, *checklists* de segurança, etc.) dos mecanismos de controle e análise da ferramenta. O aluno, no momento da criação do ambiente, deverá escolher os componentes da barra que compõem a sua própria rede, ou outra rede qualquer, e arrastá-los para o painel um a um. Após inserir os componentes de seu ambiente no painel, o aluno deverá indicar as conexões existentes entre os componentes e as suas propriedades. Este procedimento deverá ser repetido até que o ambiente de comércio eletrônico imaginado pelo aluno esteja representado na tela da ferramenta. Durante a especificação do ambiente, este estará sendo validado pelo ambiente de experimentação para garantir a consistência. Depois de finalizada a especificação do ambiente, este será analisado quanto a vulnerabilidades. Para cada componente do ambiente, será indicada *checklists* de segurança correspondentes.
- Regras de Validação e Análise:** conjunto de regras utilizadas para checagem da especificação correta do ambiente e para identificação de possíveis vulnerabilidades no ambiente descrito.

- c) **Mecanismos de controle e análise:** estes mecanismos são responsáveis pelo mapeamento do ambiente especificado sobre a estrutura do banco de dados, além da geração dinâmica de formulários onde o aluno especificará as propriedades de cada componente do ambiente, análise do ambiente em busca de vulnerabilidades e pela identificação dos *checklists* referentes aos componentes do ambiente;
- d) **Base de Dados:** responsável pelo armazenamento do ambiente especificado pelo usuário. O objetivo da base de dados é possibilitar o armazenamento dos ambientes gerados pelos alunos e prover uma representação estruturada desses ambientes na interface que possibilite o processo de análise de segurança.

O curso é responsável por dar uma visão geral da área de segurança de redes e, mais especificamente, de sistemas na WWW, além de suportar a avaliação de ambientes especificados pelo aluno, através de regras de validação, análise e de *checklists* de segurança para cada tipo de componente especificado no ambiente, juntamente com informações sobre as características dos componentes e sobre as técnicas de segurança adotadas nos *checklist*.

Um nível adequado de segurança de sistemas não pode ser conseguido apenas com a aquisição de ferramentas e adoção de tecnologias. Uma política eficaz de segurança, bem como o treinamento adequado dos responsáveis pela segurança do sistema, são questões fundamentais para a sobrevivência de empresas, em especial a das chamadas PontoCom.

Este artigo apresentou um ambiente de ensino de segurança em sistemas de comércio eletrônico, que se diferencia dos demais ambientes de ensino disponíveis tanto no mundo presencial quanto no virtual por oferecer um nível de experimentação que, além de ajudar a consolidar os ensinamentos, tenta motivar os alunos, através da apresentação de cenários, avaliações em tempo-real de cenários pré-concebidos e de cenários personalizados, mantendo-os engajados no curso.