Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística

Plano de Ensino

1) Identificação

Disciplina: INE5680 - Segurança da Informação e de Redes
Turma(s): 08238A, 08238B
Carga horária: 72 horas-aula Teóricas: 44 Práticas: 28
Período: 2º semestre de 2013

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- INE5625 - Computação Distribuída

4) Ementa

Introdução à Segurança. Conceitos básicos. Técnicas clássicas de criptografia. Criptografia Simétrica. Acordo de chave de Diffie-Hellman. Criptografia de Chave Pública. Gerenciamento de chaves públicas. Funções Hash. Assinaturas Digitais. Certificação Digital. Protocolos de Autenticação. Protocolos Criptográficos. Segurança de aplicações. Redes Privadas Virtuais. Tecnologias disponíveis para defesa. Gestão da Segurança da Informação.

5) Objetivos

Geral: Introduzir a área de segurança computacional, com relação as suas subáreas de: segurança da informação, segurança de redes, segurança de sistemas e segurança de aplicações. Estudar técnicas focadas em segurança da informação, capacitando o aluno para o desenvolvimento de sistemas seguros através da modelagem de protocolos para segurança da informação (protocolos criptográficos), além de torná-lo apto à formalização e prova de segurança de protocolos para segurança da informação.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos de criptografia.
- Especificar protocolos criptográficos.
- Empregar ferramentas que servem de suporte à segurança computacional.
- Conhecer os fundamentos para Gestão de Segurança da Informação.
- Desenvolver expressão oral e escrita.

6) Conteúdo Programático

6.1) Apresentação da disciplina e plano de ensino [2 horas-aula]
- Apresentação de tarefa Servidor Web e BD

6.2) Plano de Ensino, Ambientes cooperativos [2 horas-aula]
- O que é Segurança: Informação, Rede, Sistema, Aplicação

6.3) Necessidade de segurança [2 horas-aula]

6.4) Introdução à Segurança da Informação [2 horas-aula]

6.5) Criptografia Simétrica [2 horas-aula]

6.6) Riscos que rondam as organizações [2 horas-aula]
- Os potenciais atacantes
- Vulnerabilidades, Ameaças, Riscos, Ataques, Intrusões [2 horas-aula]
- Os pontos explorados

6.7) Criptografia Assimétrica [2 horas-aula]

6.8) Planejamento e Anatomia de ataques [2 horas-aula]
- Ataques para obtenção de informaçoes
- Ataques de Negação de Serviços Coordenados
- Ataque ativo contra TCP
- Ataques no nível da aplicação

6.9) Varredura de Portas e Serviços [2 horas-aula]
6.10) Funções Hash [2 horas-aula]
6.11) Análise de Vulnerabilidades em Serviços [2 horas-aula]
6.12) Assinatura Digital [2 horas-aula]
6.13) Protocolo de Autenticação de Acesso Remoto [2 horas-aula]
6.14) Infra-estrutura de chaves públicas [2 horas-aula]
6.15) Segurança de Aplicação de Email [2 horas-aula]
6.16) Protocolos criptográficos [2 horas-aula]
6.17) Segurança de servidor web [2 horas-aula]
6.18) Técnicas e Tecnologias disponíveis para defesa [2 horas-aula]
- Firewall
- Proxy
- DMZ
- NAT
- Host de segurança
- Honeypots
- IDS
- Roteador de perímetro
- Política de segurança

6.19) Protocolos básicos [2 horas-aula]
6.20) Redes Privadas Virtuais [2 horas-aula]
6.21) Protocolos intermediários [2 horas-aula]
6.22) Modelo de Segurança em Ambientes Cooperativos [2 horas-aula]
6.23) Protocolos Avançados, Certificados de Atributo [2 horas-aula]
6.24) Apresentação oral de tópicos selecionados pelos alunos [6 horas-aula]
6.25) Aulas práticas [10 horas-aula]
6.26) Tarefas teóricas/práticas [8 horas-aula]

7) Metodologia

Conforme o cronograma indica as datas das aulas, AT=Aula Teórica, TT=Tarefa Teórica, AP=Aula Prática.
Aula 1: AT, TT.
Aula 2: AT, TT, AP.
Aula 3: AT, AP.
Aula 4: AT, AP.
Aula 5: AT, Palestra, TT.
Aula 6: AT, TT.
Aula 7: AT, Palestra, TT.
Aula 8: Avaliação escrita.
Aula 9: AP.
Aula 10: AP.
Aula 11: AP.
Aula 12: AP, Palestra, TT.
Aula 13: AP.
Aula 14: AP.
Aula 15: Apresentação oral da Tarefa 16 pelos alunos. Avaliação Oral.
Aula 16: Apresentação oral da Tarefa 16 pelos alunos. Avaliação Oral.

8) Avaliação

MT = (NT1*P1 + ... + NTn*Pn), onde MT é a média aritmética ponderada entre as notas das tarefas teóricas e práticas; NTi é a nota da iésima tarefa e Pi é o peso da iésima tarefa definido no sistema Moodle.

A média final das avaliações (MF)consistirá das notas obtidas na prova escrita (NPr) e da média ponderada obtida nas tarefas teóricas e práticas realizadas em laboratório ou em casa. MF será calculada conforme:

MF = 0,6*NPr + 0,4*MT

Caso MF >= 6,0 o aluno estará aprovado em primeira instância e sua NF será NF = MF.

Conforme parágrafo 2º do artigo 70 da Resolução 17/CUn/97, o aluno com frequência suficiente (FS) e média final no período (**MF**) entre 3,0 e 5,5 terá direito a uma nova avaliação ao final do semestre (**REC**), sendo a nota final (**NF**) calculada conforme parágrafo 3º do artigo 71 desta resolução, ou seja: **NF = (MF + REC) / 2**.

9) Cronograma

16/08 Aula 1: Plano de Ensino. Questionário sobre experiência dos alunos.
Organização dos Grupos. Novo ambiente de aulas práticas. Introdução à Segurança Computacional: segurança da informação, segurança de redes,
segurança de aplicações, segurança de sistemas. Modelo de Segurança. Protocolo de Segurança, Vulnerabilidades, Ameaças, Riscos, Severidade.
Ataques e tipos de ataques,Intrusões. Requisitos de Segurança. Política de Segurança. Serviços de Segurança. Mecanismos de Segurança. Arquitetura de Segurança. Níveis de Segurança. Visão Geral das Técnicas de Segurança: Criptografia, Usos de Criptografia(confidencialidade, integridade, assinaturas), Certificados, Controle de Acesso, Credenciais. Tarefa 1: Questionário Conceitual.
23/08 Aula 2: Formas de Ocultação de Mensagens: Código, Esteganografia, Técnicas Clássicas de Criptografia: Modelo de Criptosistema Convencional (algoritmo, chave, cifra, criptonálise, tipos de ataques), Aritmética modular. Gerador de Números Aleatórios. Construindo Chaves. Ou Exclusivo. Algoritmos: Técnicas de Substituição, Técnicas de Transposição. Princípios Fundamentais da Criptografia. Conceitos da Teoria da Informação (Difusão, Confusão, Entropia, Segurança Perfeita). Dispositivos de Criptografia (caixas). Algoritmos Criptográficos Simétricos. Modos de Cifra. O que são Funções Hash. Gerenciamento de Chaves Simétricas. Tarefa 2.
30/08 Aula 3: Acordo de Chave Diffie-Hellman. Mais Funções Hash. Criptografia de Chaves Públicas Assinaturas Digitais. Tarefa 3: RSA e GnuPG. Gerenciamento de Chaves Públicas.
06/09 Aula 4: Integridade e Autenticação de Mensagens. Código de Autenticação de Mensagens (MAC). Tarefa 4: Autenticação e Segurança na Comunicação Web (OpenSSL).
13/09 Aula 5: Certificados Digitais. Tarefa 5: Redes Privadas Virtuais (OpenVPN). Infraestrutura de Chaves Públicas. Infraestrutura de Gerenciamento de Privilégios (certificados de atributo). Palestra 1 e Tarefa 6.
20/09 Aula 6: Entrega no Moodle da Tarefa 6: Questionário da palestra 1. Protocolos Criptográficos Básicos.
27/09 Aula 7: Tarefa 7: Exercitando a Notação para Protocolos Criptográficos Básicos. Protocolos Criptográficos Intermediários. Protocolos Criptográficos Avançados. Palestra 2 e Tarefa 8.
04/10 Aula 8: Entrega no Moodle da Tarefa 8: Questionário da palestra 2. Prova 1 (Avaliação da Primeira Parte).

11/10 Aula 9: Tipos de Ataques em Redes. Aplicações e Sistemas. Anatomia de Ataques. Conceito de DMZ. Tarefa 9: Firewall (Iptables, Microtick) e NAT. Sistemas de Detecção de Intrusão (Host, Rede), Honeypots.
18/10 Aula 10: Ferramenta de Reconhecimento de Portas e Serviços (Tarefa 10: Nmap). Ferramenta de Análise de Vulnerabilidades (Tarefa 10: Nessus/OpenVAS).
25/10 Aula 11: Ataques na Web. Ferramenta para Análise de Vulnerabilidades na Web (Tarefa 11: Nikto).
01/11 Aula 12: Sistemas de Detecção de Intrusão (OSSEC, SNORT, Palestra), Tarefa 12: Teste de Penetração com Metasploit.
08/11 Aula 13: Ataques e Tarefa 13: Ferramenta para Avaliação de Segurança de Bancos de Dados.
22/11 Aula 14: Tarefa 14: Ferramentas para Verificação da Segurança em Sistemas.
29/11 Aula 15: Tarefa 15: Apresentação Oral - 13 grupos no máximo (Gestão de Segurança da Informação).
06/12 Aula 16: Continuação da Tarefa 15: Apresentação Oral - 12 grupos no máximo (Avaliação de Ferramentas de Segurança).
09/12 Prova de Recuperação da primeira parte, para casos necessários.

10) Bibliografia Básica

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Pearson.
- Segurança de Redes, Emílio T. Nakamura e Paulo L. de Geus, 4 Edição, Futura.
- Segurança de Dados, Routo Terada, 2 Edição, Editora Blucher, 2008.

11) Bibliografia Complementar

- Redes de Computadores, Tanembaum e Wetherall, 5 Edição, Pearson.
- Diversos e-books da área da disciplina.