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: 40 Práticas: 32
Período: 2º semestre de 2012

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.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos e protocolos criptográficos.
- Empregar ferramentas que servem de suporte à segurança computacional.
- Conhecer os fundamentos para Gestão de Segurança da Informação.
- Escrever artigo para desenvolver a linguagem escrita.
- Apresentar oralmente trabalho sobre tem escolhido.

6) Conteúdo Programático

6.1) Introdução à Segurança Computacional [2 horas-aula]
6.2) Conceitos básicos e técnicas clássicas de criptografia [2 horas-aula]
6.3) Criptografia Simétrica [4 horas-aula]
6.4) Gerenciamento de chaves simétricas [2 horas-aula]
6.5) Acordo Diffie-Hellman, Criptografia e Gerenciamento de Chave Pública [6 horas-aula]
6.6) Funções Hash, Assinatura Digitais [6 horas-aula]
6.7) Infraestrutura de Chaves Públicas e Certificação Digital [6 horas-aula]
6.8) Protocolos criptográficos [6 horas-aula]
6.9) Segurança de Aplicações [4 horas-aula]
6.10) Redes Privadas Virtuais [4 horas-aula]
6.11) Vulnerabilidades, Ameaças e Anatomia e Tipos de Ataques [2 horas-aula]
6.12) Políticas de Segurança [1 horas-aula]
6.13) Protocolos de autenticação, Segurança de acesso remoto [3 horas-aula]
6.14) Tecnologias disponíveis para defesa [6 horas-aula]
6.15) Conectando-se à Internet com segurança [2 horas-aula]
6.16) Modelos de segurança para ambientes cooperativos [2 horas-aula]

6.17) Avaliação escrita da aprendizagem [2 horas-aula]

6.18) Apresentação de tópicos selecionados por grupos [12 horas-aula]
- Gestão de Segurança da Informação
- Segurança de Aplicações e Protocolos Criptográficos
- Ferramentas de segurança
- Outros tópicos de interesse

7) Metodologia

AT-Aula Teórica
AP-Aula Prática (seguindo modelo organizado para aulas-práticas)
TT-Tarefa Teórica (seguindo modelo de relatório apropriado)
TP-Tarefa Prática (seguindo modelo de relatório apropriado)
APP-Apresentação Prática (slides de demo mostrando ferramentas de segurança)
APT-Apresentação Teórica/Prática
Utilização do sistema Moodle para entrega de relatórios:
(seguindo modelo de relatório apropriado)

8) Avaliação

Após as notas das provas P1 e P2, será atribuída ao aluno a média das provas MP=(P1+P2)/2.

Após a conclusão das tarefas teóricas (TT), práticas (TP), orais (APP, APTP) ou realizadas em aulas práticas (AP), será atribuída ao aluno, os percentuais obtidos, que definirão a média das tarefas MT=%T1+....+%TN, considerando-se N tarefas (teóricas (TT), práticas (TP), tarefas em aulas-práticas (AP) e apresentações orais (APP, APT), nas duas partes da disciplina (Segurança da Informação + Segurança de Rede).

A média final MF será calculada como MF = 0,6*MT + 0.4*MP.

1) Se o aluno tiver MF >= 6,00 então será APROVADO e a nota final NF = MF alcançada.

2) Se o aluno tem frequência suficiente (FS) e média final no período (MF) entre 3,0 (inclusive) e 5,5 (< 6,00) terá direito a uma nova avaliação ao final do semestre (REC), sendo a nota final (NF) calculada como NF = (MF + REC)/2.

3) Caso o aluno tenha frequência suficiente (FS), mas MF < 3,00, será REPROVADO e a nota final NF será NF = minimo{MT, MP}, ou seja, será igual ao valor mais baixo entre a média das tarefas teóricas, práticas e orais MT e a média das provas MP.

4) Avaliação das tarefas (TT, AP, TP, APP ou APT): Corresponde a percentuais que correspondem a pesos definidos para as tarefas teóricas, práticas, as realizadas nas aulas práticas ou em apresentações orais, conforme assim estabelecidos, de acordo com o tempo estimado para cada tarefa:

"O seu Ambiente Cooperativo" + "Conceitos Básicos" + "Ex. de Ataque" = (5%)
"Varredura de Portas e Serviços" (10%)
"Análise de Vulnerabilidades em Serviços" (10%)
"Implementação de Protocolo Simplificado de Autenticação" (15%)
"Segurança de Email" (10%)
"Segurança de Servidor Web com SSL" (Prof. Bosco) (10%)
"Redes Privadas Virtuais - VPN" (10%)
"Apresentações de Tópicos Selecionados" (10%)
"Segurança de Aplicação com Servidor Web, segurança para um BD, autenticação e protocolos criptográfico" (20%)

Totalizando a média da tarefas MT = (%T1+ .... + %TN)

Os percentuais acima referidos correespondem a percentuais máximos para cada tarefa, podendo o professor avaliar conforme sua visão quanto ao aproveitamento do aluno, levando em consideração a pontualidade no prazo de entrega das tarefas no sistema Moodle, ou seja, tarefas entregues fora do prazo serão desconsideradas para avaliação. As notas das tarefas serão dadas, até 1 semana depois do prazo de entrega indicado no Moodle, no sentido do professor acompanhar a elaboração das mesmas, podendo ser o aluno solicitado a entregar novamente o relatório de uma tarefa parcial (Prof. Bosco). A tarefa prática solicitada pelo Prof. Zancanella tem, praticamente, seu desenvolvimento durante o período, e sendo entregue ao final do mesmo, sua entrega será definitiva.

As notas de provas e tarefas serão postadas no Moodle.

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

14/09 Apresentação da disciplina e plano de ensino, Introdução à Segurança da Informação,
Apresentação da Tarefa prática "Servidor Web e BD, sem segurança" (AT) (2),
Plano de Ensino, Ambiente cooperativo, O que é Segurança da Informação, de Redes, de Sistemas e de Aplicações (AT) (2).
Tarefa teórica (TT) "O Ambiente Cooperativo e Conceitos Básicos".

21/09 Criptografia Simétrica (AT) (2),
Criptoanálise e Tipos de Ataques. A Necessidade de Segurança (2),

28/09 Criptografia Assimétrica (AT)(2),
Riscos que rondam as organizações: os potenciais atacantes, Vulnerabilidades, Ameaças, Risco, Ataques, Intrusões, Planejamento e Anatomia de ataques (AT) (2). Tarefa Teórica (TT): "Exemplificando Riscos"

05/10 Funções Hash, Assinatura Digital (AT) (2),
Ataques para obtenção de informaçoes, (AT) (2).
Tarefa Prática (TP): "Ferramentas de Aquisição de Informações"
"Ferramentas Scanner de Rede: Varredura de Portas e Serviços".

12/10 10 Infra-estrutura de chaves públicas (AT) (2),
Ataques de Negação de Serviços, Ataque ativo contra TCP, Ataques no nível da aplicação (AT) (2).
Tarefa Prática (TP): "Scanner de Vulnerabilidades".
Aulas no Moodle.

19/10 Prova P1 (4).

26/10 Protocolos criptográficos (AT)(2),
Técnicas e Tecnologias de defesa (AT), Exemplo de Política de Segurança (2)

02/11 Tarefa Prática (TP) "Ferramentas Scanner de Aplicações Web, Segurança de servidor Web com SSL - OpenSSL"
Aula no Moodle. (4)

09/11 Protocolos básicos (AT) (2), VPN (AT) (2).
Tarefa Prática (TP): "VPN".

16/11 Protocolos intermediários (AT) (2),
Modelo de Segurança para um Ambiente Cooperativo (AT) (2).

23/11 Protocolos Avançados, Certificados de Atributo (AT) (2).
Escolha de tema para a apresentação de trabalho sobre o tópico selecionado (Formas de ataques, Ferramentas de Monitoramento ou Ataque, Demo de Ferramentas para Testes de Invasão, Aspectos Éticos ou Jurídicos envolvendo segurança, Forense Computacional, Segurança em Redes sem Fio, Protocolos de Autenticação, Infraestrutura de segurança, Criptografia com Curvas Elípticas, Segurança em redes sem fio), (TP) ou (TT) (2).

30/11 Prática de construção de Protocolos (4)

07/12 Prática de construção de Protocolos (4)

14/12 Prova P2 (4).

21/12 Apresentação de trabalhos práticos (4)

---------- 2013----------
18/02 à 21/02 Apresentação de tarefas práticas na sala do professor (8)

22/02 Prova de Recuperação (4)

25/02 à 28/02 Notas Finais

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

- Segurança e Auditoria em Sistemas de Informação, M. R. Lyra, C. Moderna.
- A Nova Escola de Segurança da Informação, A. Shostack et al. Alta Books.
- Redes de Computadores, Tanenbaum e Wetherall, 5 Edição, Pearson.
- Analysing Computer Security, H. Pfleeger e S. Pfleeger, Prent. Hall, 2012.
- Formal Correctness of Security Protocols, G. Bella, Springer, 2010.