

Instituto de Informática
Departamento de Informática Aplicada

Dados de identificação

Disciplina: SEGURANÇA EM SISTEMAS DE COMPUTAÇÃO

Período Letivo: 2016/2

Período de Início de Validade: 2016/2

Professor Responsável pelo Plano de Ensino: RAUL FERNANDO WEBER

Sigla: INF01045

Créditos: 4

Carga Horária: 60

Súmula

Segurança de dados, em redes e de computadores pessoais. Criptografia de chave única e criptografia de chave pública. Funções de verificação de integridade. Protocolos criptográficos. Principais tipos de ataques à segurança. Principais metodologias e ferramentas utilizadas para impedir ou restringir ataques. Programas daninhos. Características de intrusão e métodos de detecção.

Currículos

Currículos	Etapa Aconselhada	Natureza
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO		Eletiva
ENGENHARIA DE COMPUTAÇÃO	9	Eletiva

Objetivos

Estudar segurança em três aspectos distintos da computação: segurança de dados, segurança em redes e segurança de computadores pessoais. Apresentar os principais tipos de ataques e as principais ferramentas utilizadas para sua prevenção. Permitir que o aluno compreenda e saiba analisar as características de um sistema de computação quanto a sua segurança.

Conteúdo Programático

Semana: 1 Título: Conceituação e Introdução Conteúdo: Significado e consequências de Segurança. Segurança de dados, de redes e de computadores. Tipos de atacantes - ataques ativos e passivos. Intrusão.
Semana: 2 Título: Segurança de dados e criptografia Conteúdo: Modelo de um sistema criptográfico. Criptografia segura (one time pad). Criptografia tradicional e computacional. Algoritmos de chave única (simétrica) e pública (assimétrica).
Semana: 3 Título: Criptografia Tradicional Conteúdo: Métodos de Substituição e Permutação. Cifras monoalfabéticas e polialfabéticas. Cifra de César. Cifra de Substituição. Cifra de Vigenere. Criptoanálise. Máquina Enigma.
Semana: 4 Título: Criptografia de chave única Conteúdo: Exemplo de algoritmos de chave única: DES e IDEA. Criptoanálise linear e diferencial. Algoritmos AES (Mars, Serpent, RC6, Twofish, Rijndael).
Semana: 5 Título: Criptografia de chave pública Conteúdo: Exemplo de algoritmos de chave pública: RSA e El-Gamal. Fundamentação matemática. Complexidade computacional. Funções para o RSA. Teste de primalidade. Biblioteca de grandes números. Assinatura digital. Análise do DSS (Digital Signature Standard). Criptografia de curvas elípticas.
Semana: 6 Título: Funções de hash unidirecionais Conteúdo: Funções de hash unidirecionais e seu uso como Message Digest. Exemplo de algoritmos: RC5 e SHA. Análise de caso de sistema de criptografia: PGP (Pretty Good Privacy). Exercícios práticos.
Semana: 7 Título: Protocolos criptográficos

Conteúdo: Problema do homem no meio. Sistemas de autenticação de usuários. Divisão e compartilhamento de segredos. Sistemas de distribuição de chaves. Exemplo: Kerberos. Votação eletrônica e dinheiro digital.

Semana: 8

Título: Segurança em redes

Conteúdo: Segurança em rede. Protocolos de rede e suas vulnerabilidades. Ataques ao protocolo IP. Análise do IPsec.

Semana: 9

Título: Vulnerabilidades em serviços de redes

Conteúdo: Vulnerabilidades em serviços de redes. Sistema SSL. Sistema SSH. Ataques de Negação de Serviço.

Semana: 10

Título: Varreduras de exploração e de identificação.

Conteúdo: Análise de casos práticos de varreduras de exploração e de identificação.

Semana: 11

Título: Estouro de Buffers

Conteúdo: Estouro de Buffers e Exploração de vulnerabilidades. Programação Segura. Análise de casos práticos.

Semana: 12

Título: Firewalls

Conteúdo: Firewall: Filtro de pacotes e servidores proxies. Estudo de caso. Redes Virtuais Privadas (VPN) e Tradução de Endereços (NAT).

Semana: 13

Título: Política de Segurança

Conteúdo: Política de Segurança: itens a proteger, aspectos relevantes, custo x benefício. Sistemas de Detecção de Intrusão.

Semana: 14 a 15

Título: Casos práticos

Conteúdo: Experiências em laboratório com máquinas virtuais.

Metodologia

A disciplina será desenvolvida através de aulas expositivas, exercícios práticos de criptografia e laboratórios de segurança.

As 60 horas previstas para atividades teóricas e práticas indicadas neste Plano de Ensino incluem 30 encontros de 100 minutos de duração (2 períodos de 50 minutos por encontro, 2 encontros por semana, durante 15 semanas), num total de 3.000 minutos, e mais 10 horas (600 minutos) de atividades autônomas, realizadas sem contato direto com o professor, correspondentes a exercícios e trabalhos extraclasse, conforme Resolução 11/2013 do CEPE/UFRGS, Artigos 36 a 38.

Carga Horária

Teórica: 48

Prática: 12

Experiências de Aprendizagem

Serão realizados 6 trabalhos práticos de criptografia, 6 trabalhos práticos de segurança, além de duas verificações e/ou trabalhos.

Critérios de avaliação

Sendo V1 e V2 as notas das verificações, C a média dos trabalhos de criptografia e S a média dos trabalhos de segurança, a média final é calculada por:

$$M = (V1 + V2 + C + S)/4$$

A conversão da média final M para conceitos é feita por meio da seguinte tabela:

9,0 ≤ M = 10,0: conceito A (aprovado)

7,5 ≤ M < 9,0: conceito B (aprovado)

6,0 ≤ M < 7,5: conceito C (aprovado)

5,0 ≤ M < 6,0: sem conceito (recuperação)

0,0 = M < 4,0: conceito D (reprovado)

Não entrega dos trabalhos práticos (funcionais): conceito D (reprovado)

Faltas > 25%: conceito FF (reprovado)

Atividades de Recuperação Previstas

Recuperação por motivo de saúde: de acordo com o regimento da Universidade, através de processo aberto na Junta Médica da UFRGS, o aluno poderá recuperar as provas ou os trabalhos em data, horário e local a serem marcados pelo professor.

Recuperação de média insuficiente: o aluno com média inferior a 6 mas superior a 4, e que tiver entregue todos os trabalhos da disciplina poderá recuperar o conceito realizando uma prova versando sobre todo o conteúdo do programa, que substitui a menor nota entre as 2 provas. Não há recuperação dos trabalhos

Bibliografia

Básica Essencial

Sem bibliografias acrescentadas.

Básica

Howard, Michael; LeBlanc, David. Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World. Microsoft Press, 2002. ISBN 0735617228.

Menezes, Alfred; van Oorschot, Paul; Vanstone, Scott. Handbook of Applied Cryptography. CRC Press, 1996. ISBN 0849385237.

Schneier, Bruce. Applied cryptography :protocols, algorithms, and source code in c. New York: John Wiley, c1996. ISBN 0471117099.

Stinson, Douglas R.. Cryptography: Theory and Practice. Chapman, 2005. ISBN 1584885084.

Zwicky, Elizabeth; Cooper, Simon; Chapman, D. Brent; Russel, Deborah. Building Internet Firewalls. O'Reilly Media, Inc., 2000. ISBN 1565928717.

Complementar

Sem bibliografias acrescentadas

Outras Referências

Não existem outras referências para este plano de ensino.

Observações

Nenhuma observação incluída.