UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Instituto de Informática - Departamento de Informática Aplicada

Disciplina: Arquitetura e Organização de Computadores I
Código: INF01045
Pré-Requisito: Redes de Computadores e Complexidade de Algoritmos
Carga Horária: 4 horas aula/semana
Créditos: 04 (quatro)
Semestre: 2009/2
Professor: Turma U – Raul Weber

Súmula e 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. Permitir que o aluno compreenda e saiba analisar as características de um sistema de computação quanto a sua segurança.

Conteúdo Programático

Módulo 1 - Criptografia

Aula	Conteúdo
1	Conceituação e Introdução. Significado e conseqüências de Segurança. Segurança de dados, de redes e de computadores. Tipos de atacantes - ataques ativos e passivos. Intrusão.
2	Segurança de dados e criptografia. Modelo de um sistema criptográfico. Criptografia segura (one time pad). Criptografia tradicional e computacional. Algoritmos de chave única (simétrica) e pública (assimétrica).
3	Criptografia tradicional. Métodos de Substituição e Permutação. Cifras monoalfabéticas e polialfabéticas.
4	Cifra de César. Cifra de Substituição. Cifra de Vigenere. Criptoanálise. Máquina Enigma.
5	Exemplo de algoritmos de chave única: DES e IDEA. Criptoanálise linear e diferencial.
6	Algoritmos AES (Mars, Serpent, RC6, Twofish, Rijndaell).
7	Exemplo de algoritmos de chave pública: RSA e El-Gamal. Fundamentação matemática. Complexidade computacional.
8	Funções para o RSA. Teste de primalidade. Biblioteca de grandes números.
9	Assinatura digital. Análise do DSS (Digital Signature Standard). Criptografia de curvas elípticas.
10	Funções de hash unidirecionais e seu uso como Message Digest. Exemplo de algoritmos: RC5 e SHA.
11	Análise de caso de sistema de criptografia: PGP (Pretty Good Privacy). Exercícios práticos.
12	Protocolos criptográficos. Problema do homem no meio. Sistemas de autenticação de usuários. Divisão e compartilhamento de segredos.
13	Sistemas de distribuição de chaves. Exemplo: Kerberos.
14	Votação eletrônica e dinheiro digital.
15	**Primeira verificação.**

Modulo 2 - Segurança

Aula	Conteúdo
1	Segurança em rede. Protocolos de rede e suas vulnerabilidades.
2	Ataques ao protocolo IP. Análise do IPsec.
3	Vulnerabilidades em serviços de redes. Sistema SSL.
4	Sistema SSH.
5	Ataques de Negação de Serviço e Estouro de Buffers. Exploração de vulnerabilidades.
6	Varreduras de exploração e de identificação.
7	Mecanismos de segurança: Firewalls, arquiteturas, componentes e funcionamento.
8	Firewall: Filtro de pacotes e servidores proxies.
9	Firewall: estudo de caso.
10	Análise de casos práticos.
11	Redes Virtuais Privadas (VPN) e Tradução de Endereços (NAT).
12	Sistemas de Detecção de Intrusão.
13	Análise de casos práticos.
14	Comércio Eletrônico: SSL e SET. Certificados digitais.
15	Política de Segurança: itens a proteger, aspectos relevantes, custo x beneficio.
16	Segurança em computadores pessoais. Vírus de computador.
17	**Segunda verificação.**

Total de horas/aula previstas: 60 horas/aula
Horas/aula disponíveis para avaliação: 4 horas/aula

Técnicas de ensino (experiências de aprendizagem):

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

Sistema de Avaliação

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

Divulgação dos resultados

Os prazos para divulgação dos resultados das provas e trabalhos seguirão os seguintes critérios:

- Provas realizadas no sistema Moodle, sem questões dissertativas: divulgação após a realização das provas por todas as turmas.
- Provas realizadas no sistema Moodle, com questões dissertativas: divulgação em até uma semana após a realização das provas por todas as turmas.
- Provas em papel, sem questões dissertativas: divulgação em até duas semanas após a realização das provas por todas as turmas.
- Provas em papel, com questões dissertativas: divulgação em até três semanas após a realização das provas por todas as turmas.
- Trabalhos com correção automática: divulgação em até duas semanas após a entrega dos trabalhos por todas as turmas
- Trabalhos sem correção automática: divulgação em até quatro semanas após a entrega dos trabalhos por todas as turmas
- Situações imprevistas poderão estender os prazos estabelecidos acima.

Freqüência

De acordo com o regimento da UFRGS, é exigida freqüência mínima de 75%.

Atividades de recuperação

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

[Gar96] Garfinkel, Simson e Spafford, Gene. *Practical Unix & Internet Security, 2nd edition*. O'Reilly & Associates, abril 1996, 971p.

[Men96] Menezes, Alfred et al. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathemathics, 1996.

[Sch96] Schneier, Bruce. *Applied Cryptography, 2nd edition*. John Wiley & Sons, 1996, 758 p.

[Zwi00] Zwicky, Elizabeth; Cooper, Simon e Chapman, Brent. *Building Internet Firewalls, second edition*. O'Reilly & Associates, 2000, 870 p.

Notas de aula.

Material selecionado da Internet.