Engenharia de Segurança

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
kalinka@icmc.usp.br

TÓPICOS

- Boas vindas/Apresentação da Professora
- Apresentação do Cronograma/Ritmo
- Apresentação da Bibliografia
- Problemas já identificados
- Reflexões
- Apresentação dos Alunos

APRESENTAÇÃO DA PROFESSORA

- Tecnóloga – FIL
  (Tecnologia em Processamento de Dados)
- Especialista – FIL
  (Análise de Projeto de Sistemas)
- Mestre – ICMC – USP
  (Sistemas Computacionais Distribuídos/Computação Paralela)
- Doutora – ICMC – USP
  (Sistemas Computacionais Distribuídos)
- Livre Docente – ICMC – USP
  (Redes de Computadores)
- Pós-Doutorado – University of Sydney
  (Veículos Aéreos não Tripulados)

ÁREAS DE ATUAÇÃO

- Processamento de Alto Desempenho (PAD)
  - Programação paralela e distribuída
  - *Clusters* & *Grids* Computacionais
  - Escalonamento de processos
- Redes de computadores
  - Ataques/Segurança
  - Mobilidade
- Sistemas embarcados
  - Segurança
  - Mobilidade
  - Veículos autônomos

REGRAS DO "JOGO"

- Princípios básicos:
  - 1) Engenharia de Segurança de redes é uma disciplina importante.
  - 2) O objetivo de todos é entender a disciplina e aprender o conteúdo
    - NÃO é ganhar uma nota
    - NÃO é passar no semestre seguinte
    - NÃO é rodar os alunos… :o)
- Presença:
  - Haverá chamada sistemática (assinatura da lista)
  - O importante é entender os conceitos
  - Eu aconselho fortemente estar presente

REGRAS DO "JOGO"

- Página WEB/bibliografia
  - Moodle (https://edisciplinas.usp.br)
  - Ele não é suficiente (material adicional)
- Durante a aula
  - Prestar atenção/fazer os trabalhos
  - ANOTAR
  - Perguntas interativas
  - Horários de entrada/saída
  - Silêncio
- Provas
  - Tudo pode cair na prova
  - Provas dissertativas?
    - Escrever pouco, claramente, e JUSTIFICAR.
  - Provas práticas?
    - Ser objetivo e direto.

Objetivos da Disciplina

- Familiarizar o aluno com conceitos básicos de segurança computacional e algoritmos criptográficos. Devem ser tratados aspectos práticos.

7

Plano de Ensino

- Conceitos: ameaças, ataques, e recursos; princípios e estratégias de segurança; hacking ético. Criptografia: codificação simétrica para confidencialidade; autenticação de mensagens; codificação com chaves assimétricas; esteganografia. Autenticação: princípios de autenticação de usuários; palavras-chave, tokens, biometria; autenticação remota. Controle de acesso: usuários, objetos, e direitos de acesso; conjunto de direitos de acesso (papeis); controle baseado em atributos de acesso; identidade, credencial, e controle de acesso. Segurança em bancos de dados: ataques por SQL (injection); controle de acesso; criptografia em bancos de dados; inferência sobre dados; segurança em computação de nuvem. Software malicioso: tipos; ameaças persistentes; vírus, worms, spam, trojan, keyloggers, phishing, spyware, backdoors, entre outros; contra-ataque. Ataque por recusa de serviço: flooding, ataques distribuídos, mecanismos de defesa e de resposta. Firewalls: características e políticas de acesso; tipos; configuração. Governança da Internet: definições e esclarecimentos sobre governança da internet. Estudos de caso realizados em aulas práticas.
- Utilização do software NetKit

8

Cronograma de aulas

- 31/07 – Apresentação da Disciplina
- 07/08 – Conceitos Básicos de Segurança
- 14/08 – Ameaças e Vulnerabilidades
- 21/08 – Ameaças e Vulnerabilidades
- 28/08 – Ameaças e Vulnerabilidades
- 11/09 – Criptografia (história, tipos, usos) e Principais Algoritmos Criptográficos (Cryptus)
- 18/09 – Sistemas de Autenticação e Assinatura Digital
- 25/09 – Governança da Internet
- 02/10 – SEMCOMP
- 09/10 – Primeira Prova
- 16/10 – Laboratório de Firewall
- 23/10 – Laboratório de VPNs
- 30/10 – Laboratório de IPSEC-Racoon
- 06/11 – Laboratório de Man in The Middle
- 13/11 – Laboratório de Portscan/HoneyPot
- 20/11 – Segunda Prova
- 27/11 – Sub para quem perder uma das provas

9

Cronograma Criptus

- 11/09 - Introdução a criptografia
- 18/09 - Usos de criptografia
- 25/09 - Algoritmos simétricos
- 22/09 - Algoritmos assimétricos
- 02/10 - Algoritmos desafiadores
- 09/10 - Esteganografia
- 16/10 - Introdução a criptoanálise
- 30/10 - Prova online de criptografia

10

CRITÉRIOS DE AVALIAÇÃO

- 3 Provas + 1 Prova Substitutiva (para quem perder)
- 1 Trabalho Prático

- Cálculo das Notas:
- Média das provas MP = ((2*P1) + (3*P2)+ (1*P3)) / 6
- Média dos trabalhos MT = T1
- Média dos exercícios ME = (E1 + E2+ E3 + E4) / 4

- Média final MF:
- Se MP, ME e MT ≥ 5, então, MF = (0.7 * MP) + (0.3 * (0.7 * MT + 0.3 * ME)).
- Caso contrário, MF = mínimo(MP, MT, ME)

- Frequência mínima (presença) 70%

11

Ritmo/ Datas Importantes

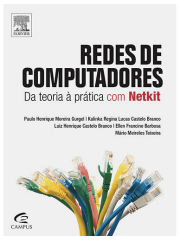
- Aulas
  - Quartas (21:00h as 22:40h) – Sala 5-004
    Laboratório (6-00?)
    Campus I
- Provas
  - 09/10; 20/11 (Sub para quem perder 27/11)
  - Prova *online* 30/10

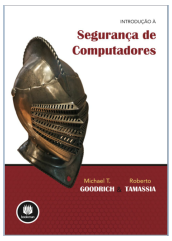
12

BIBLIOGRAFIA BÁSICA

- STALLINGS, W. Criptografia e Segurança de Redes, 4a. Edição – Prentice Hall, 2008.
- ANDERSON, Ross. Security Engineering, 2nd Edition, Willey, 2008.
- Goodrich, M. T. And Tamassia, R. – Introdução à Segurança de Computadores – Bookman Editora LTDA, 2013.
- Gurgel et. Al – Redes de Computadores. Da teoria à prática com Netkit – Editora Campus, 2014. (http://www.lsec.icmc.usp.br/livronetkitbr/)

13





14

Reflexões

- O sucesso é 90% transpiração e 10 % inspiração (Albert Einstein)
- Sucesso = trabalho + persistência + boa orientação + foco

15

Reflexões

- Dedicação aos estudos;
- Respeito e confiança nos professores;
- Trabalho Duro;
- Cordialidade com os colegas;
- Escolham ser vencedores.

16

PROBLEMAS JÁ IDENTIFICADOS

- Falta às aulas;
- Desatenção às aulas;
- Pouco estudo complementar;
- Não fazer exercícios de fixação;
- Pouca leitura/conhecimento complementar;
- Menosprezar o assunto;
- Superestimar a própria inteligência.

17

APRESENTAÇÃO DOS ALUNOS

18