Segurança da Informação
Professor: Raphael Machado

Proposta do Curso e Organização do Conteúdo

Objetivo desta apresentação

- Apresentar o professor/instrutor do curso
- Apresentar os objetivos do curso
- Apresentar a organização e o conteúdo do curso
  - Esta apresentação já funciona como uma "aula 0" onde os primeiros conceitos e ideias serão transmitidos

Sobre o Professor

- Atua na área de segurança desde 2003 (e com TIC desde o milênio passado=)
- Experiência de Pesquisa, Ensino, Governo, Defesa e Mercado
- Não é ”hacker” -> atua em muitas áreas da segurança, mas, atualmente, em mais alto nível

Objetivos do Curso

- Apresentar conceitos fundamentais de Segurança da Informação e a nomenclatura usada na área
- Dar uma visão geral dos métodos de ataque e das ferramentas de defesa
- Fornecer treinamento inicial em Criptografia
- Mostrar como a Segurança da Informação impacta o dia-a-dia das organizações, dos países e das pessoas
- Apresentar tópicos de pesquisa e desenvolvimento na área de Segurança da Informação

Objetivos... Em outras palavras

- Convencer o aluno de que Segurança da Informação...
  - é uma questão real (e que ataques cibernéticos são um problema capaz de grande impacto "real")
  - é um tema transversal, perpassa todas as áreas de negócio (e da sociedade)
  - dá origem a interessantes temas de pesquisa e desenvolvimento
- Apresentar ao aluno os fundamentos e conceitos que o permitirão trabalhar no tema de segurança – ou, pelo menos, compreendê-lo
- Disponibilizar ao aluno ferramentas que permitam-no analisar rigorosamente riscos cibernéticos e modelos de ataque
- Apresentar ao aluno, temas de trabalho, desenvolvimento tecnológico e pesquisa científica na área de segurança

Abordagem do Curso

- Diferentes visões e aplicações de segurança
  - Governo, Mercado, Academia,...
- Curso fortemente orientado a ataques.
  - Muito além de Alice e Bob
- Curso fortemente orientado a padrões.
  - Buscar conhecimento na fonte
- Curso alterna momentos “informativos” e “formativos”
  - Primeira parte é mais “informativa”, enquanto a segunda parte é mais “formativa”

Organização do curso

- Duas partes: Segurança de Sistemas e Criptografia
- Cada parte é organizada em 10 módulos
  - Cada módulo corresponde (aproximadamente=) a uma aula
- Primeira parte: Segurança de Sistemas de Informação
  - Visão mais "prática" da segurança
  - Conceitos, métodos de ataque e ferramentas de defesa
- Segunda parte: Criptografia
  - Presente em (praticamente) toda solução de segurança
    - Inclusive compõe um módulo da primeira parte
  - Arcabouço para análise rigorosa de segurança

Segurança de Sistemas de Informação

1. Motivação e Conceitos Básicos
2. Vulnerabilidade de Software
3. Software Malicioso
4. Ataques DDoS
5. Ameaças Avançadas e Persistentes
6. Criptografia
7. Autenticação de Usuário
8. Controle de Acesso
9. Detecção de Intrusão
10. Firewall e Segurança de Rede

Criptografia

1. Introdução à Criptografia
2. Cifras de Stream e Geradores de Números Aleatórios
3. Data Encryption Standard
4. Advanced Encryption Standard
5. Modos de operação e encriptação múltipla
6. Cifras de chave pública e o RSA
7. Acordo de chaves com Diffie-Hellman
8. Assinatura Digital, Hash, MAC
9. Estabelecimento de Chaves, Certificado Digital, PKI
10. Protocolos de Segurança para Redes e Internet

Site Web

- https://ensinopesquisa.com.br/cursos/seginfo/
- Visão geral do Curso
  - Material didático básico: Segurança de Computadores, Stallings/Brown; Understanding Cryptography, Christof Paar
- Conteúdo por módulo:
  - Objetivo
  - Slides / Vídeo
  - Leitura recomendada
  - Sugestões de vídeos
  - Material complementar

Material Complementar

› Artigos científicos

› Estudos, reportagens, white papers

› Vídeos, Webinars, Podcasts

› Livros de divulgação

› Normas, Guias e Manuais