Sistemas Distribuídos e Criptografia

MEI 2014-2015

Manuel Barbosa

HASLab — INESC TEC e Universidade do Minho

Confiabilidade

Correcção

Integridade

Escalabilidade

Disponibilidade

Confidencialidade

Autenticidade

Elasticidade

Resiliência

Contexto

- **Origem nas antigas UCE**
  Criptografia e Segurança de Sistemas Informáticos
  Sistemas Distribuídos

- **High Assurance Software**

  Confiabilidade: sistema garante conjunto bem definido de requisitos, mesmo na presença de situações de excepção

  Situações de excepção: ataques intencionais + erros de operação e/ou implementação + condições ambientais

- **Objectivos**
  Ênfase em conteúdos profissionalizantes
  Formar peritos em software para Sistemas Confiáveis
  Aplicações: infra-estruturas Cloud e outras infra-estruturas críticas

Estrutura Curricular

UC	Sem	Doc	Horas	Dia	Per
Criptografia e Segurança da Informação (CSI)	1	JBA, **JMV**, MBB	1T / 2TP	2a	M
Paradigmas de Sistemas Distribuidos (PSD)	1	**JOP**, **PSA**, VFF	1T / 2TP	2a	T
Segurança de Sistemas Informáticos (SSI)	2	JBA, **MBB**, **VFF**	1T / 2TP	2a	M
Sistemas Distribuídos Confiáveis (SDC)	2	**JOP**, **RCO**, **CBM**	1T / 2TP	2a	T

Criptografia e Segurança da Informação

- Segurança de um sistema relativa a um modelo de segurança e a dicotomia objectivo de segurança/modelo do atacante.

- Dimensões fundamentais da segurança da informação e primitivas criptográficas que lhes estão associadas.

- Problemas difíceis no contexto da criptografia e teoria de números computacional modernas: prova / redução de segurança.

- Funcionamento interno das técnicas criptográficas mais relevantes e modelos de segurança teóricos para cada técnica criptográfica.

Segurança de Sistemas Informáticos

- Utilizações correntes da criptografia, protocolos comerciais, certificação digital e Public Key Infrastructure.

- Análise de segurança, concepção e implantação de medidas correctivas e mitigadoras, administração de sistemas e perímetros de segurança.

- Técnicas e boas práticas de programação segura.

- Análise forense de sistemas informáticos.

Paradigmas de Sistemas Distribuídos

- Principais paradigmas de programação de sistemas distribuídos.

- Mecanismos distribuídos no middleware empresarial e em plataformas de computação Cloud.

- Planeamento e implementação de sistemas distribuídos

- Combinação e composição de componentes de middleware e de computação em nuvem.

Sistemas Distribuídos Confiáveis

- Fundamentos de sistemas distribuídos: modelação, tempo lógico e observação global, acordo e detecção de faltas.

- Sistemas distribuídos de grande escala: comunicação epidémica, comunicação por publicação/subscrição, arquitecturas peer-to-peer, gestão de dados com coerência eventual.

- Sistemas distribuídos tolerantes a faltas: transacções distribuídas, comunicação em grupo, replicação com coerência forte.

Últimas Notas

- Avaliação em todas as UCs do perfil:
  - teste final (mínimo de 60%)
  - outro elemento de avaliação:
    projectos práticos
    estudo de publicações científicas
    monografias
- Projecto integrador com colaboração da indústria e/ou integração em projectos de R&D
- Visão integrada de todas as actividades do perfil:

  http://www.di.uminho.pt/~mbb/SDC

Perguntas ?