Ciências ULisboa

Tolerância a Intrusões

Código: 425184
ECTS: 6
Ano Letivo: 2015/16
Carga horária: T: 2:00 h; TP: 1:30 h; OT: 2:00 h;
Departamento: Informática
Área Científica: Informática;

Objetivos da Unidade Curricular

Debater os métodos de obtenção de segurança baseados no paradigma da confiabilidade na presença de faltas maliciosas (vulnerabilidades, ataques e intrusões), isto é: detecção e tolerância a intrusões. As competências adquiridas com a disciplina consistem de um corpo de conhecimento complementar à aproximação clássica da prevenção (de intrusões), que requer níveis de robustez de componentes difíceis de conseguir, bem como intervenção humana intensiva e dispendiosa. Os estudantes irão dominar os conceitos fundamentais, paradigmas e mecanismos da tolerância a intrusões. Ficarão igualmente aptos a incorporar estas noções com as noções clássicas de segurança, num projecto completo de sistemas computacionais seguros. Os estudantes que adquiram estas competências são susceptíveis de obter uma vantagem competitiva em relação a investigadores ou profissionais com formação clássica em segurança, dada a aceitação crescente de TI.

Pré-requisitos

- Segurança Informática (26714)
- Segurança (26735)

Conteúdos

Revisão de conceitos fundamentais em segurança e confiabilidade.

Conceitos e terminologia em tolerância a intrusões.

Mecanismos a enquadramentos em TI.

Estratégias para tolerância a intrusões.

Modelação de faltas maliciosas.

Arquitecturas para sistemas tolerantes a intrusões.

Tolerando intrusões.

Resistindo a ataques.

Testando ataques.

Descrição detalhada dos conteúdos programáticos

Componente Teórica

* Revisão de conceitos fundamentais em segurança e confiabilidade.

    Tolerância a faltas e segurança clássicas;

    Confiabilidade como ponto comum.

* Conceitos e terminologia em tolerância a intrusões.

    Modelo AVI; confiança vs. Confiabilidade; cobertura.

* Mecanismos e enquadramentos em TI.

    Enquadramentos e estratégias para a operação TI;

    Tolerância a intrusões baseada em HW e em SW;

    Mecanismos de detecção de intrusões;

    Processamento automático de intrusões.

* Estratégias para tolerância a intrusões.

    Prevenção vs. Tolerância a intrusões;

    Operação confidencial;

    Operação non-stop e reconfigurável;

    Operação recuperável e segura em falha.

* Modelação de faltas maliciosas.

    Hipóteses de falha arbitrária; Hipóteses híbridas de falha.

* Arquitecturas para sistemas tolerantes a intrusões.

    Hipóteses fracas e fortes; Hibridização arquitectural;

Utilizando componentes confiáveis;

Uma arquitectura de referência para TI.

* Tolerando intrusões.

Comunicação resiliente a falhas Bizantinas;

Cripto de limiar e partilha de segredo;

Sistemas de quóruns; Replicação de Máquina de Estados;

Confidencialidade da Informação;

Exemplos de sistemas e projectos em TI.

* Resistindo a ataques.

Falhas por exaustão e Segurança contra Exaustão;

Recuperação Reactiva e Proactiva;

Gestão da diversidade;

Resiliência Proactiva;

Cenários de aplicação.

* Testando ataques.

Perfil de ataques; avaliação de vulnerabilidades.

Componente Teórica-Prática

Pormenores adicionais sobre certos paradigmas.

Alguns algoritmos em detalhe.

Introdução aos trabalhos de projecto.

Estudos de caso.

Leituras e apresentações de artigos.

Componente Prática

Projecto de um sistema baseado em técnicas de tolerância a intrusões, as quais possibilitarão atingir um nível mais elevado e eficiente de confiabilidade através de segurança automática.

O projecto será desenvolvido em duas fases:

I. Ante-projecto de um sistema exibindo os necessários mecanismos de segurança para atingir o nível adequado de prevenção e tolerância a intrusões.

II. Projecto final e demonstração argumentativa da capacidade de abordar os requisitos do trabalho.

Bibliografia

Recomendada

~~Intrusion-Tolerant Architectures: Concepts and Design~~. P. Veríssimo, N. Neves, and M. Correia. An extended version of the paper in: Architecting Dependable Systems. R. Lemos, C. Gacek, A. Romanovsky (eds.), Springer-Verlag LNCS 2677 (2003). Technical Report DI/FCUL TR03-5, Department of Informatics, University of Lisboa (2003). Intrusion-Resilient Middleware Design and Validation. P. Verissimo, M. Correia, N. Neves, P. Sousa. In Annals of Emerging Research in Information Assurance, Security and Privacy Services, H. Rao and S. Upadhyaya (Eds.), Elsevier 2008 .

Outros elementos de estudo

P. Veríssimo e L. Rodrigues, Distributed Systems for System Architects, Kluwer Academic Publishers, 2001, 650pp., review of Fault Tolerance and Security.

Several research and design papers, available on the Web.

Métodos de Avaliação

Regras de classificação:
45% - Projecto e Trabalhos
05% - Participação nas aulas
50% - Exame final

- Eliminatório: Exame Final, Projecto e Trabalhos

* Projecto e Trabalhos práticos
  - Conjunto de estudos de papel e caneta e um projecto em várias fases, distribuídos ao longo do semestre.

* Participação em classe e regularidade
  - Participação activa e a contribuição para os debates estão previstos e serão consideradas.

* Exame Final
  - Exame Final é um exame de 2,5 horas e abrangente.

Língua de ensino

English, or Portuguese if only native speakers