XIV Workshop do LCoN
Edição Especial
'Flash Edition' on Cyber Security Analytics

PROGRAMA PRELIMINAR

Local: LCoN (PPGEE – Mackenzie) **Data**: 10 de Setembro de 2014

Lista de Convidados Externos:

- M.Sc. João Daher Neto
- Dr. Rodrigo Pasti

14.00h-15.00h: Palestra: *Hipercaixas Delimitadoras Aplicadas na Detecção de Intrusos em Redes de Computadores* (M.Sc. João Daher Neto)

Resumo: Essa palestra resume um trabalho de dissertação que apresenta um sistema de classificação supervisionado através da junção de uma técnica de colisão de objetos, AABB, estratégias de quebra de caixas e inferência numérica. Adaptado para n-dimensões e com regras estatísticas de decisão, os experimentos mostraram bons resultados na classificação de conjuntos de dados conhecidos, melhores que algumas técnicas existentes em literatura. O classificador desenvolvido foi uma abordagem inovadora na área de segurança de redes, sendo capaz de analisar características de pacotes da rede e identificar diferentes tipos de intrusos de forma satisfatória.

15.10h-16h10: Palestra: *A Investigação do Cyber Crime em um Contexto de Big Data: Um Estudo de Caso Real por meio de um Sistema de Análise Forense* (Dr. Rodrigo Pasti)

Resumo: O crescimento da Internet ao longo dos anos trouxe um novo cenário ao investigador do *cyber crime*: os incontáveis meios computacionais produzem uma quantidade imensa de dados. Processos investigativos, muitas vezes, estão sujeitos a este contexto de *Big Data*, o que torna o problema de encontrar vestígios e evidências de crimes certamente mais complexo, assim como torna essencial o desenvolvimento de ferramentas de análise de dados voltadas a auxiliar o investigador. Nesta palestra serão apresentados alguns dos desafios que este cenário impõe, assim como propostas de ferramentas e métodos para contorná-los, fundamentados essencialmen-

te nas áreas de Processamento de Linguagem Natural, Aprendizado de Máquina e Computação Natural. O ponto de partida é um estudo de caso real: um sistema de análise forense voltado para grandes quantidades de dados, atualmente em desenvolvimento no Centro de Tecnologia da Informação (CTI). Serão apresentados os primeiros resultados decorrentes da fase inicial do projeto, assim como futuras frentes de pesquisa e desenvolvimento.

16.10h-16.30h: Discussões sobre ações do LCoN: logo, criação de um *suite* de algoritmos, manutenção dos sites (institucional, computação natural, mídias, etc.), LVCoN, matérias para imprensa, Mackenzie Day, etc.

16.30h-18.00h: Confraternização

Anexo I
Biografias dos Convidados

M.Sc. João Daher Neto

Bacharel em Ciência da Computação pela Universidade Federal de Lavras/MG em 2011, atuando com diversos projetos de extensão de inclusão digital em comunidades carentes e breve atuação na área de pesquisa com o projeto de iniciação científica "Algoritmos Imunológicos na Detecção de Intrusos". Mestre em Ciência e Tecnologia da Computação, na área de concentração Matemática Computacional, pela Universidade Federal de Itajubá/MG em 2014, atuando com o projeto de dissertação "Hipercaixas Delimitadoras aplicadas na Detecção de Intrusos em Redes de Computadores". Atualmente trabalhando no Centro de Tecnologia da Informação Renato Archer, em Campinas/SP, como analista desenvolvedor forense, atuando com pesquisa e desenvolvimento de técnicas inteligentes de detecção e prevenção de crimes cibernéticos.

Dr. Rodrigo Pasti

Rodrigo Pasti possui Graduação em Engenharia de Computação pela Universidade São Francisco (2004), Mestrado em Informática pela Universidade Católica de Santos (2007) e Doutorado pela Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas (2013). Atualmente é pesquisador no Centro de Tecnologia da Informação Renato Archer (CTI), onde é bolsista do Programa de Capacitação Institucional do CNPq, e atua em estágio de pós-doutorado no Laboratório de Computação Natural (LCoN) do programa de Pós-Graduação em Engenharia Elétrica da Universidade Presbiteriana Mackenzie. Suas principais linhas de pesquisa são: Computação Natural, Aprendizado de Máquina, Mineração de Dados, Otimização, Pesquisa Operacional, Cyber Segurança e Forense Computacional.