

Hórus: um EWS para Cibersegurança Baseado em Fontes Abertas de Dados

Dia 25/11/2016 das 11:15 às 12:15 horas Sala H- 301

A palestra apresentará o sistema Hórus, um sistema de alerta antecipado (Early Warning System -- EWS) para cibersegurança que vem sendo desenvolvido desde 2014 como resultado das teses de doutorado dos Professores Rodrigo Campiolo e Luiz Arthur. O principal diferencial do Hórus em relação a outros EWS existentes é o suporte a fontes abertas de dados, com destaque para redes sociais. Diversos resultados obtidos com a utilização do Hórus nos últimos anos mostram as vantagens em se monitorar fontes abertas de dados quando o objetivo é antecipar, ou detectar o mais rápido possível, falhas de segurança computacional em uma organização. Esses resultados, bem como os vários problemas de pesquisa relacionados, resolvidos e em aberto, serão apresentados na palestra.



Prof. Daniel Macêdo Batista

Instituto de Matemática e Estatísticas, Universidade de São Paulo

Daniel Batista obteve o título de doutor em Ciência da Computação pela Unicamp em 2010 com uma tese relacionada com escalonamento de tarefas para grades computacionais. Desde 2011 ele é professor no Departamento de Ciência da Computação do Instituto de Matemática e Estatística da USP, onde tem orientado trabalhos de mestrado e doutorado em vários tópicos de redes de computadores: sistemas RFID, segurança da informação, virtualização, computação em nuvem e serviços web. Desde 2015 Daniel é o coordenador do Grupo de Trabalho da RNP GT-EWS, onde coordena a pesquisa e o desenvolvimento do sistema Hórus, um Sistema para Alertas Antecipados baseado em fontes abertas de dados, com o foco em redes sociais.