CONVITE À COMUNIDADE

A Coordenação do Programa de Pós-Graduação em Informática PPGI/UFAM tem o prazer de convidar toda a comunidade para a sessão pública de apresentação de defesa de exame de qualificação de mestrado:

Metamorphic Malware Detection Through Code Dependency Graphs Datasets Indexing

RESUMO: O Metamorfismo é considerado uma das técnicas mais efetivas utilizadas pelos desenvolvedores de malware para evitar que o seu produto seja detectado. Um malware metamórfico, em cada replicação, é capaz de transformar seu próprio código de maneira que resulte em uma nova assinatura não existente nas bases dos antivírus, sem que suas funcionalidades originais sejam prejudicadas. Também é possível criar novos malwares mediante a aplicação de técnicas de metamorfismo em instâncias de malware anteriores. Por causa disso, os sistemas computacionais para a segurança que utilizam assinaturas baseadas em trechos de código de versões anteriores ao metamorfismo apresentam dificuldade na detecção já que o arquivo malicioso altera sua estrutura em cada replicação o que demanda uma rápida e constante atualização das bases. O seguinte trabalho pretende demonstrar como as assinaturas baseadas em grafos de dependências de códigos (CDG) são uma opção viável, visto que representam à semântica e intenção por trás do código, sem importar as modificações obtidas ao aplicar metamorfismo. Este trabalho de pesquisa propõe uma metodologia para identificação de arquivos maliciosos por meio do uso de modelos de indexação de bases de grafos que, dado um vetor de características extraídas do CDG do arquivo analisado, sejam capazes de filtrar grandes bases de CDGs de malwares conhecidos para obter um conjunto reduzido de CDGs que melhor se encaixam com o padrão do arquivo analisado. Este conjunto é, então, usado para calcular o máximo isomorfismo entre cada um dos grafos obtidos e o grafo que é analisado. Tal comparação é baseada em uma medida de similaridade que é usada no processo de classificação, visando atingir uma melhor acurácia e desempenho na detecção de malwares metamórficos

CANDIDATO(A): Luis Miguel Rojas Aguilera

BANCA EXAMINADORA:

Prof. Eduardo James Pereira Souto - PPGI/UFAM (Presidente)
Prof. Eduardo Luzeiro Feitosa - PPGI/UFAM
Prof. Marco Antonio Pinheiro de Cristo - PPGI/UFAM

LOCAL: Sala de Seminários do Instituto de Computação

DATA: 17/03/2016

HORÁRIO: 08:30h

Professor Dr. Eduardo Luzeiro Feitosa
Coordenador do Programa de Pós-Graduação em Informática PPGI/UFAM