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 dissertação:

RIP-ROP: UMA PROTEÇÃO CONTRA ATAQUES DE EXECUÇÃO DE CÓDIGO ARBITRÁRIO BASEADOS EM RETURN-ORIENTED PROGRAMMING

RESUMO: Return-Oriented Programming (ROP) é o nome de uma técnica usada para o desenvolvimento de códigos maliciosos que vem sendo amplamente utilizada para forçar a execução de códigos arbitrários em aplicações vulneráveis. Ela baseia-se na interligação de pequenas frações de código pertencentes aos próprios processos atacados, o que permite a superação de proteções largamente difundidas, como aquela oferecida pelo bit de execução (NX/XD).

Em função de seu vasto emprego em investidas contra sistemas computacionais modernos, proteções contra exploits baseados em ROP têm sido extensamente estudadas. Apesar disso, ainda não se conhece uma solução capaz de aliar eficácia contra todas as modalidades de ROP, eficiência computacional e viabilidade de emprego na proteção de aplicações. Com o intuito de facilitar o entendimento desses requisitos, bem como das implicações inerentes a métodos de proteção contra ataques ROP, este trabalho oferece um levantamento bibliográfico do estado-da-arte envolvendo esse tema. Para isso, são propostas neste trabalho: (i) métricas para avaliação e comparação de proteções contra ataques ROP e (ii) taxonomias para classificação dessas proteções em função das estratégias de bloqueio e das abordagens de implementação utilizadas em cada solução.

Esta dissertação provê ainda um novo método de proteção contra ataques de execução de código arbitrário baseados em ROP que busca abarcar os requisitos de eficácia, eficiência e viabilidade. Demonstrou-se que, através do controle da frequência de instruções de desvio indireto executadas pelas aplicações, é possível distinguir ataques ROP de códigos autênticos e, assim, evitar a sua consolidação.

Em um framework de instrumentação binária dinâmica, foi desenvolvido um protótipo - denominado RIP-ROP - destinado a ambientes Windows e Linux. Experimentos realizados com códigos maliciosos disponíveis em repositórios públicos de exploits confirmaram a viabilidade do modelo proposto para a proteção de aplicações reais. Além disso, o custo computacional imposto pelo RIP-ROP é comparável e, em alguns casos, inferior àquele alcançado por proteções correlatas.

CANDIDATO(A): MATEUS FELIPE TYMBURIBÁ FERREIRA

BANCA EXAMINADORA:

Prof. Eduardo Luzeiro Feitosa - PPGI/UFAM (Presidente)
Prof. Eduardo James Pereira Souto - PPGI/UFAM
Prof. Fernando Magno Quintão Pereira - DCC/UFMG

LOCAL: Sala de Seminários do Instituto de Computação

DATA: 06/08/2014

HORÁRIO: 09:00h

Professora Dra. Eulanda Miranda dos Santos
Coordenadora do Programa de Pós-Graduação em Informática PPGI/UFAM