GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

PALESTRA

Prof. Ricardo Dahab

Universidade Estadual de Campinas (Unicamp)

Palestra: 13/8/2013 às 10:30 – Sala H301

T-DRE: A Hardware Trusted Computing Base for Direct Recording Electronic Vote Machines

(Trabalho conjunto com R. Gallo, H. Kawakami, R. Azevedo,S. Lima e G. Araujo.)

Resumo: We present a hardware trusted computing base (TCB) aimed at Direct Recording Voting Machines (T-DRE), with novel design features concerning vote privacy, device verifiability, signed-code execution and device resilience. Our proposal is largely compliant with the VVSG (Voluntary Voting System Guidelines), while also strengthening some of its reccomendations. To the best of our knowledge, T-DRE is the first architecture to employ multi-level, certification-based, hardware-enforced privileges to the running software. T-DRE also makes a solid case for the feasibility of strong security systems: it is the basis of 165,000 voting machines, set to be used in a large upcoming national election. In short, our contribution is a viable computational trusted base for both modern and classical voting protocols.

Biografia - Ricardo Dahab é professor livre-docente do Instituto de Computação da Universidade Estadual de Campinas, UNICAMP. Tem mestrado pela UNICAMP em Criptografia e doutorado pela Universidade de Waterloo, em Combinatória e Otimização. Seus interesses de docência e pesquisa estão nas áreas de Algoritmos e Protocolos Criptográficos, Segurança da Informação e, em menor escala, Teoria dos Grafos. Foi um dos coordenadores do projeto ICP-EDU, em parceria com a RNP, UFSC, UFMG e Kryptus Tecnologias de Segurança, do qual resultou o primeiro hardware de alta segurança (HSM) totalmente nacional. Esse HSM hoje equipa a autoridade certificadora-raiz da ICP Brasil, da qual participa também como membro do comitê gestor. Têm participado e coordenado projetos de pesquisa e desenvolvimento acadêmicos e com a indústria, na área de autenticação para tecnologia bancária, avaliação de segurança de dispositivos, e implementação eficiente de métodos criptográficos. Junto com as comunidades de Criptografia e Segurança vem cooperando ativamente na consolidação dessas áreas no Brasil e na América Latina, participando da Comissão Especial de Segurança da SBC, da organização de eventos como o SBSeg, a Escola Avançada de Criptografia e o Latincrypt. Iniciou, com outros colegas, a Maratona de Programação da ACM no Brasil, em 1996, que se tornou a Regional Brasileira do ACM International Collegiate Programming Contests. Hoje é diretor destas competições para a América Latina. É pesquisador nivel 2 do CNPq e foi agraciado, em 2011, com o prêmio Zeferino Vaz de Excelência Acadêmica da UNICAMP.