XII Congresso 22 a 24 de setembro de 2004
Interno de Iniciação Científica da UNICAMP
Ginásio Multidisciplinar da UNICAMP

E261

BLINDED-KEY SIGNATURES: ANÁLISE E VERIFICAÇÃO

Rafael Dantas de Castro (Bolsista PIBIC/CNPq) e Prof. Dr. Ricardo Dahab (Orientador), Instituto de Computação - IC, UNICAMP

Blinded-key Signatures foram sugeridas como uma solução parcial para o problema de proteção de chaves privadas hospedadas em agentes móveis. Neste ambiente depara-se com o difícil problema de proteger informações contidas em agentes que executarão em hosts potencialmente maliciosos, mas que precisam ser capazes de gerar assinaturas válidas e verificáveis em nome de seu dono. A técnica aqui abordada foi desenvolvida, inicialmente para o RSA e posteriormente estendida para outros criptossistemas, para proporcionar exatamente isto: segurança e autonomia. Neste trabalho analisamos a proposta original, que apesar de robusta apresenta alguns problemas de segurança inerentes ao seu projeto, como a necessidade de uma exagerada confiança num notário, e, posteriormente, analisamos duas novas propostas de melhorias: Optimistic Blinded-Keys e Double Signatures. Chegamos à conclusão de que esta última era intrinsicamente insegura, mas a anterior é realmente promissora, eliminando os problemas de segurança básicos inerentes à técnica original, mantendo porém o mesmo nível de autonomia. Esta técnica também pode ser estendida a outros esquemas de assinatura como o ElGamal, Schnorr e DSA, mantendo as mesmas propriedades.

Assinatura Digital - Criptografia - Agentes Móveis