Cryptology ePrint Archive: Report 2011/214

On ``identities'', ``names'', ``NAMES'', ``ROLES'' and Security: A Manifesto

Charles Rackoff

Abstract: There is a great deal of confusion in the cryptology literature relating to various identity related issues. By ``names'' (lower case), we are referring to informal, personal ways that we indicate others; by ``NAMES'' (upper case) we are referring to official ways that we use to indicate others. Both of these concepts are often confused with ``identity'', which is something else altogether, and with ``ROLES''. These confusions can lead to insecurities in key exchange as well as in other internet activities that relate to identity. We discuss why we should not use names in protocols and why we \textit{cannot} use identities. We discuss why, in a public-key infrastructure, we need to use NAMES in key-exchange protocols, and how they should be chosen and why they have to be unique, and why we should \textit{not} use NAMES in session protocols. We also argue for the importance of secure ROLEs in key-exchange protocols.

Category / Keywords: cryptographic protocols /

Date: received 26 Apr 2011

Contact author: rackoff at cs toronto edu