POLITECNICO DI TORINO
Repository ISTITUZIONALE

The ForwardDiffSig scheme for multicast authentication

Original
The ForwardDiffSig scheme for multicast authentication / Berbecaru, DIANA GRATIELA; Albertalli, L.; Lioy, Antonio. - In: IEEE-ACM TRANSACTIONS ON NETWORKING. - ISSN 1063-6692. - STAMPA. - 18:6(2010), pp. 1855-1868.

Availability:
This version is available at: 11583/2370848 since:

Publisher:
IEEE

Published
DOI:10.1109/TNET.2010.2052927

Terms of use:
openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

22 September 2019

authors D. Berbecaru, L. Albertalli, A. Lioy

title The ForwardDiffSig scheme for multicast authentication

journal IEEE/ACM Transactions on Networking

ISSN 1063-6692

issue Vol. 18, No. 6, December 2010

pages 1855-1868

DOI 10.1109/TNET.2010.2052927

abstract This paper describes ForwardDiffSig, an efficient scheme for multicast authentication with forward security. This scheme provides source authentication, data integrity, and non-repudiation since it is based on the use of asymmetric cryptography. At the same time, it offers also protection against key exposure as it exploits OptiSum, our optimized implementation of the ISum forward-secure signature scheme. A tradeoff exists in the used keys: Short keys provide speed at the signer, whereas long keys are preferable for long-term non-repudiation. Performance has been evaluated with a custom packet simulator and shows that, by grouping the packets, ForwardDiffSig is efficient in terms of speed even for long keys at the price of a significant signature overhead. Therefore, ForwardDiffSig is fast, exhibits low delay, and provides non-repudiation and protection against key exposure, but has a nonnegligible impact in applications with strict energy or bandwidth constraints.