Scopus

Document details

Back to results | 1 of 1

Export Download Print E-mail Save to PDF Add to List More...

Full Text View at Publisher

Proceedings - 5th International Conference on Computer and Communication Engineering: Emerging Technologies via Comp-Unication Convergence, ICCCE 2014
4 February 2015, Article number 7031662, Pages 300-303
5th International Conference on Computer and Communication Engineering, ICCCE 2014; Sunway Putra HotelKuala Lumpur; Malaysia; 23 September 2014 through 24 September 2014; Category numberE5413; Code 110844

An investigation of Cryptographically Generated Address (CGA) based authentication for mobile IPv6 (Conference Paper)

Qadir, S. ✉, Siddiqi, M.U.

Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur, Malaysia

Abstract

View references (20)

It is well known that the most promising approach to solving the problem of authentication in a mobile IPv6 network is to use CGA-based authentication. The only drawback is that CGA algorithms can be computationally expensive. This study analyses the performance of the CGA generation algorithm and proposes changes to impose a minimal computational security while maintaining reasonable performance. This study also compares the use of Rivest Shamir Ad leman (RSA) signatures with the Merkle Signature Scheme (MSS) for generating CGA Signatures. It finds that using MSS significantly improves the key generation time. However, more work needs to be done to improve both the CGA generation algorithm and MSS in order to make CGA-based authentication an attractive option in MIPv6 setups. © 2014 IEEE.

Author keywords

Authentication Cryptographically Generated Address Merkle Signature Scheme Performance Rivest Shamir Adleman

Indexed keywords

Engineering controlled terms: Cryptography Network security Satellites

Computational security
Cryptographically Generated Address
Generation algorithm
Key generation
Merkle signatures
Mobile IPV6 networks
Performance
Rivest-shamir-adleman

Engineering main heading: Authentication

ISBN: 978-147997635-5
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ICCCE.2014.91
Document Type: Conference Paper
Volume Editors: Gunawan T.S.
Sponsors: Felda Wellness Corporation,Malaysia Convention and Exhibition Bureau (MyCEB),Malaysian Industry-Government Group for High Technology,University Putra Malaysia,Yayasan Kesejanteran Bandar
Publisher: Institute of Electrical and Electronics Engineers Inc.

Find more related documents in Scopus based on:

Authors > Keywords >

References (20)

View in search results format >

All | Export | Print | E-mail | Save to PDF | Create bibliography

1 Sun, H., Song, J., Chen, Z.
Survey of authentication in mobile IPv6 network

(2010) *2010 7th IEEE Consumer Communications and Networking Conference, CCNC 2010*, art. no. 5421695. Cited 3 times.
ISBN: 978-142445176-0
doi: 10.1109/CCNC.2010.5421695

View at Publisher

2 Arkko, J., Vogt, C., Haddad, W.
(2007) *Enhanced Route Optimization for Mobile IPv6*. Cited 45 times.
http://tools.ietf.org/pdf/rfc4866.pdf

3 Aura, T.
Cryptographically Generated Addresses (CGA)

(2003) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2851, pp. 29-43. Cited 38 times.

View at Publisher

4 Bos, J.W., Özen, O., Hubaux, J.-P.
Analysis and optimization of cryptographically generated addresses

(2009) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5735 LNCS, pp. 17-32. Cited 15 times.
ISBN: 3642044735; 978-364204473-1
doi: 10.1007/978-3-642-04474-8_2

View at Publisher

5 Kuang, S., Elz, R., Kamolphiwong, S.
Investigating enhanced route optimization for mobile IPv6

(2008) *13th IEEE Asia-Pacific Computer Systems Architecture Conference, ACSAC 2008*, art. no. 4625457. Cited 6 times.
ISBN: 978-142442683-6
doi: 10.1109/APCSAC.2008.4625457

View at Publisher

6 Arkko, J., Vogt, C., Haddad, W.
(2007) *Enhanced Route Optimization for Mobile IPv6*. Cited 45 times.
http://tools.ietf.org/pdf/rfc4866.pdf

7 Castelluccia, C.
(2004) *Cryptographically Generated Addresses for Constrained Devices*. Cited 2 times.
http://www.inrialpes.fr/planete/splasli/PDF/effcga.pdf

8 Cheneau, T., Boudguiga, A., Laurent, M.
Significantly improved performances of the cryptographically generated addresses thanks to ECC and GPGPU

(2010) *Computers and Security*, 29 (4), pp. 419-431. Cited 15 times.
doi: 10.1016/j.cose.2009.12.008

View at Publisher

9 Auia, T.
(2005) *Cryptographically Generated Addresses (CGA)*. Cited 162 times.
http://tools.ietf.org/pdf/rfc3972.pdf

10 Alsa'deh, A., Cheng, F., Meinel, C.
CS-CGA: Compact and more secure CGA

(2011) *ICON 2011 - 17th IEEE International Conference on Networks*, art. no. 6168492, pp. 299-304. Cited 8 times.
ISBN: 978-145771825-0
doi: 10.1109/ICON.2011.6168492

View at Publisher

11 Alsa'deh, A., Cheng, F., Meinel, C.
Comparison of Key Length (NIST)
http://www.keylength.eom/en/4/

12 Böck, J.
(2011) *RSA-PSS - Provable Secure RSA Signatures and Their Implementation*. Cited 3 times.
http://rsapss.hboeck.de/rsapss.pdf

13 Wang, X.
(2006) *Cryptanalysis on Hash Functions*
https://www.ipa.go.jp/files/000013331.pdf

14 Qadir, S., Siddiqi, M.U., Al-Khateeb, W.F.M.
An investigation of different cryptographic primitives in CGA algorithms
(2013) *Poster Presented at International Research Invention & Innovation Exhibition (IRIIE 2013)*

15 Buchmann, J., Dahmen, E., Szydlo, M.
Hash-based digital signature schemes
(2009) *Post-Quantum Cryptography*, pp. 35-93. Cited 12 times.
[Ed: D.J. Bernstein, J. Buchmann and E. Dahmen], Springer Berlin Heidelberg

16 Becker, G.
(2008) *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*. Cited 10 times.
[PhD Thesis]
http://www.emsec.rab.de/media/crypto/attachments/files/2011/04/becker_1.pdf

17 Dahmen, E., Krau, C.
Short hash-based signatures for wireless sensor networks

(2009) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5888 LNCS, pp. 463-476. Cited 11 times.
ISBN: 3642104320; 978-364210432-9
doi: 10.1007/978-3-642-10433-6_31

View at Publisher

18 Durdağı, E., Buldu, A.
IPV4/IPV6 security and threat comparisons

(2010) *Procedia - Social and Behavioral Sciences*, 2 (2), pp. 5285-5291. Cited 17 times.
doi: 10.1016/j.sbspro.2010.03.862

View at Publisher

19 Alsa'Deh, A., Meinel, C.
Secure neighbor discovery: Review, challenges, perspectives, and recommendations

(2012) *IEEE Security and Privacy*, 10 (4), art. no. 6148204, pp. 26-34. Cited 33 times.
doi: 10.1109/MSP.2012.27

View at Publisher

20 Qadir, S., Siddiqi, M.U., Al-Khateeb, W.F.M.
An investigation of the merkle signature scheme (MSS) for cryptographically generated address (CGA) signatures in mobile IPv6
International Journal of Network Security (IJNS)
in press

‹ Back to results | 1 of 1 ^ Top of page