IETF91
14 November 2014
Honolulu
6man WG

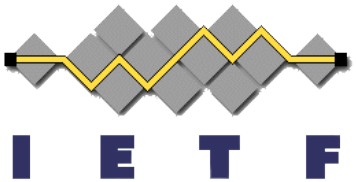
CGA Security Improvement

draft-rafiee-rfc3972-bis-00

Author:

Hosnieh Rafiee
HuaweiTechnologies Duesseldorf GmbH, Munich, Germany

Dacheng Zhang
HuaweiTechnologies, China



Cryptographically Generated Addresses (CGA) – RFC 3972

- **What is CGA**
  - Proof of IP address ownership by finding a binding between public key and IPv6 address of the node
    - Hash (public key | other parameters) and use 64bits of this hash as anIPv6 address of the node
    - Sent with packet: public key and other parameters signed by private key
    - Use some condition to increase the security over 64 bits limit of interface ID: sec value 0 - 7
- **Problem with CGA**
  - All explained in the following documents

    https://tools.ietf.org/html/draft-rafiee-6man-cga-attack-02

Problems & Solutions with CGA - I

- Problem with CGA and SeND specification document
  - Possibility to match CGA generated by sec value 0 to CGA higher sec values
  - Solution: Needs to check with source IP address and target IP address
- RSA weak key size
  - Matching CGA value generated by RSA weak key size with value generated by legitimate node
  - Legitimate node use weak key size that is easily breakable by the attacker
  - Solution: Node should discard any message with weak key sizes

Problems & Solutions with CGA - II

- Variable length prefix
  - Prefix information should be sent by router
  - Less than 64 bits interface ID has high impact on node's security and should be avoided

Question?

- Any suggestion?
- Does WG want to adopt this document?