VANCOUVER

Cga and Send maIntenance BOF

70th IETF meeting

SeND status

- SeND is defined in
  - RFC 3971 - *SEcure Neighbor Discovery*
    - Proposed standard - March 2005
  - RFC 3972 - *Cryptographically Generated Addresses*
    - Proposed standard - March 2005
- As of today, deployment is very limited, but with considerable potential…
- Implementations
  - Cisco
  - DoCoMo
  - Other efforts, not ready yet
- Interop event planned for early 2008

SeND status

- SeND requirement in IPv6 capable products
  - DISA - DoD IPv6 Standard Profiles For IPv6 Capable Products Version 2.0 (FINAL DRAFT – UNCLASSIFIED – Version 2.0 – 01 August 2007)
    - IPsec Capable products SHOULD support RFC 3971, SEcure Neighbor Discovery (SEND) and RFC 3972 Cryptographically Generated Addresses (CGAs).
  - NIST - A Profile for IPv6 in the U.S. Government – Version 1.0
    - RFC 3971 Secure Neighbor Discovery [15] is brought under the Base profile in this USG profile and specified as SHOULD+ for both Hosts and Routers. (CGA are also SHOULD+)

SeND status

- Additional work on SeND since the specs came out:
  - RFC 4892 - *Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)*, Jul 07
  - RFC 4581 - *Cryptographically Generated Addresses (CGA) Extension Field Format*, Oct 06
- Other IETF protocols using CGAs
  - Shim6
    - draft-ietf-shim6-proto-09
    - draft-ietf-shim6-hba-04
  - MIPv6
    - RFC 4866 - Enhanced Route Optimization for Mobile IPv6

CSI bof - Interest so far

- Discussion started in San Diego IETF
  - Int Area meeting presentation by jak
- Some drafts have been submitted
  - draft-kempf-cgaext-ringsig-ndproxy-00.txt
  - draft-jiang-sendcgaext-cga-config-00.txt
  - draft-krishnan-cgaext-send-cert-eku-00.txt
  - draft-krishnan-cgaext-proxy-send-00.txt
  - draft-haddad-cgaext-optisend-00.txt
  - draft-laganier-ike-ipv6-cga-02.txt
  - draft-daley-send-spnd-prob-01.txt
  - draft-van-beijnum-cga-dhcp-interaction-00.txt
  - draft-haddad-cgaext-symbiotic-sendproxy-00
- Some discussion in the CGAext ml and Int area ml:
  - 50 subscriptions

Crypto Agility – Introduction

- RFC 3971 - *SEcure Neighbor Discovery* **LACKS** crypto agility
  - SHA -1 and RSA hardcoded
- RFC 3972 - *Cryptographically Generated Addresses* only **PARTIAL** crypto agility
  - Multiple hash algorithm support defined in RFC 4982
  - RSA hardcoded

Crypto Agility – Introduction

- RFC4270 - *Attacks on Cryptographic Hashes in Internet Protocols*
  - Both authors agree that work should be done to **make all Internet protocols able to use different hash algorithms with longer hash values**. Fortunately, most protocols today already are capable of this; **those that are not should be fixed soon.**
  - **Any new protocol must have the ability to change all of its cryptographic algorithms, not just its hash algorithm.**

Crypto Agility – Proposed Charter Items

- Develop an informational document analyzing the implications of recent attacks on hash functions used by SeND protocol.
  - A.K.A. Bellovin-Rescorla analysis
- Define standard-track extensions to the SeND protocol (RFC3971) to support multiple hash algorithms.
- Specify a standards-track CGA and SeND extensions to support multiple public key algorithms.

Proxy SeND – Introduction

- Proxy ND is covered in
  - RFC4861 - *Neighbor Discovery in IPv6* (section 7.2.8)
  - RFC4389 - *Neighbor Discovery Proxies*
  - RFC3775 - *Mobility Support for IPv6*
- RFC3271 - *SEcure Neighbor Discovery* does not provide protection for Proxy ND

Proxy SeND – Proposed Charter Item

- ✓ Produce a problem statement document for Neighbor Discovery Proxies
- ✓ Specify standards-track SeND Extensions to support Neighbor Discovery Proxies:
- ✓ Extensions to the SeND protocol will be defined in order to provide equivalent SeND security capabilities to ND Proxies.

CGAs and DHCP – Introduction

- CGAs as defined in RFC 3972 are locally generated by the hosts
- How can be used in site that uses DHCP?
- Different interactions:
  - Allow the DHCP server to learn the CGAs
    - IA address option?
  - Allow DHCP server to inform CGA parameters
    - Sec value to be used
    - Other extensions (.g. Multiprefix extension value)
  - Off-loading Modifier generation to the DHCP server
    - For resource constrained hosts and Sec>0
  - Can CGA contribute to DHCP security?

CGAs and DHCP – Proposed charter item

- ✓ Develop an informational document analysing different approaches to allow SeND and CGAs to be used in conjunction with DHCP, and making recommendations on which are the best suited. Recharter based on the result of the analysis

X.509 Extended Key Usage

- RFC 3971 uses general purpose X.509 certificates
  - May have IP address extension
- Not specified the actual permissions over the addresses/prefixes
- Proposed Charter Item:
  - Definition of X.509 Extended Key Usage for SeND.

Updating RFC 3971 and RFC 3972

- Motivations
  - Experience from implementations and interop
  - Changes resulting from additional work done in CSI
  - Moving to draft standard?
- Proposed charter item:
  - Update base specifications (RFC 3971 and 3972), if needed.

Discussion

Charter: http://www.it.uc3m.es/marcelo/CSI_charter.txt

ML: https://www1.ietf.org/mailman/listinfo/cga-ext