802.16 Security TG Proposal

IEEE 802.16 Presentation Submission

Document Number:

IEEE S802.16mgt-04/02

Date Submitted:

2004-05-11

Source:

David Johnston
Intel
2111 NE 25th
Hillsboro, OR 97124

Voice: 503 264 3855
Fax: 503 202 5047
E-mail: dj.johnston@intel.com, david.johnston@ieee.org

Venue:

May 2004 802.16 Interim, Schenzen, China

Base Document:

Purpose:

Proposal to form a security task group within the 802.16 WG.

802.16 Security Enhancement Task Group Proposal

David Johnston, Intel,
dj.johnston@intel.com

Overview

- This presentation
  - Attempts to show a need for new link ciphers to meet immediate and future requirements
  - Attempts to show feasibility for such link ciphers
  - Attempts to show a need for a PKM fix
  - Attempts to show feasibility for such a fix
  - Attempts to justify the formation a Security TG to address these needs

Link Ciphers

- The DES-CBC cipher mode
  - IV preparation is insecure
  - Only provides privacy to a 56 bit key strength
- AES-CCM meets security needs
  - 128 bit key strength
  - Privacy, integrity, authenticity
  - But comes at a cost – 12 bytes per MPDU
- There have been calls for
  - A more efficient cipher (in terms of bytes)
  - A more scaleable cipher (parallel algorithm)
  - A fix to DES mode for existing designs
  - An integrity/authentication only mode

A DES Fix

- It is possible to fix DES-CBC by only changing the IV preparation
  - Works with existing designs that prepare IV in SW
    - Define a synchronous SEQ#
    - Per key, Compute DES_IV_TEK = DES(TEK,0)
    - Per MPDU, compute IV=DES(DES_IV_TEK,SEQ#)
  - This is proven to be secure
  - Doesn’t change frame format
  - Shows feasibility of a DES fix mode

Auth only mode

- Requirements..
  - Base upon FIPS standards
  - Use AES as basic block function

- So use OMAC
  - Lower overhead than CCM
    - Choose number of bits of protection by truncating the ICV
  - Benefits for multicast & MBS services

Fast Link Cipher

- 802.1AF standardizing on GCM
  - Galois Counter Mode
  - Parallelizable
    - Can scale to multi gigabits
  - On track for FIPS
- May meet future needs

PKM

- PKM has issues
  - No mutual auth
    - Rogue basestations
    - MITM Attacks
  - Key exchange is insecure
    - 1 packet DOS attacks
    - SS has to ask, BS can’t initiate
  - Multicast keying has performance implications
    - Swamps contention window
  - EAP support is insufficient
    - No RFC2284bis support (EAP transport reqs)
    - No key binding between authorization and authentication

PKMv2

- PKM is extensible
  - A PKM version is negotiated
  - Easy to add a new PKM (PKMv2)
  - Hard to fix PKMv1 in a backwards compatible way
  - No fast and secure handover
- PKMv2
  - Meets mutual auth needs
  - Provides AAA, cert key binding
  - Provides secure key exchange
  - Provides efficient multicast support
    - Works with both existing multicast features and recent MBS proposals

PKMv2

- PKM is extensible
  - A PKM version is negotiated
  - Easy to add a new PKM (PKMv2)
  - Hard to fix PKMv1 in a backwards compatible way
- PKMv2
  - Pre authentication support via backhaul
  - Meets mutual auth needs
  - Provides AAA, cert key binding
  - Provides secure key exchange
  - Provides efficient multicast support
    - Works with both existing multicast features and recent MBS proposals
  - See PKMv2 Slides

Security and 802.16e

- 802.16e is amending the specification for mobility
  - Security is a related but distinct discipline from mobility
  - 802.16e will be delayed if we try to address all security needs in 802.16e
  - A security TG can
    - Focus on security
    - Meet in parallel with other for efficiecny (PHY, MIBs?)
    - Work to a different timeline than 802.16e

Anticipated Work

- Definition of new link cipher mode
  - Des Fix, OMAC, maybe GCM for future proof
- Definition of PKMv2
  - RFC2284bis, key exchange, mcast, BS certs
- Potentially need to add to the MAC service definition
  - Ability to request a ciphersuite

Security PAR

- Security PAR Purpose
  - Provide confidentiality of user information being transferred over the wireless medium and prevent unauthorized use of 802.16 services.
- Security PAR Scope
  - This document provides enhancements to the IEEE 802.16-RevD/802.16e MAC to provide confidentiality of user data and authorization and authentication between base stations and fixed and mobile subscriber stations.