

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.

Notice:

This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release:

The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.

IEEE 802.16 Patent Policy:

The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <<http://ieee802.org/16/ipr/patents/policy.html>>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <<mailto:chair@wirelessman.org>> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <<http://ieee802.org/16/ipr/patents/notices>>.

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 efficiency (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.