

TSG CORRESPONDENCE

Mr. Nick Yamasaki
Chair, 3GPP2 TSG-S
KDDI
GARDEN AIR TOWER
3-10-10, Iidabashi, Chiyoda-ku
Tokyo 102-8460 Japan
tsgs_chair@3gpp2.org

19 May 2005

Toni Paila
Chair, OMA BAC BCAST
OMA-LIAISON@MAIL.OPENMOBILEALLIANCE.ORG

RE: Integrity Protection in OMA BCAST

Dear Mr Paila,

There is concern that a requirement for integrity protection (authentication) in OMA BCAST will make 3GPP2 BCMCS incompatible with OMA BCAST. This liaison is intended to clarify the incompatibility, explain the reasons behind the 3GPP2 specifications, and provide some suggestions for resolving this issue.

Introduction

It has come to the attention of 3GPP2 TSG-S WG4 (Security) that the OMA BCAST specifications currently state that

“Authentication is MANDATORY for the Broadcast System to use” [1; page 3].

TSG-S would like to inform OMA BCAST that the existing 3GPP2 BCMCS specification [2] conflicts with this requirement. The specification [2] explicitly states

“The SRTP authentication algorithm shall be null” [2; page 55].

There are two reasons for concern:

1. This small (and unnecessary) conflict in requirements will result in the existing BCMCS implementations incompatible with OMA BCAST. Furthermore, upcoming R-UIM specifications will not support generation of authentication keys for BCMCS SRTP.
2. WG4 made a deliberate decision to specify no integrity protection, in order to ensure that BCMCS maintained the highest security (see the following paragraph). Unless WG4 is convinced otherwise, BCMCS specifications will continue to specify that the integrity protection (authentication) algorithm should be null for BCMCS. Consequently, this incompatibility will continue into the future unless either OMA BCAST changes their specifications, or OMA BCAST convinces WG4 to allow integrity protection.

Reasons for the 3GPP2 BCMCS requirement for the authentication algorithm to be null

3GPP2 TSG-S WG4 (Security) spent considerable time discussing the issue of providing integrity protection (authentication) for BCMCS data. This would be analogous to including integrity protection in the OMA BCAST service protection. WG4 examined the existing methods for providing integrity protection, such as the use of Message Authentication Codes (MAC) as used in SRTP and IPSec. The group agreed that all subscribers could access the integrity keys, because the keys would be present in the terminal, which is always assumed to be insecure in 3GPP2. All subscribers would be capable of producing MACs that would appear to have been produced by the service provider. WG4 concluded that the examined methods could not provide integrity protection in a broadcast scenario. To specify a security mechanism that did not provide the claimed protection is considered unwise in the opinion of WG4. Thus, WG4 specified that the integrity protection (authentication) algorithm should be null for BCMCS.

We stress that system considered in this security analysis is the equivalent of OMA BCAST service protection, and the analysis is not expected to extend to BCAST content protection.

Conclusion

The current draft for the OMA BCAST specification is incompatible with the published 3GPP2 BCMCS specification. In order that existing (and future) BCMCS implementations may utilize OMA BCAST, we request that OMA help in resolving this conflict. We have provided two suggestions (below) for resolving this issue.

1. If the OMA BCAST group decides not to mandate that authentication is used, then 3GPP2 requests that the OMA BCAST working group replaces the current requirement with a requirement that will not exclude the use of Broadcast systems that do not use integrity protection.
2. If the OMA BCAST group remains convinced that the OMA specifications should mandate that authentication is used, then 3GPP2 requests the OMA BCAST working group to provide an adequate security analysis to 3GPP2 TSG-S WG4 (Security) in which OMA explains the reasons why the mandate for authentication should remain.

When the time arrives to consider the next upgrade of OMA BCAST and 3GPP2 BCMCS specifications, it will be appropriate for the corresponding organizations to review if the requirements for integrity protection have changed.

[1] OMA-BCAST-2005-0176-LATE-CR-IPsec-and-SRTP-authentication.doc

[2] 3GPP2 X.S0022 "BCMCS in cdma2000 Wireless IP Network"

Regards,

山崎徳和

Nick Yamasaki
Chair, 3GPP2 TSG-S

cc: Y.K. Kim
Vicky Bosserman

Chair, 3GPP2 SC
3GPP2 Sr. Manager

ykim@lgtel.co.kr
vbosserman@tiaonline.org