Title: Response to SC6 N6818: ″Security Services in Support of Routeing Protocols″

Source: IBM

BACKGROUND:

At the July 1991 SC6/WG2 meetings, the UK expressed the position that security mechanisms should be defined in a Network Layer Security Protocol, and that routeing protocols should thus make use of the NLSP to provide security whenever possible, rather than defining protocol-specific methods within the routeing protocol itself.

This UK viewpoint is reflected in the ″Note″ that appears in clause 8.9 of CD 10747 (IDRP). In addition to this note, the UK experts desired comment from other National Bodies, and this request for comment is contained in SC6 N6818.

PROPOSED RESPONSE TO SC6 N6818:

1. *Which security services are desirable for protection of the protocol-specific PDUs of a routeing protocol (such as the BISPDUs of the inter-domain routeing protocol, for example)?*

   ISO 7498-2 lists the following security services that may be provided within the Network layer:

   a. peer entity authentication
   b. data origin authentication
   c. access control service
   d. connection confidentiality
   e. connectionless confidentiality
   f. traffic flow confidentiality
   g. connection integrity without recovery
   h. connectionless integrity

   Correct operation of any routeing protocol depends on receiving ″error-free″ routeing information. Both the inter-domain and the intra-domain routeing protocols incorporate a mandatory checksum on their protocol-specific PDUs in order to accomplish this. In the context of CD 10747, where BISPDUs are carried as the data portion of ISO 8473 NPDUs, ″connectionless integrity″ of BISPDUs is needed.

   In implementing a routeing information exchange protocol, especially in the case of inter-domain routeing where there is no assumption of mutual trust between routeing domains, it is highly desirable to provide peer entity authentication, so that protocol-specific PDUs will be accepted only from a known set of peers. Thus, it is desirable, but not essential, to provide peer entity authentication[1] for BISPDUs.

[1] Since IDRP establishes a connection between neighbor BISs for the purpose of exchanging routeing information, I believe that the term *peer entity authentication* is correct, in preference to the term *data origin authentication*. Regardless of which term we use here, the intent is the same: a BIS wants to verify that it is talking with a known peer.

2. *Should such services be provided by the use of an appropriate Network layer security protocol operating in conjunction with the routeing protocol, or by explicit elements of procedure within the routeing protocols themselves?*

   Since the function of data integrity is critical to the correct operation of a routeing protocol, this function should be provided within the routeing protocol itself. From the perspective of the routeing protocol, it is immaterial whether data integrity was compromised by natural causes (for example, noisy communications links) or a successful security threat. Thus, even if security threats are of no concern, data integrity is still required by the routeing protocol, and methods for providing it should be a mandatory part of its elements of procedure.

   On the other hand, peer entity authentication is of concern only in the context of a perceived security threat. If the peer is trusted, or its identity can be verified by means such as a Network Layer Security Protocol, then there is no need for the routeing protocol itself to define methods to authenticate the peer. Peer entity authentication should at most be an optional function within the routeing protocol; and if present, should be decoupled from the data integrity (checksum) mechanism.

   In summary, if an authentication mechanism is available in a Network layer security protocol which can provide security of the ISO 8473 NPDUs that are the encapsulating medium for the BISPDUs, then it is preferable to use the external protocol. If such an external protocol is not available, then the routeing protocol should provide peer entity authentication as an optional feature.

3. **Practical Considerations:**

   NLSP is much less mature than the routeing protocols, and is likely that CD 10747 will progress to an international standard well before NLSP becomes stable. Hence, we should leave IDRP's functionality "as is" for now: checksums are mandatory, authentication is optional, both are defined within IDRP. Were NLSP further along in its progression cycle, the USA would be amenable to removing authentication from IDRP entirely. However, given today's situation, this would be impractical.

   Since BISPDUs are carried as the data portion of ISO 8473 NPDUs, it follows that all the functionality of a mature NLSP can easily be used to complement IDRP.

   Finally, it is not clear how (or even if) NLSP could be used to protect the protocol-specific PDUs of IS 10589. Further work on NLSP is needed before we can form an opinion on this question.