Frame Relay Forum Technical Committee Contribution

Subject: Requirements for the proposed Frame Relay Privacy I/A (FRF.priv)

Contact: David A. Sinicrope
IBM Corporation
800 Park Offices Drive CE6A/664
Research Triangle Park, NC 27709 USA
+1 (919) 254-1207
FAX: +1 (919) 254-5483
Internet/e-mail: david@raleigh.ibm.com

Date: November 13-14, 1997

Location: San Diego, California

Distribution: Participants in the Frame Relay Forum Technical Committee.

Abstract: This contribution contains the scope and requirements for continued work on the Frame Relay Privacy Implementation Agreement. This contribution reflects the results of the September 9, 1997 Frame Relay Forum Technical Committee adhoc group meeting on Frame Relay Privacy.

Introduction

This contribution contains the scope and requirements for continued work on the Frame Relay Privacy Implementation Agreement. This contribution reflects the results of the September 9, 1997 Frame Relay Forum Technical Committee adhoc group meeting on Frame Relay Privacy. Contributions on Frame Relay Privacy should address the requirements and scope below. Contributions should also address the current level of the Frame Relay Privacy Implementation Agreement (FRF.priv) baseline text.

Scope

The Frame Relay Privacy I/A will limit itself to addressing confidentiality of traffic per VC between two frame relay TEs.

Requirements

1. **Confidentiality and Encryption**
   The principle goal and number one requirement of the privacy I/A is traffic confidentiality. The I/A must limit itself to addressing this as much as possible. Encryption is required, but is only a part of the solution. Other aspects such as authentication and key exchange are also needed and their requirements are described below.

2. **Key Exchange**
   The I/A must address automated key exchange.. This would include both generating secret keys for encryption as well as periodically changing the keys during VC usage. Automated key exchange is crucial to using the restricted key sizes required for export while still providing a reasonable level of privacy.

3. **Authentication**
   Authentication is required to the extent that it is authenticating the frame relay peer device for providing confidentiality. This function is necessary to meeting the confidentiality requirement.

4. **Role or Topological placement**
   The I/A will address end to end function per VC. The I/A protocol(s) are implemented per VC between two frame relay DTEs (e.g., routers, FRADs, controllers, etc.). The internal or external placement of the actual security function are not restricted. (Similar to placement of an external FR/ATM interworking unit.)

5. **SVC and PVC considerations**
   Functions defined for the user plane must be applicable to both PVCs and SVCs. However, other issues related to SVCs, e.g., Closed User Group, and calling party number screening are for further study. The initial release of the I/A will address PVCs only but will not prohibit SVCs.

6. **Government Import/Export Requirements**
   The I/A must be exportable and importable to as many markets, domestic and foreign, as possible. The default encryption algorithm must be exportable and use exportable key sizes. To augment the use of small keys it is recommended that frequent key exchange be specified. Other export regulations must also be met, e.g., key recovery. Import regulation requirements should also be addressed.

7. **Intellectual Property**
   IP law issues must be considered when choosing the algorithms for the required function. License costs and alternatives will be considered.

8. **Hardware and Software requirements**
   Implementation of the algorithms in both hardware and software will be considered when specific algorithms are discussed. It is recommended that selected algorithms that are processing intensive be available in hardware or with hardware assist. Also consideration will be given to requirements that the algorithms be implemented completely in hardware.

9. **Compatibility with current frame relay traffic**
   The I/A protocols and algorithms must work with multiprotocol encapsulated traffic (FRF.3.1/RFC 1490), voice traffic, data compression, fragmentation, etc. The frame format and the order in which the privacy

encodings appear in a frame relative to other protocol encodings must be defined. For example, if data compression and encryption are used on the same VC, the frame is first compressed and then encrypted. The NLPID encodings would reflect this order.

10. **Simplicity**
    In line with the "keep it simple" philosophy of frame relay, the I/A protocols and algorithms must be relatively simple to implement and must capitalize on function already available in the industry. For example, PPP encryption, IP Security, RSA, DES, etc.

11. **Control and negotiation protocol**
    A mode 1/mode 2 approach similar to Data Compression over Frame Relay (FRF.9) is required. Mode 1 would result in the selection of the default algorithm(s) and communicate the parameters needed for the default.

12. **RFC 1490 identified frame format (NLPID encoded)**
    The frame format for frame relay privacy should be NLPID encoded. The multiprotocol encapsulation encoding facilitates reducing system configuration and mixing privacy encoded and non-privacy encoded traffic on the same VC. It also clearly identifies the frame encoding when using frame relay privacy function on multiprotocol encapsulated traffic. For example, for a private, compressed, IP frame, there is clear NLPID identification that the frame is to be decrypted, decompressed and sent to the IP layer protocol.

13. **Selective application to a subset of the VC traffic**
    Frame relay privacy features must be able to be selectively applied to a subset of the VC traffic. More study is needed into the flexibility/complexity tradeoffs.