

NCS TIB 93-8

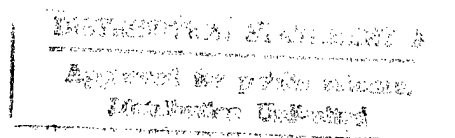


## NATIONAL COMMUNICATIONS SYSTEM

### TECHNICAL INFORMATION BULLETIN 93-8

## SECURITY MEASURES FOR WIRELESS COMMUNICATIONS

MAY 1993



OFFICE OF THE MANAGER  
NATIONAL COMMUNICATIONS SYSTEM  
701 SOUTH COURT HOUSE ROAD  
ARLINGTON, VA 22204-2198

19970117 050

| REPORT DOCUMENTATION PAGE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                        | Form Approved<br>OMB No. 0704-0188                                     |                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------|------------------------------------------------------------------------|-------------------------------------------------------|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.                                                                                                                                                                                                                                                                                                                                                                          |  |                                                        |                                                                        |                                                       |
| 1. AGENCY USE ONLY (Leave blank)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  | 2. REPORT DATE<br>May 1993                             |                                                                        | 3. REPORT TYPE AND DATES COVERED<br>Final Report      |
| 4. TITLE AND SUBTITLE<br><br>Security Measures for Wireless Communications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |                                                        | 5. FUNDING NUMBERS<br><br>DCA100-91-C-0015                             |                                                       |
| 6. AUTHOR(S)<br><br>Nicholas Andre                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |                                                        |                                                                        |                                                       |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Booz, Allen and Hamilton, Inc.<br>8283 Greensboro Drive<br>McLean, Virginia 22102                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                                        | 8. PERFORMING ORGANIZATION<br>REPORT NUMBER                            |                                                       |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>National Communications System<br>Office of Technology and Standards Division<br>701 South Court House Road<br>Arlington, Virginia 22204-2198                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |                                                        | 10. SPONSORING/MONITORING<br>AGENCY REPORT NUMBER<br><br>NCS TIB #93-8 |                                                       |
| 11. SUPPLEMENTARY NOTES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                                        |                                                                        |                                                       |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT<br><br>Approved for public release; distribution is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                        | 12b. DISTRIBUTION CODE                                                 |                                                       |
| 13. ABSTRACT (Maximum 200 words)<br>This report provides architecture planners with information on the availability, capabilities, and other parameters of commercially available security measures supporting wireless communications, identifies common solutions to the security threats in different wireless communication environments, defines the implications of available wireless security services for NS/EP telecommunications, and provides information useful for developing a strategy to ensure that NS/EP security requirements for wireless communications are addressed in the standards-making process. This report describes the results of an analysis and comparison of security services for nine cross-section communication services commonly used by NS/EP personnel. This study is based upon assumed threats to wireless communications. A reliable and continuing assessment of the threats and vulnerabilities to wireless communications and the recommendation of appropriate and effective implementation of countermeasures are beyond the scope of this study. |  |                                                        |                                                                        |                                                       |
| 14. SUBJECT TERMS<br>Public Switched Network (PSN)<br>Wireless Communications<br>National Security/Emergency Preparedness                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                        | 15. NUMBER OF PAGES<br>100                                             |                                                       |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |                                                        | 16. PRICE CODE                                                         |                                                       |
| 17. SECURITY CLASSIFICATION<br>OF REPORT<br>UNCLASS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  | 18. SECURITY CLASSIFICATION<br>OF THIS PAGE<br>UNCLASS |                                                                        | 19. SECURITY CLASSIFICATION<br>OF ABSTRACT<br>UNCLASS |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |                                                        |                                                                        | 20. LIMITATION OF ABSTRACT<br><br>UNLIMITED           |

## GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

**Block 1. Agency Use Only (Leave blank).**

**Block 2. Report Date.** Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

**Block 3. Type of Report and Dates Covered.** State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

**Block 4. Title and Subtitle.** A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

**Block 5. Funding Numbers.** To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

|                             |                                     |
|-----------------------------|-------------------------------------|
| <b>C</b> - Contract         | <b>PR</b> - Project                 |
| <b>G</b> - Grant            | <b>TA</b> - Task                    |
| <b>PE</b> - Program Element | <b>WU</b> - Work Unit Accession No. |

**Block 6. Author(s).** Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

**Block 7. Performing Organization Name(s) and Address(es).** Self-explanatory.

**Block 8. Performing Organization Report Number.** Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

**Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es).** Self-explanatory.

**Block 10. Sponsoring/Monitoring Agency Report Number.** (If known)

**Block 11. Supplementary Notes.** Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

**Block 12a. Distribution/Availability Statement.** Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

**DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."

**DOE** - See authorities.

**NASA** - See Handbook NHB 2200.2.

**NTIS** - Leave blank.

**Block 12b. Distribution Code.**

**DOD** - Leave blank.

**DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.

**NASA** - Leave blank.

**NTIS** - Leave blank.

**Block 13. Abstract.** Include a brief (*Maximum 200 words*) factual summary of the most significant information contained in the report.

**Block 14. Subject Terms.** Keywords or phrases identifying major subjects in the report.

**Block 15. Number of Pages.** Enter the total number of pages.

**Block 16. Price Code.** Enter appropriate price code (*NTIS only*).

**Blocks 17 - 19. Security Classifications.** Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

**Block 20. Limitation of Abstract.** This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

NCS TIB 93-8



# NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 93-8

## SECURITY MEASURES FOR WIRELESS COMMUNICATIONS

MAY 1993

OFFICE OF THE MANAGER  
NATIONAL COMMUNICATIONS SYSTEM  
701 SOUTH COURT HOUSE ROAD  
ARLINGTON, VA 22204-2198

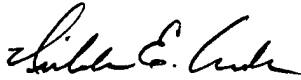
NCS TECHNICAL INFORMATION BULLETIN 93-8

SECURITY MEASURES FOR WIRELESS COMMUNICATIONS

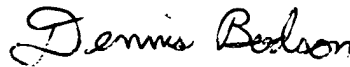
MAY 1993

PROJECT OFFICER

APPROVED FOR PUBLICATION:



NICHOLAS ANDRE  
Computer Scientist  
Office of Technology  
and Standards



DENNIS BODSON  
Assistant Manager  
Office of Technology  
and Standards

FOREWORD

The National Communications System (NCS) is an organization of the Federal Government whose membership is comprised of 23 Government entities. Its mission is to assist the President, National Security Council, Office of Science and Technology Policy, and Office of Management and Budget in:

- The exercise of their wartime and non-wartime emergency functions and their planning and oversight responsibilities.
- The coordination of the planning for and provisions of National Security/Emergency Preparedness communications for the Federal Government under all circumstances including crisis or emergency.

Maximizing the use of commercial networks, especially wireless networks, is a major strategy for future communications supporting National Security/Emergency Preparedness (NS/EP) missions. Wireless communications enhance NS/EP communication capabilities; however, unprotected signals transmitted over wireless links are vulnerable to security threats that can compromise NS/EP information. This report provides information on the applicability of commercially available security measures supporting wireless communications for NS/EP use.

Comments on this TIB are welcome and should be addressed to:

Office of the Manager  
National Communications System  
Attn: NT  
701 S. Court House Road  
Arlington, VA 22204-2198

## TABLE OF CONTENTS

|                                                                           | <u>Page<br/>Number</u> |
|---------------------------------------------------------------------------|------------------------|
| FOREWORD                                                                  |                        |
| EXECUTIVE SUMMARY.....                                                    | ES-1                   |
| <br>1.0 INTRODUCTION .....                                                | 1-1                    |
| 1.1 Background .....                                                      | 1-2                    |
| 1.2 Purpose.....                                                          | 1-3                    |
| 1.3 Scope .....                                                           | 1-3                    |
| 1.4 Organization .....                                                    | 1-4                    |
| <br>2.0 WIRELESS TELECOMMUNICATIONS ENVIRONMENT .....                     | 2-1                    |
| 2.1 Definition of Wireless .....                                          | 2-1                    |
| 2.2 The Wireless Environment .....                                        | 2-2                    |
| <br>3.0 SECURITY THREATS IN A WIRELESS COMMUNICATIONS<br>ENVIRONMENT..... | 3-1                    |
| 3.1 Overview of Security Threats to Wireless Communications.....          | 3-1                    |
| 3.2 Assumed Threats.....                                                  | 3-3                    |
| 3.2.1 Monitoring/Eavesdropping .....                                      | 3-3                    |
| 3.2.2 Traffic Flow Analysis .....                                         | 3-4                    |
| 3.2.3 Masquerading .....                                                  | 3-4                    |
| 3.2.4 Information Modification.....                                       | 3-4                    |
| 3.2.5 Denial of Service .....                                             | 3-5                    |
| 3.3 Countermeasures.....                                                  | 3-5                    |
| 3.3.1 Encrypt the Information.....                                        | 3-5                    |
| 3.3.2 Prevent Pattern Detection.....                                      | 3-7                    |
| 3.3.3 Control Access .....                                                | 3-8                    |
| 3.3.4 Use Trusted Computer Bases .....                                    | 3-8                    |
| 3.4 Required Security Services .....                                      | 3-9                    |
| 3.4.1 Information Confidentiality.....                                    | 3-9                    |

TABLE OF CONTENTS  
(Continued)

|                                                        | <u>Page<br/>Number</u> |
|--------------------------------------------------------|------------------------|
| 3.4.2 Traffic Flow Confidentiality .....               | 3-10                   |
| 3.4.3 Authentication and Access Control.....           | 3-10                   |
| 3.4.4 Information Integrity.....                       | 3-10                   |
| 3.4.5 Trusted Operating Systems.....                   | 3-10                   |
| <br>4.0 SECURITY SYSTEM AND SERVICE REQUIREMENTS ..... | <br>4-1                |
| 4.1 Air-to-Ground Telephone .....                      | 4-1                    |
| 4.2 Cellular Radio.....                                | 4-3                    |
| 4.3 Cordless Telephone.....                            | 4-9                    |
| 4.4 Land-Mobile Radio.....                             | 4-11                   |
| 4.5 Mobile Satellite Systems.....                      | 4-15                   |
| 4.5.1 GEO Mobile Satellite Systems .....               | 4-15                   |
| 4.5.2 LEO Mobile Satellite Systems.....                | 4-16                   |
| 4.6 Paging .....                                       | 4-18                   |
| 4.7 Wireless Local Area Networks .....                 | 4-19                   |
| 4.8 Wireless Private Branch Exchanges .....            | 4-22                   |
| 4.9 Wireless Subscriber Loops .....                    | 4-24                   |
| <br>5.0 FINDINGS.....                                  | <br>5-1                |

ACRONYMS AND ABBREVIATIONS

REFERENCES

GLOSSARY

## LIST OF EXHIBITS

| <u>Exhibit</u>                                                                 | <u>Page<br/>Number</u> |
|--------------------------------------------------------------------------------|------------------------|
| 2-1 Wireless Definition.....                                                   | 2-1                    |
| 2-2 The Wireless Services Environment.....                                     | 2-3                    |
| 3-1 Security Threats to the Wireless Environment.....                          | 3-1                    |
| 3-2 Threats, Countermeasures, and Required Security Services .....             | 3-2                    |
| 3-3 Assumed Threats.....                                                       | 3-3                    |
| 3-4 Countermeasures.....                                                       | 3-6                    |
| 3-5 Required Security Services .....                                           | 3-9                    |
| 4-1 Air-to-Ground Telephone—Methods of Protecting the Wireless<br>Channel..... | 4-2                    |
| 4-2 Security Services for Air-to-Ground Telephone.....                         | 4-3                    |
| 4-3 Air-to-Ground Telephone—Types of Information Protected.....                | 4-4                    |
| 4-4 Security Services for Cellular Radio.....                                  | 4-5                    |
| 4-5 Cellular Radio—Types of Information Protected .....                        | 4-6                    |
| 4-6 Types of Cellular Network Products.....                                    | 4-6                    |
| 4-7 Cellular Radio—Methods of Protecting the Wireless Channel.....             | 4-7                    |
| 4-8 Cellular Radio—Link Versus End-to-End Privacy .....                        | 4-7                    |
| 4-9 Cellular Radio—Price Ranges for Various Security Services.....             | 4-8                    |
| 4-10 Cellular Radio—Distribution of Security Services.....                     | 4-8                    |
| 4-11 Security Services for Cordless Telephones.....                            | 4-10                   |
| 4-12 Cordless Telephone—Types of Information Protected.....                    | 4-10                   |
| 4-13 Cordless Telephone—Methods of Protecting the Wireless Channel.....        | 4-11                   |
| 4-14 Types of Land-Mobile Radio Products.....                                  | 4-12                   |
| 4-15 Security Services for Land-Mobile Radio .....                             | 4-12                   |
| 4-16 Land-Mobile Radio—Distribution of Security Services .....                 | 4-13                   |
| 4-17 Land-Mobile Radio—Types of Information Protected.....                     | 4-14                   |
| 4-18 Land-Mobile Radio—Methods of Protecting the Wireless Channel.....         | 4-14                   |
| 4-19 Security Services for GEO Satellite Systems.....                          | 4-16                   |
| 4-20 GEO Satellite Systems—STU-III Compatibility .....                         | 4-17                   |



**LIST OF EXHIBITS**  
**(Continued)**

| <u>Exhibit</u>                                                                   | <u>Page</u><br><u>Number</u> |
|----------------------------------------------------------------------------------|------------------------------|
| 4-21 Security Services for LEO Satellite Systems .....                           | 4-17                         |
| 4-22 LEO Satellite Systems—Types of Information Protected.....                   | 4-18                         |
| 4-23 LEO Satellite Systems—STU-III Compatibility .....                           | 4-19                         |
| 4-24 Security Services for Wireless LANs.....                                    | 4-21                         |
| 4-25 Wireless LANs—Types of Information Protected.....                           | 4-21                         |
| 4-26 Wireless LANs—Methods of Protecting the Wireless Channel .....              | 4-22                         |
| 4-27 Security Services for Wireless PBXs .....                                   | 4-23                         |
| 4-28 Wireless PBXs—Types of Information Protected.....                           | 4-24                         |
| 4-29 Wireless PBXs—Methods of Protecting the Wireless Channel.....               | 4-25                         |
| 4-30 Security Services for Wireless Subscriber Loops.....                        | 4-26                         |
| 4-31 Wireless Subscriber Loop—Methods of Protecting the Wireless<br>Channel..... | 4-26                         |
| 4-32 Wireless Subscriber Loop—Types of Information Protected.....                | 4-27                         |

## EXECUTIVE SUMMARY

The Office of the Manager, National Communications System (OMNCS) is responsible for coordinating plans and provisions for National Security and Emergency Preparedness (NS/EP) communications during crises or emergencies. Wireless access to commercial communication networks is becoming an increasingly available and attractive option for supporting NS/EP missions. Unprotected signals transmitted over wireless links, however, are vulnerable to various threats that might compromise NS/EP information. This Technical Information Bulletin (TIB) surveys equipment providing security services to users of wireless commercial communication services and assesses the level of protection afforded by such equipment.

The wireless communications environment can be extensive, ranging from commercial dispatch and cellular radio to satellite communications and television broadcasts. For the purpose of this TIB, the wireless services environment is defined as consisting of nine wireless services:

- Air-to-Ground Telephone
- Cellular Radio
- Cordless Telephone
- Land-Mobile Radio
- Mobile Satellite Service
- Paging
- Local Area Networks (LANs)
- Private Branch Exchanges (PBXs)
- Subscriber Loop.

Security threats can exist anywhere along a communications path. Active threats (e.g., intrusion) typically cause alteration in the information contained in the system or changes to the state or operation of the wireless system. Passive threats (e.g., eavesdropping) do not result in any modification to the information contained in the wireless transmission. There are five assumed threats in the wireless communications environment:

- Monitoring/Eavesdropping
- Traffic Flow Analysis
- Masquerading
- Information Modification
- Denial of Service.

The nine wireless services mentioned above were analyzed with respect to the security measures provided by the products in each wireless service category. *None of the products surveyed completely mitigated all associated threats in the wireless environment.* Information confidentiality is the most common security service among the products surveyed. *However, the security services and mechanisms found in most commercially available wireless communication equipment do not provide adequate security or privacy protection against the assumed threats, and hence to NS/EP telecommunications.*

Joint Government and industry action is needed to address the NS/EP security requirements for wireless communications. Alternatives are available to address NS/EP security needs:

- Local link security services, such as encryption, are applicable to cordless telephones, wireless PBXs, and wireless LANs.
- End-to-end security solutions may be more cost-effective than coordinating link security solutions with individual service providers.

The OMNCS will continue its analysis of wireless and security standards to ensure that they are being developed to support NS/EP requirements for security and privacy.

This TIB provides information from the ongoing analytical process.

## 1.0 INTRODUCTION

## 1.0 INTRODUCTION

The Department of Defense as well as other Federal departments and agencies want to make maximum use of commercial networks for future emergency communications (Ref. 1). More and more, these commercial networks are using a wireless infrastructure, and wireless access to these commercial networks is becoming increasingly available and attractive. Because of the availability of wireless communications solutions, National Security and Emergency Preparedness (NS/EP) telecommunication users will have access to a wider variety of services to meet their needs. Some of the networks may be completely wireless (e.g., a high-frequency or microwave radio network), and some may be subnetwork extensions of nonwireless systems (e.g., a cellular radio network that interfaces with the Public Switched Network [PSN]).

Wireless communications enhance users' communications capabilities, including improved flexibility and mobility, and provide alternative access to and egress from the PSN. Unprotected signals transmitted over the air waves, however, are vulnerable to active and passive security threats that can compromise all internal and connected systems and networks. The increasing demand for and use of wireless communications in the networks supporting NS/EP users add new dimensions to the requirement for an overall NS/EP security architecture.

According to industry experts serving on the President's National Security Telecommunications Advisory Committee (NSTAC), recent evidence suggests that criminal elements are exploring PSN vulnerabilities through electronic intrusion. According to the NSTAC Network Security Task Force, a motivated and resourceful adversary can degrade service in the PSN and disrupt telecommunications serving NS/EP users (Ref. 2). These individuals pose a significant and increasing threat to NS/EP telecommunications, especially during crises and emergencies.

The overall security architecture for a telecommunications system or service also must address its wireless adjuncts and interfaces. The security architecture requires comprehensive planning for countermeasures to network vulnerabilities and intensive architectural design for network security. To ensure adequate and affordable protection against security threats and to guarantee compatibility and compliance with existing

security architectures, wireless communications service providers and subscribers need to know what security services are available, what type of protection they afford, and how much they cost.

This Technical Information Bulletin (TIB) provides NS/EP telecommunication users and planners with information that can be used to determine whether commercial products can satisfy NS/EP security requirements.

## **1.1 BACKGROUND**

To ensure the maximum use of all existing and planned security services, the Office of the Manager, National Communications System (OMNCS) requires information about commercially available security measures for wireless communications. Adequate security protection is a vital planning criterion in the National Communications System (NCS) architecture design for the telecommunication services and systems supporting the NS/EP users. Adequate communications security is vitally important to the operational effectiveness of NS/EP personnel. All components of the architecture must support NS/EP requirements, including that of providing adequate levels of information security protection. All security planning activities of the OMNCS are directed toward safeguarding Government information and the systems that process or transport Government information from exploitation by hostile threats.

As part of the architecture planning and analysis process within the OMNCS, all aspects of security are being considered. For example, the OMNCS is addressing the issue of PSN security, focusing on the threat posed by electronic intruders into telecommunication network elements. The OMNCS initiated three projects to foster improvements in the security of the nation's telecommunications infrastructure: an assessment of the hacker threat to the PSN, a research and development project to develop a tool to analyze PSN software vulnerabilities, and a program to collect and analyze PSN software vulnerability data.

Wireless communication systems that interface with the PSN also have vulnerabilities that can threaten NS/EP telecommunications. To assist with security planning in the OMNCS, a survey of commercially available security services for wireless communications has been completed. This TIB presents the results of this

survey, and this information is being made available to the NCS members, particularly to NS/EP users.

## 1.2 PURPOSE

The following list outlines the purpose of this TIB:

- To provide OMNCS architecture planners with information on the availability, capabilities, and other parameters of commercially available security measures supporting wireless communications
- To identify common solutions to the security threats in different wireless communication environments
- To define the implications of available wireless security services for NS/EP telecommunications
- To provide the Assistant Manager, Office of Technology and Standards, NCS (NT) with information useful for developing a strategy to ensure that NS/EP security requirements for wireless communications are addressed in the standards-making process.

## 1.3 SCOPE

This TIB describes the results of an analysis and comparison of security services for the following cross-section of commercially available wireless communication services commonly used by NS/EP personnel:

- Air-to-Ground Telephone
- Cellular Radio
- Cordless Telephone
- Land-Mobile Radio
- Mobile Satellite Service
- Paging
- Local Area Networks (LANs)
- Private Branch Exchanges (PBXs)
- Subscriber Loop.

The following are types of product data collected and compared for this study:

- Price for product or service
- Date of availability of the product or service

- Security services provided, such as information confidentiality, traffic flow confidentiality, denial of service protection, information integrity, authentication, and access control
- Type of key system used
- Algorithm used.

This study is based upon assumed threats to wireless communications. A reliable and continuing assessment of the threats and vulnerabilities to wireless communications and the recommendation of appropriate and effective implementation of countermeasures are beyond the scope of this study.

## **1.4 ORGANIZATION**

This TIB is organized into five chapters. Chapter 1 introduces the TIB and provides background information on its purpose and content. Chapter 2 defines the wireless environment analyzed for applicable security services. Chapter 3 presents the assumed security threats, countermeasures, and NS/EP-required security services for wireless communications. Chapter 4 provides a general overview and comparison of the information collected on commercially available security measures for wireless communications. Chapter 5 describes the implications of secure wireless communications to the NS/EP user. The glossary defines the terms used in this report.



## **2.0 WIRELESS TELECOMMUNICATIONS ENVIRONMENT**

## 2.0 WIRELESS TELECOMMUNICATIONS ENVIRONMENT

The words "wireless communications" offer several interpretations for many different technologies: cellular radio, LANs, Citizen Band (CB) radios, commercial dispatch radios, satellite communications. Although all of these technologies are "wireless," it is difficult to define the term "wireless" other than to say, "without wires."

This chapter presents a working definition of the term "wireless." It also defines the wireless services environment that will be investigated for available security services in this TIB.

### 2.1 DEFINITION OF WIRELESS

The term "wireless" has different meanings in various contexts. Exhibit 2-1 presents the working definition of "wireless" for this TIB.

#### EXHIBIT 2-1 Wireless Definition

Communications that utilize an unbounded, tetherless channel to propagate information signals through free space or atmosphere in the form of electromagnetic radiation.

Communication channels are classified in three ways: transmission line (as in telephony and telegraphy), optical fiber (as in optical communication), and wireless (Ref. 3). This TIB focuses on wireless channels.

The term "unbounded" is gaining acceptance as a technical term to describe one characteristic of a communication channel. As defined by the thesaurus, "unbounded" means "Having no bound, unlimited in extent, degree, or quantity; unchecked, uncontained, unrestrained; having no ends or limits" (Ref. 4). Beker and Piper state that wireless radio channels are unbounded in the sense that electromagnetic waves propagate into free space (Ref. 5). The unbounded nature of the channel is a very important distinction between wireless communications and wire communications.

Another concept used to describe wireless transmission channels is "tetherless," which describes an unrestrained or unlimited object. An example of a "tetherless" communications channel is the wireless channel. The working definition for tetherless at Bell Communications Research (Bellcore) is "having no wires" (Ref. 6). The term tetherless implies that the transmission path can be dynamically located, allowing changes in location at one or both ends of the channel.

The working definition shown in Exhibit 2-1 is intended only to clarify the term wireless in the context of this TIB. This definition may be used by other parties wishing to provide a definition of the term. It is not, however, an official definition used by the OMNCS or any of the member agencies of the NCS and has not been formally approved by these entities.

## **2.2 THE WIRELESS ENVIRONMENT**

As mentioned earlier in this chapter, many different technologies fall in the wireless category. Not all of these technologies are analyzed in this TIB. Exhibit 2-2 presents the nine types of wireless service that make up the wireless services environment for this TIB. Each system in this wireless services environment operates in frequencies designated by the Federal Communications Commission (FCC) as being for commercial licensed or unlicensed use.

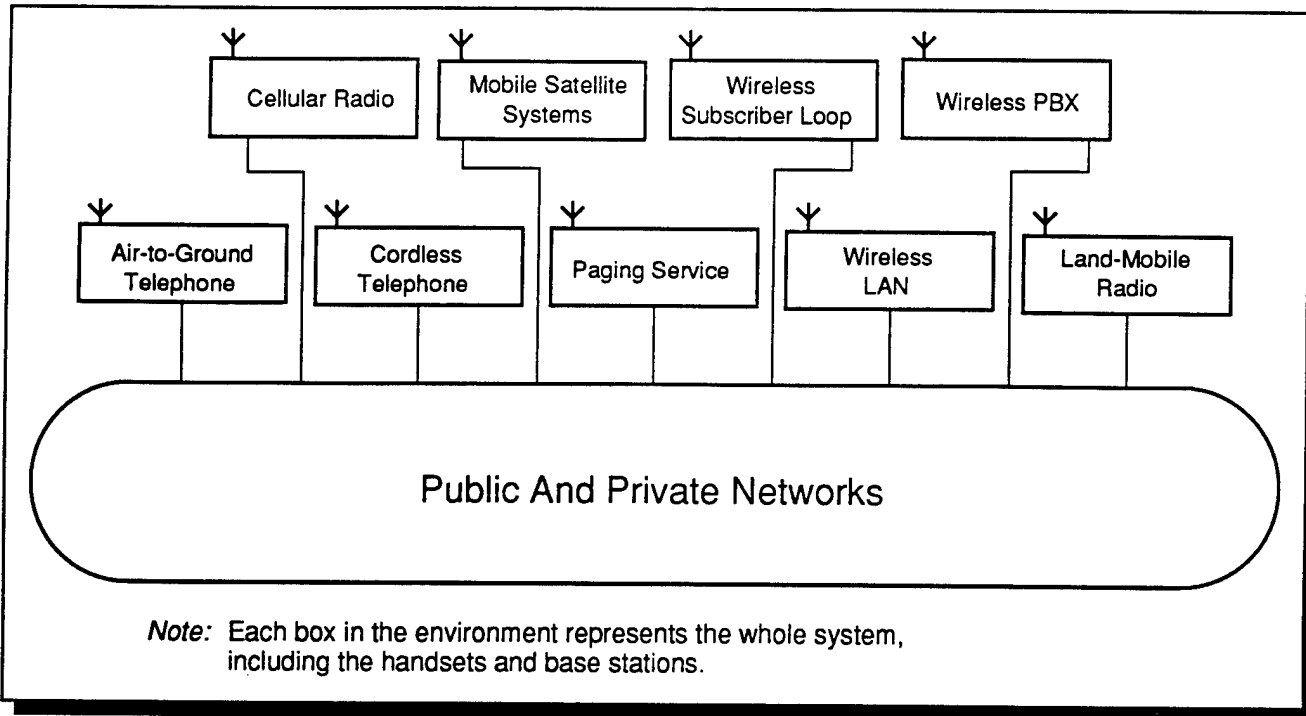
Wireless systems that use frequencies allocated for Government use (e.g., tactical radio systems) were excluded from this TIB, although NS/EP users may use tactical radio systems during a crisis or emergency. Tactical communication systems that use security measures to protect information transmitted over the wireless link are assumed to provide sufficient protection for NS/EP use.

The six wireless services shown in Exhibit 2-2 that primarily use commercial frequencies and are offered for public use by a service provider licensed by the FCC are air-to-ground telephone, cellular radio, cordless telephone<sup>1</sup>, mobile satellite systems,

---

<sup>1</sup> A cordless telephone system uses a fee-for-service arrangement to provide voice service to subscribers through either Cordless Telephone-Second Generation (CT-2) or Cordless Telephone-Third Generation (CT-3) equipment. The Cordless Telephone-First Generation (CT-1) found in many households is not considered in this TIB a part of the Cordless Telephone category, because Plain Old Telephone Service (POTS) does not depend upon the type of terminal equipment used.

**EXHIBIT 2-2**  
**The Wireless Services Environment**



03.134.93-1

paging, and wireless subscriber loop. Many of these wireless services are beginning to be addressed as a common set of services potentially offered by one service provider or a set of cooperating service providers. A potential third generation of wireless communication services, often referred to as Future Public Land Mobile Telecommunications System (FPLMTS), is being defined by telecommunication organizations to succeed the current generations of analog and digital networks. Currently, international standards work on FPLMTS is being supported in CCIR Task Group 8/1.

Another two of the services shown in Exhibit 2-2, wireless LAN and wireless PBX, usually operate in the unlicensed spectrum; therefore, a user can operate the system without a license from the FCC. These applications are being increasingly used to provide terminal mobility and network configuration flexibility. These products can help quickly reconstitute local area voice and data traffic support in a crisis or emergency.

The last wireless service, land-mobile radio, is provided by a collection of radio systems that might be used by NS/EP telecommunication users in a crisis or

emergency. Often, NS/EP users will need to communicate with users of land-mobile equipment, including state and local governments and law enforcement personnel, in a crisis or emergency. The equipment in this category uses commercial rather than Government frequencies for many radio networks.

### **3.0 SECURITY THREATS IN A WIRELESS COMMUNICATIONS ENVIRONMENT**

### 3.0 SECURITY THREATS IN A WIRELESS COMMUNICATIONS ENVIRONMENT

Threats may exist anywhere along a communications path. This study focuses on threats that can occur along the wireless segment of a communications path.

This chapter describes the assumed security threats to wireless communications. The threats described in this chapter do not constitute a Government-validated threat model for wireless communications.

#### 3.1 OVERVIEW OF SECURITY THREATS TO WIRELESS COMMUNICATIONS

Exhibit 3-1 shows categories of the sources and types of threats that can be envisioned in a wireless communications environment. Each source of threats (e.g., human/intentional) contains unique types of threats (e.g., monitoring). This exhibit identifies active and passive threats that can occur either accidentally or intentionally.

**EXHIBIT 3-1**  
**Security Threats to the Wireless Environment**

| HUMAN/INTENTIONAL                                                                                                                                                                                        | ENVIRONMENTAL/NATURAL                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Monitoring/Eavesdropping</li><li>• Traffic Flow Analysis</li><li>• Masquerading/Hacking</li><li>• Information Modification</li><li>• Denial of Service</li></ul> | <ul style="list-style-type: none"><li>• Fire</li><li>• Flood</li><li>• Earthquake</li><li>• Wind</li></ul>                                                                                             |
| ENVIRONMENTAL/FABRICATED                                                                                                                                                                                 | HUMAN/UNINTENTIONAL                                                                                                                                                                                    |
| <ul style="list-style-type: none"><li>• Sabotage</li><li>• Conventional Warfare</li><li>• Unconventional Warfare</li></ul>                                                                               | <ul style="list-style-type: none"><li>• Accidental Discovery</li><li>• Spurious Emissions</li><li>• Improper Use of Equipment</li><li>• Equipment Malfunction</li><li>• Property Destruction</li></ul> |

03.134.93.3-1

Active threats (e.g., intrusion) typically cause alteration in the information transmitted in the wireless system or changes to the state or operation of the system. Because of the nature of the wireless channel, intruders may be able to access and perform unauthorized activities from mobile or remote locations that may be difficult to locate without employing radio intercept techniques.

Passive threats (e.g., eavesdropping), if realized, would not result in any modification to the following areas:

- Information contained in the wireless transmission
- Operation of the wireless system
- Configuration of the wireless system.

The analysis of the commercially available security services and mechanisms addresses only the assumed threats listed under the "Human/Intentional" category shown in Exhibit 3-1. None of the products were surveyed regarding protection from the other categories of wireless communication threats.

Exhibit 3-2 characterizes the assumed threats, countermeasures, and required security services for the wireless communications environment.

**EXHIBIT 3-2**  
**Threats, Countermeasures, and Required Security Services**

| <b>Assumed Threats</b>   | <b>Countermeasures</b>                       | <b>Required Security Services</b>                          |
|--------------------------|----------------------------------------------|------------------------------------------------------------|
| Monitoring/Eavesdropping | Encrypt the Information                      | Information Confidentiality                                |
| Traffic Flow Analysis    | Prevent Pattern Detection                    | Traffic Flow Confidentiality                               |
| Masquerading             | Control Access                               | Authentication/Access Control                              |
| Information Modification | Encrypt the Information<br>Control Access    | Information Integrity<br>Authentication/Access Control     |
| Denial of Service        | Use Trusted Computer Bases<br>Control Access | Trusted Operating Systems<br>Authentication/Access Control |

03.134.93.3-2(a)



These threats and security services are key parameters for analyzing and comparing the products surveyed during this study.

### 3.2 ASSUMED THREATS

The sections below define the assumed threats highlighted in Exhibit 3-3.

**EXHIBIT 3-3**  
**Assumed Threats**

| <b>Assumed Threats</b>          | <b>Countermeasures</b>                       | <b>Required Security Services</b>                          |
|---------------------------------|----------------------------------------------|------------------------------------------------------------|
| <b>Monitoring/Eavesdropping</b> | Encrypt the Information                      | Information Confidentiality                                |
| <b>Traffic Flow Analysis</b>    | Prevent Pattern Detection                    | Traffic Flow Confidentiality                               |
| <b>Masquerading</b>             | Control Access                               | Authentication/Access Control                              |
| <b>Information Modification</b> | Encrypt the Information<br>Control Access    | Information Integrity<br>Authentication/Access Control     |
| <b>Denial of Service</b>        | Use Trusted Computer Bases<br>Control Access | Trusted Operating Systems<br>Authentication/Access Control |

03.134.93.3-2(a)

#### 3.2.1 Monitoring/Eavesdropping

Monitoring, the unauthorized observation of information passing between users over a communications channel, is a major wireless communications threat. By monitoring legitimate call setup and/or call content information, an intruder can gather intelligence that can be used for various unauthorized, destructive, or disruptive activities.

An eavesdropper can use call setup information for subsequent network intrusion. For example, access and authorization codes can be collected by monitoring the air waves and subsequently used to gain access to the network. An intruder gaining access to a network can perform a variety of active and passive actions (e.g., inserting

misinformation into a database, infecting software with viruses, downloading information files).

Eavesdroppers also can gain access to sensitive information being passed between legitimate network users. By recording and analyzing one or more legitimate call setups and conversations, an eavesdropper can gather sensitive NS/EP information being transported via a wireless communications means. This information might then be distributed to potentially threatening parties.

### **3.2.2 Traffic Flow Analysis**

Changes to normal traffic patterns (e.g., changes from the average calls made per day or traffic volume) among NS/EP personnel may provide knowledge about a new or pending activity that, for national security reasons, must be restricted. Intelligence can be gained by analyzing the traffic patterns of either encrypted or unencrypted signals. For example, an increase in transmissions among NS/EP users could indicate that an exercise or contingency situation is about to occur or has occurred.

### **3.2.3 Masquerading**

Masquerading occurs when individuals overtly or covertly gain unauthorized access to unprotected wireless communication systems, which may provide them access to controlled information and to priority treatment capabilities established for NS/EP users. A masquerading threat exists when either a human or computer process pretends to be a different entity for the purpose of gaining unauthorized access to a network service or network component. Usually masquerading is used in conjunction with some other form of active attack (e.g., gaining access to protected systems or manipulating the legitimate network users). The masquerading entity may be an end user (e.g., a human or a mobile terminal) or an intermediate component in the wireless system or network (e.g., a repeater or a base station).

### **3.2.4 Information Modification**

An individual masquerading as an NS/EP user on a wireless communications network may intercept and alter data or may transmit misinformation to other NS/EP

personnel. Data communications are more vulnerable to modification than voice communications; however, both are very vulnerable to insertion of misinformation.

### **3.2.5 Denial of Service**

Unauthorized use of wireless communications may result in denial of service to legitimate users of the same or related services. For example, an intruder could "crash" a component or network by inserting enough data to overload the throughput capacity of a switch or call controller. An intruder could also modify an access profile to deny certain services to NS/EP personnel.

Another example of an overt denial-of-service action is jamming the frequencies supporting the wireless link. Jamming is the intentional transmission of radio signals in order to interfere with the reception of signals from another transmitter. Jamming may be accomplished by saturating a receiver with sufficient noise to prevent reception of the intended signals. For example, an unauthorized cellular user may deny communication services to NS/EP users by jamming the control channels supporting the cellular service.

A third example of an overt denial-of-service action is a masquerader who allows network users to detect the presence of an intruder. The resulting confusion effectively ties up a network while legitimate users identify themselves to each other.

## **3.3 COUNTERMEASURES**

This section describes the measures required to counter the threats described in Section 3.1. Exhibit 3-4 highlights the countermeasures and shows the correlation between the assumed threats and the actions needed to counter them.

### **3.3.1 Encrypt the Information**

Information encryption prevents monitoring and eavesdropping entities from understanding the information being transmitted over a wireless link in a communications path. Encrypting NS/EP information, especially on an end-to-end basis, assures recipients that the information has been kept confidential during

### EXHIBIT 3-4 Countermeasures

| Assumed Threats          | Countermeasures                              | Required Security Services                                 |
|--------------------------|----------------------------------------------|------------------------------------------------------------|
| Monitoring/Eavesdropping | Encrypt the Information                      | Information Confidentiality                                |
| Traffic Flow Analysis    | Prevent Pattern Detection                    | Traffic Flow Confidentiality                               |
| Masquerading             | Control Access                               | Authentication/Access Control                              |
| Information Modification | Encrypt the Information<br>Control Access    | Information Integrity<br>Authentication/Access Control     |
| Denial of Service        | Use Trusted Computer Bases<br>Control Access | Trusted Operating Systems<br>Authentication/Access Control |

03.134.93.3-2(b)

transmission. The strength of the protection used, based upon the type of algorithm and key management system, indicates the levels of classified information that can be transmitted. Privacy is provided on the wireless link in a variety of ways, some stronger than others:

- Digital compression
- Spread-spectrum signals, especially direct-sequence modulation schemes
- Low-probability-of-intercept signals, often provided by spread-spectrum transmission techniques
- Proprietary encryption and scrambling algorithms
- Government encryption algorithms, such as Data Encryption Standard (DES)
- NSA-approved encryption algorithms.

The Department of Defense believes that only the last encryption method can be trusted to protect classified information.

Wireless communication services used by NS/EP personnel should provide information integrity assurances. Encryption by using private keys unique to the end

users provides such assurances. The use of private keys also provides the unambiguous identification of the originator of the information or call. Cryptographic checksums provide some assurance that the information received has not been modified during transmission. Public-key cryptography is also gaining acceptance as an encryption method due to its ease of managing encryption keys. For voice applications, scrambling the signal by using strong key management systems ensures end-to-end identification and protection of the information being exchanged between the caller and the called parties.

Government-approved encryption techniques often provide more than just information confidentiality. The following also are the result of implementing these encryption techniques:

- Unique and unambiguous identification of the caller and called parties via digital signatures
- Protection from masquerading individuals or computer processes
- Varying strengths of assurances that information is protected from intentional or accidental modification.

### 3.3.2 Prevent Pattern Detection

Because of their broadcast nature, wireless communications are vulnerable to the monitoring and detection of changes in user traffic patterns. Some wireless communication services (e.g., digital cellular radio systems) employ spread-spectrum and frequency-hopping techniques that make it difficult to identify and track a complete conversation or transmission. Sophisticated electronic tracking capabilities exist, however, and can be used to overcome this difficulty. The following are methods for preventing detection of pattern changes:

- **Constant broadcasting, which masks when real information is being transmitted.** This method is costly when the users are billed for air-time usage.
- **Protection of the identity of the users through encryption of the control and signaling information.** Digital encryption technology is available to provide this capability.

- **Use of spread-spectrum, direct sequence, and frequency-hopping systems.** These systems provide protection from casual eavesdropping, traffic flow analysis, and insertion of misinformation into an active communication. This method is not totally reliable.

### 3.3.3 Control Access

Preventing masquerading entities (e.g., hackers and phreakers) from penetrating the network requires the implementation of authentication and access control mechanisms and procedures. Physical protection, coupled with the use of trusted operating systems, strengthens the overall security posture even more. Mechanisms (e.g., smart cards, devices containing private codes that a network component uses to verify the identity of the user; passwords; key certificates; tokens) can be employed to ensure the identity and access levels for NS/EP users. Two levels of authentication are typically defined for Government applications—simple and strong.

- **Simple authentication** can be provided through the use of smart cards and passwords. Unless another method (e.g., keying in a personal identification number [PIN]) is used in conjunction with the smart card, an unauthorized person using a stolen card would be identified as a valid subscriber.
- **Strong authentication** requires the exchange of cryptographic information protected by sophisticated and highly controlled key management techniques. Both public and private keys may be required to provide strong authentication of the users.

Both of these techniques can be applied to wireless communications.

### 3.3.4 Use Trusted Computer Bases

Trusted operating systems are required to protect network components against threats such as hackers, phreakers, viruses, and the intentional or accidental transmission of protected information between open and closed user communities. The application of trusted computing bases to wireless communications is appropriate for the network interface component, (e.g., a base station or repeater). Security services should be applied at all “doorways” along the communications path. For wireless communications, this could be the transceiver or first computer providing access to the originator/caller. All computers internal to the network should use trusted software.

The cost of such a configuration depends on the objectives of the applicable security architecture.

### 3.4 REQUIRED SECURITY SERVICES

Exhibit 3-5 highlights the security services deemed important for wireless communications that support NS/EP users. These services should be used to provide the minimum set of services for protecting NS/EP information. The products analyzed for this study were evaluated against and compared to these service requirements. For example, the security services listed in Exhibit 3-5 were used as a baseline to guide commercial products surveyed during the analysis.

**EXHIBIT 3-5  
Required Security Services**

| <b>Assumed Threats</b>   | <b>Countermeasures</b>                       | <b>Required Security Services</b>                          |
|--------------------------|----------------------------------------------|------------------------------------------------------------|
| Monitoring/Eavesdropping | Encrypt the Information                      | Information Confidentiality                                |
| Traffic Flow Analysis    | Prevent Pattern Detection                    | Traffic Flow Confidentiality                               |
| Masquerading             | Control Access                               | Authentication/Access Control                              |
| Information Modification | Encrypt the Information<br>Control Access    | Information Integrity<br>Authentication/Access Control     |
| Denial of Service        | Use Trusted Computer Bases<br>Control Access | Trusted Operating Systems<br>Authentication/Access Control |

03 134 93 3-2 (c)

#### 3.4.1 Information Confidentiality

To protect against monitoring or eavesdropping, NS/EP users require security services that provide information confidentiality. Security mechanisms that encrypt or scramble the information being exchanged between NS/EP users provide the best means to ensure information confidentiality. Information confidentiality should be a mandatory security service for all NS/EP telecommunication services and systems.

### **3.4.2 Traffic Flow Confidentiality**

Mechanisms and techniques that mask any changes to normal patterns are the best methods for preventing collection of intelligence through the analysis of the traffic flow between and among NS/EP users. The requirement for such protection on NS/EP telecommunication services and systems should be optional and determined locally by mission needs.

### **3.4.3 Authentication and Access Control**

Authentication and access control security services should be mandatory for all NS/EP telecommunication services and systems. The strength of the security services must be at least the minimum required by the network or service management structure. Controlling access to the services and network components supporting NS/EP telecommunications may be the primary protection required in the current threat environment for wireless communications.

### **3.4.4 Information Integrity**

Information integrity should be a mandatory security service for all NS/EP telecommunications. This service prevents unauthorized modification of NS/EP information while it is being transmitted through a wireless network. Use of a combination of encryption and access control security mechanisms and procedures, plus checksum protocols, satisfies this requirement.

### **3.4.5 Trusted Operating Systems**

To prevent NS/EP users from being denied the use of their mission-support telecommunication services, network and service providers must ensure adequate trust in the software used in the network components. Use of trusted operating systems throughout wireless networks should be a goal for NS/EP telecommunication planners. The continuous use of access control and authentication services, in conjunction with trusted operating systems, is recommended as the ideal security posture for supporting NS/EP telecommunication services and systems.



#### **4.0 SECURITY SYSTEM AND SERVICE REQUIREMENTS**

## 4.0 SECURITY SYSTEM AND SERVICE REQUIREMENTS

This chapter presents an analysis of the wireless communication products surveyed in this TIB. The analysis is divided among the nine wireless services identified in Section 2.2:

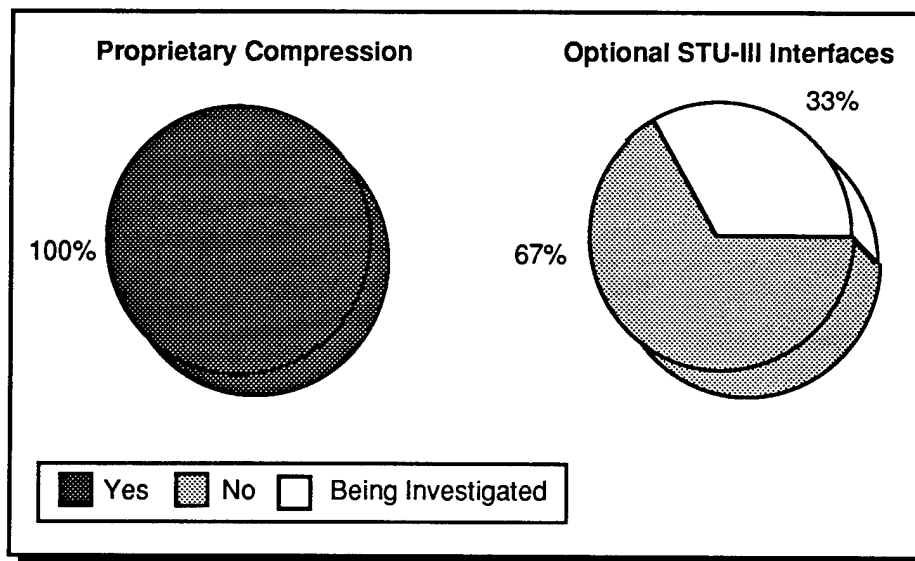
- Air-to-ground telephone
- Cellular radio
- Cordless telephone
- Land-mobile radio
- Mobile satellite systems
- Paging
- Wireless LANs
- Wireless PBXs
- Wireless subscriber loops.

The information gathered from the survey of wireless service products covers the security services provided, types of information protected, methods of protecting the wireless channel, frequencies of operation, and vendor data. This chapter analyzes information pertaining to the security measures provided by products in each wireless service environment. The exhibits presented in the following sections show what proportion of the products surveyed address the topic being discussed. For example, Exhibit 4-1 shows that 100% of the products surveyed use proprietary compression to protect the wireless channel in air-to-ground telephone, 67% do not use optional Secure Telephone Unit, Third Generation (STU-III) interfaces, and 33% of the product manufacturers are investigating use of optional STU-III interfaces.

### 4.1 AIR-TO-GROUND TELEPHONE

As mandated by the Code of Federal Regulations (47 CFR 22), air-to-ground radiotelephone service operates within the 849–851 and 894–896 megahertz (MHz) frequency ranges, and individual communication channels are allocated a bandwidth of 6 kilohertz (kHz). Transmission of digital voice (analog voice that has been pulse code modulated at 64 kb/s) or high speed data over such narrowband radio channels requires the use of data compression and digital modulation techniques. All of the carriers surveyed use proprietary compression techniques to accomplish the necessary bandwidth reduction. Furthermore, these proprietary schemes, as demonstrated in Exhibit 4-1, serve as the principal method of channel protection. Through proprietary

**EXHIBIT 4-1**  
**Air-to-Ground Telephone—Methods of Protecting the Wireless Channel**



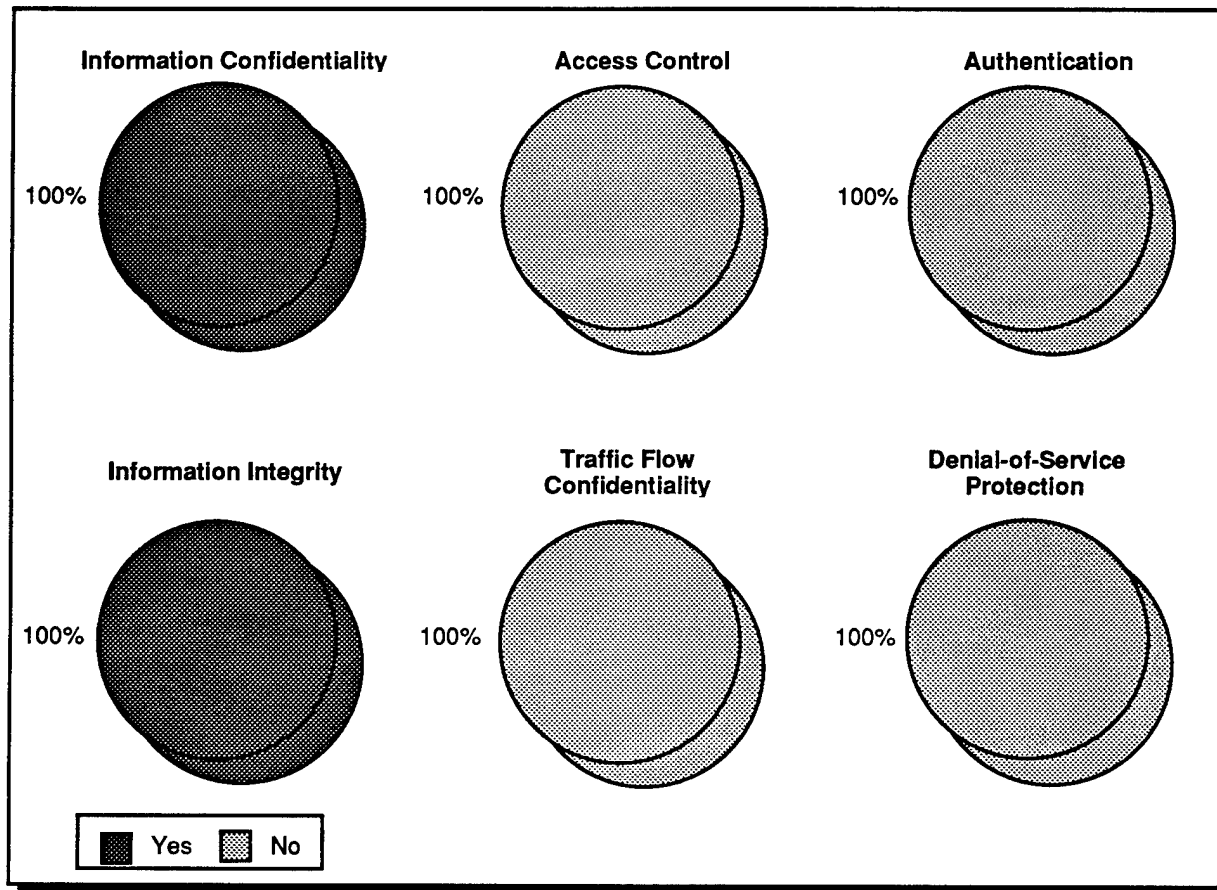
03.134.93-4-03

compression and modulation techniques, air-to-ground telephone service attains a modest amount of security, providing both information confidentiality and integrity to the call content as shown in Exhibits 4-2 and 4-3.

It is possible to intercept and decipher user communications. An eavesdropper with access to the proper devices and knowledge of the carrier schemes can monitor air-to-ground telephone transmissions, but highly sophisticated equipment is needed for monitoring digital air-to-ground communication. Consequently, digital equipment is less vulnerable to eavesdropping than are traditional technologies such as analog cordless or cellular radio equipment. Therefore, digital air-to-ground telephone service provides minimal privacy to personal communication.

To provide truly secure communications, carriers must work toward the implementation of STU-III-compatible systems. Each carrier is addressing the STU-III issue with mixed results. Air-to-ground telephone manufacturers are investigating and designing the necessary interfaces to provide STU-III functionality to the interested parties. Moreover, requests for STU-III capability are being addressed on a customized, case-by-case basis. Because deployment of STU-III capability is extremely limited, most implementations have not been fully tested.

**EXHIBIT 4-2**  
**Security Services for Air-to-Ground Telephone**



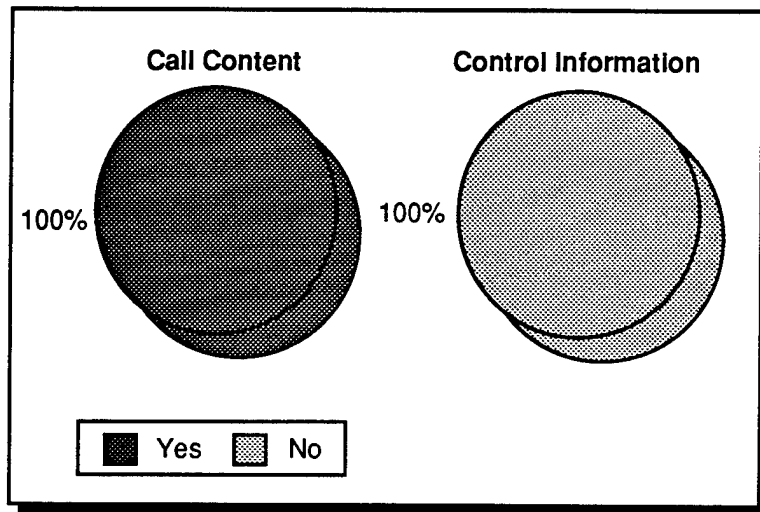
03.134.93-4-01

The other security services (e.g., authentication and access control) shown in Exhibit 4-2 are not addressed by the air-to-ground telephone industry. This is not unusual for a young industry with an undefined security risk. As with other communications and computer technologies, concerns about security become prevalent after the technology reaches maturity and has a stable body of users.

## 4.2 CELLULAR RADIO

Cellular radio is a relatively mature wireless telecommunications service. Many cellular radio services, especially in urban areas, have been operating since the early 1980s. The maturity of cellular service is reflected in the types of security and privacy products available for cellular users. Products for analog-only cellular networks are

**EXHIBIT 4-3**  
**Air-to-Ground Telephone—Types of Information Protected**



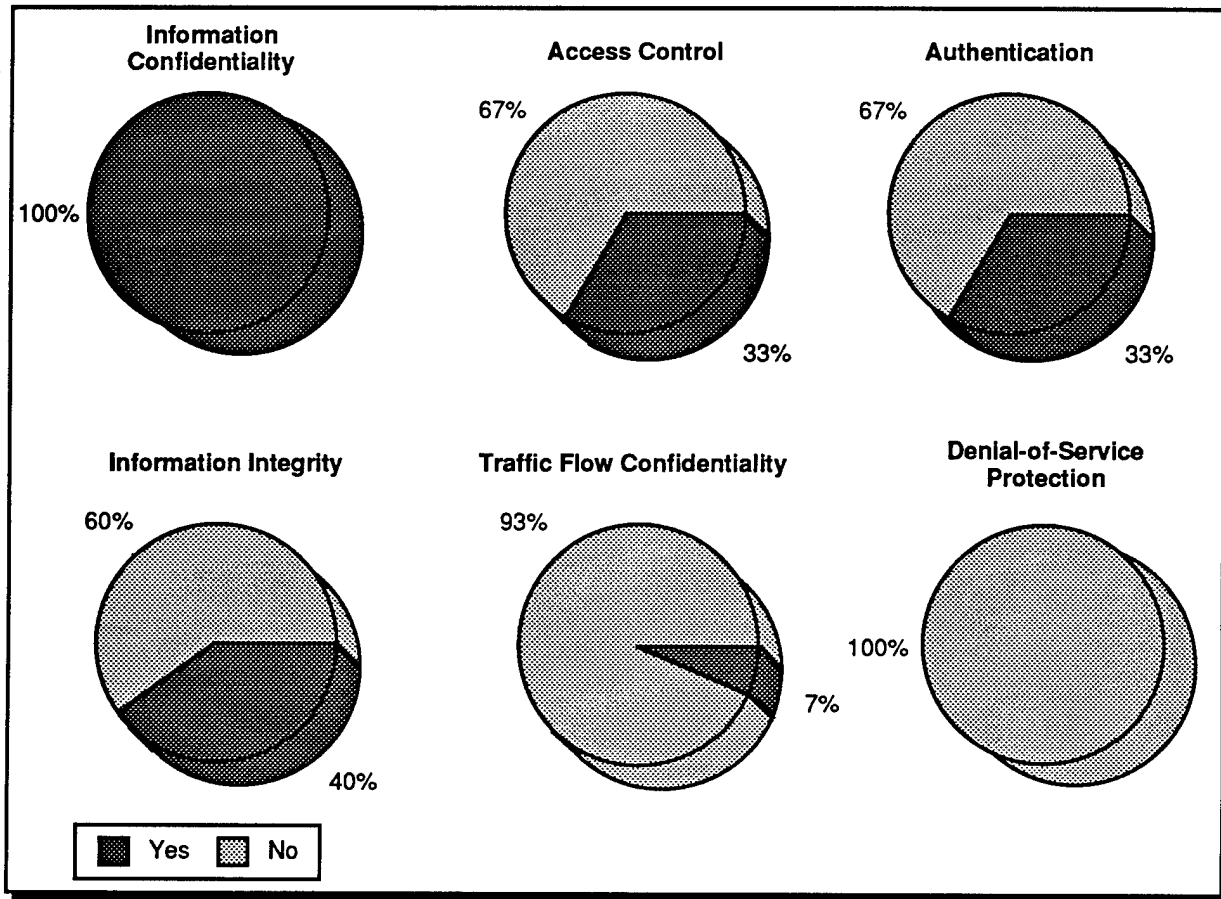
03.134.93-4-02

available as are products that support newer dual-mode analog/digital cellular networks.

Exhibit 4-4 shows the distribution of security services described in Chapter 3. The following list summarizes the security services provided by the products that were surveyed:

- All products provide some level of information confidentiality or privacy either through a spread-spectrum technique or an actual scrambling or encryption algorithm.
- Approximately 33% of the products provide authentication and access control measures to protect their users from masquerading threats. These products use some type of public or private key to validate the user and limit the use of such products.
- Approximately 40% of the products provide information integrity to ensure that information is not modified between transmitting and receiving parties. Analog products cannot provide information integrity because the information is never converted into a digital representation.
- Few of the products provide traffic flow confidentiality or denial-of-service protection. Those that provide traffic flow confidentiality do so because of a modulation scheme intended to increase system capacity, not as a result of an effort to provide traffic flow confidentiality.

**EXHIBIT 4-4**  
**Security Services for Cellular Radio**

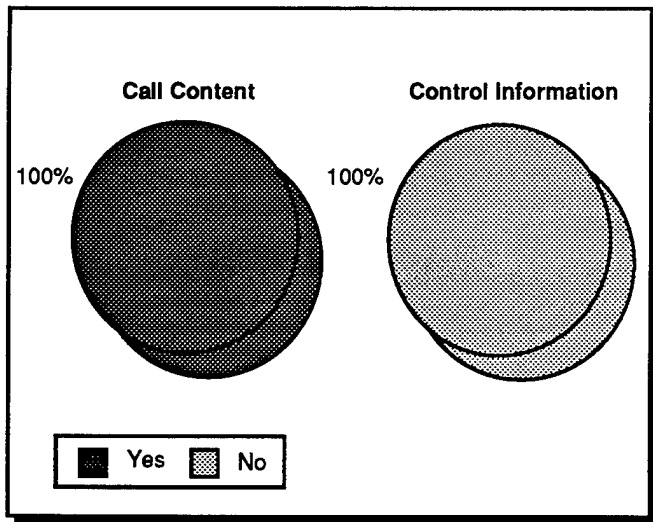


03.134.93-4-04

Exhibit 4-5 shows the types of information protected by the security and privacy products for cellular radio. All products protect the call content, which is sent on a separate channel from the control information. Control channel information must remain unaltered so that cellular subscribers who do not use privacy devices can use the same control channels.

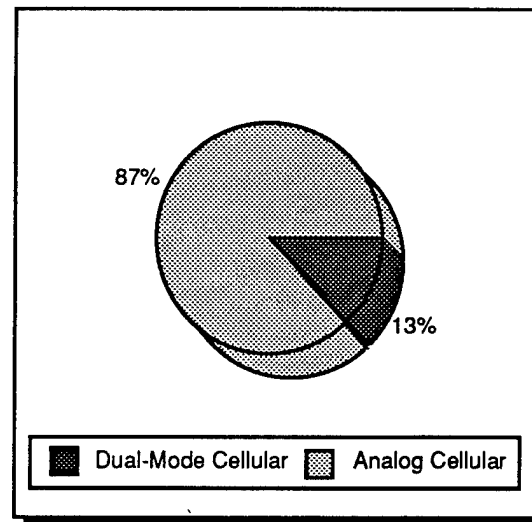
Exhibit 4-6 depicts the distribution between analog cellular products and dual-mode cellular products. Most of the products surveyed are useful only on analog cellular systems. This reflects the maturity and established customer base of analog cellular systems, as compared to the yet-to-be-deployed dual-mode cellular technologies.

**EXHIBIT 4-5**  
Cellular Radio—Types of  
Information Protected



03.134.93-4-05

**EXHIBIT 4-6**  
Types of Cellular Network Products

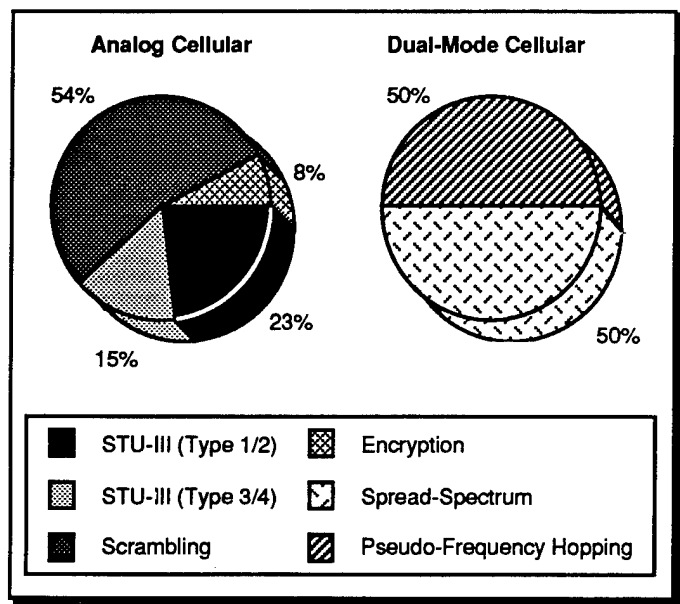


03.134.93-4-05

As shown in Exhibit 4-7, some products use STU-III technology to protect the call content. Approximately one-third of all security solutions for cellular radio use STU-III components. Type 1 STU-III products provide the highest level of protection and support both classified and unclassified traffic; types 2 through 4 STU-III products provide decreasing levels of protection to their users. Types 3 and 4 STU-III products are used mostly by non-Government users, including businesses concerned about telecommunications security. All STU-III applications available for cellular use are employed in the analog cellular networks; however, manufacturers also intend to support STU-III functionality in dual-mode networks. All other privacy techniques are based on proprietary scrambling, encryption algorithms, or spread-spectrum techniques.

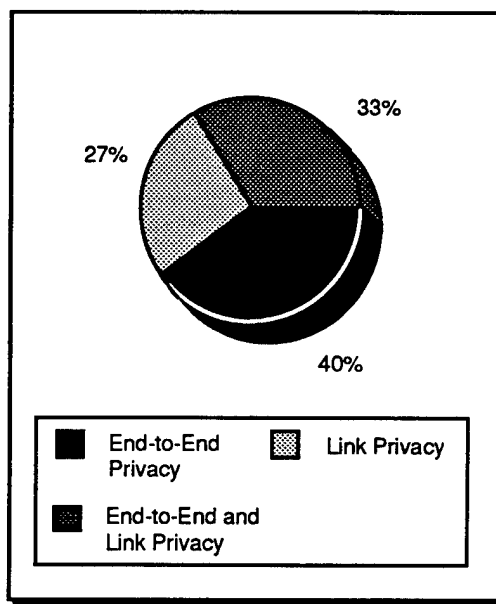
The privacy measures used to protect transmitted information can be applied either on the wireless link or on an end-to-end basis. A link protection system has a privacy unit at the cellular base station and another in a cellular terminal, whereas an end-to-end system has privacy units in both communicating terminals, at least one of which is a cellular terminal. Exhibit 4-8 shows the distribution of products according to link or end-to-end privacy measures. Some products can be used on either a link connection or an end-to-end basis if the cellular Mobile Switching Center (MSC) does not have a privacy unit installed.

**EXHIBIT 4-7**  
**Cellular Radio—Methods of**  
**Protecting the Wireless Channel**



03.134.93-4-06

**EXHIBIT 4-8**  
**Cellular Radio—**  
**Link Versus End-to-End Privacy**



03.134.93-4-06

Exhibit 4-9 compares the prices of the more common security services shown in Exhibit 4-4. The data presented in Exhibit 4-9 are dependent on the availability of pricing information.<sup>1</sup> The prices reflect a cellular handset/telephone with any additional privacy components that might need to be attached to or installed in the terminal.

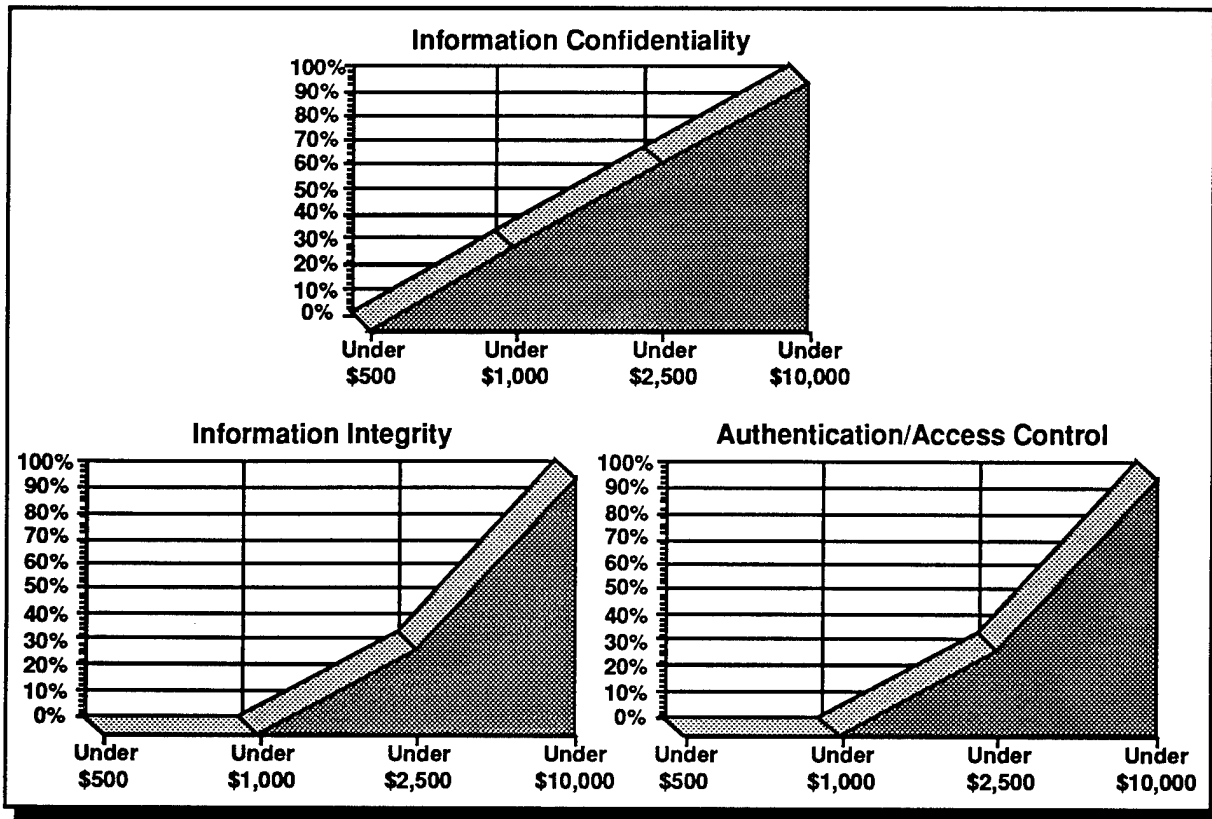
Terminals that provide information confidentiality can be purchased for under \$10,000; some may be purchased for under \$500. To obtain information integrity, authentication, and access control, however, more expensive units must be purchased. The price of the least expensive units that provide these services ranges from \$1,000 to \$2,500.

Exhibit 4-10 shows the distribution of security services among the products surveyed. As shown in the exhibit, 53% of all cellular products provide only

<sup>1</sup> Pricing information was unavailable because some terminals have not been released for sale and other terminals have restricted availability.

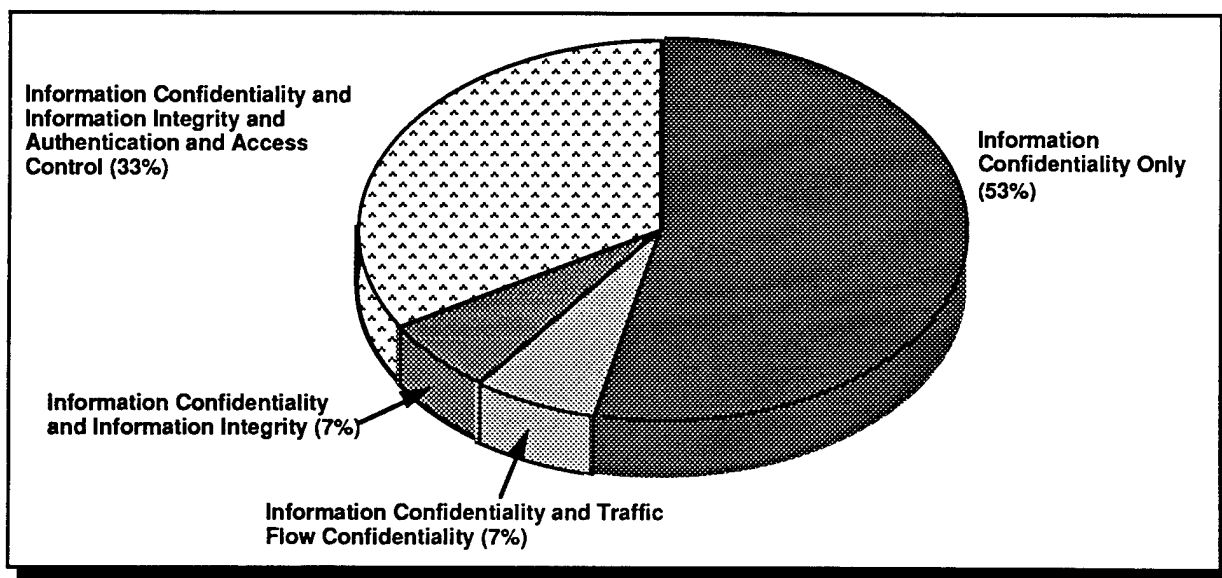


**EXHIBIT 4-9**  
**Cellular Radio—Price Ranges for Various Security Services**



03.134.93-4-07

**EXHIBIT 4-10**  
**Cellular Radio—Distribution of Security Services**



03.134.93-4-08

information confidentiality, while 33% provide information confidentiality, information integrity, authentication, and access control. Such data reinforce the notion that manufacturers are concentrating on providing some degree of privacy to cellular subscribers, without necessarily satisfying the security requirements of other users, such as NS/EP telecommunication users.

### 4.3 CORDLESS TELEPHONE

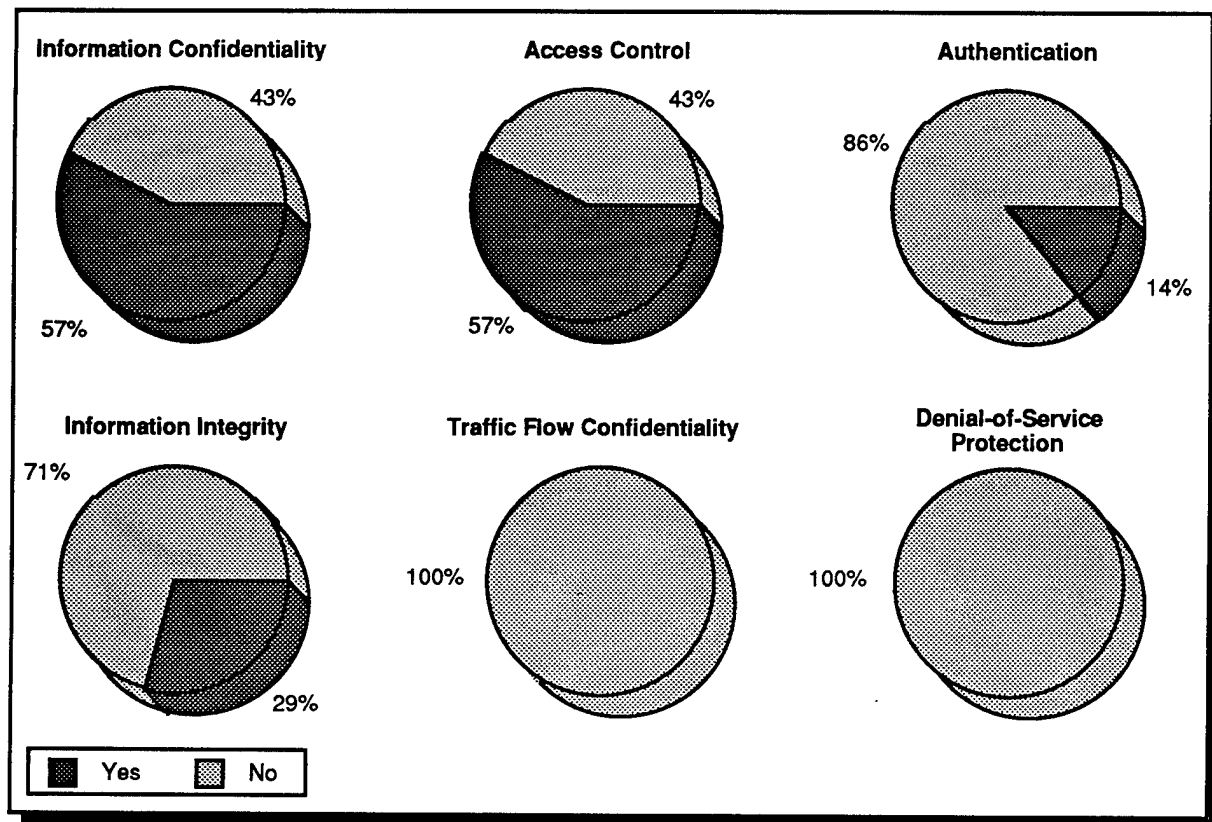
Traditionally, cordless telephones have been unable to provide privacy. Early analog sets used frequency modulation (FM) techniques that were extremely vulnerable to eavesdropping. Because users would be interrupted by conversations of other users sharing the same channel, the sets never gained acceptance in either commercial or military applications.

Second-generation cordless telephones (CT-2) are digital and afford more privacy than the original analog sets. The first digital standard, CT-2, provides some inherent privacy by using digital Frequency Division Multiple Access (FDMA) techniques. Although CT-2 type transmissions are much less susceptible to eavesdropping, they still lack the encryption and authentication procedures needed to be considered secure.

In general, as Exhibits 4-11 and 4-12 show, security services and protection are not readily available in commercial cordless telephone offerings. Recent product developments using proprietary CT-2Plus, third-generation cordless telephones (CT-3), and spread-spectrum technologies offer promise of increased security in the cordless telephone industry (see Exhibit 4-12). For example, both CT-2Plus and CT-3 claim to support encryption between the handset and base station, an improvement over the current CT-2. The use of spread-spectrum techniques and Code Division Multiple Access (CDMA) should also be highly effective in safeguarding wireless transmissions.

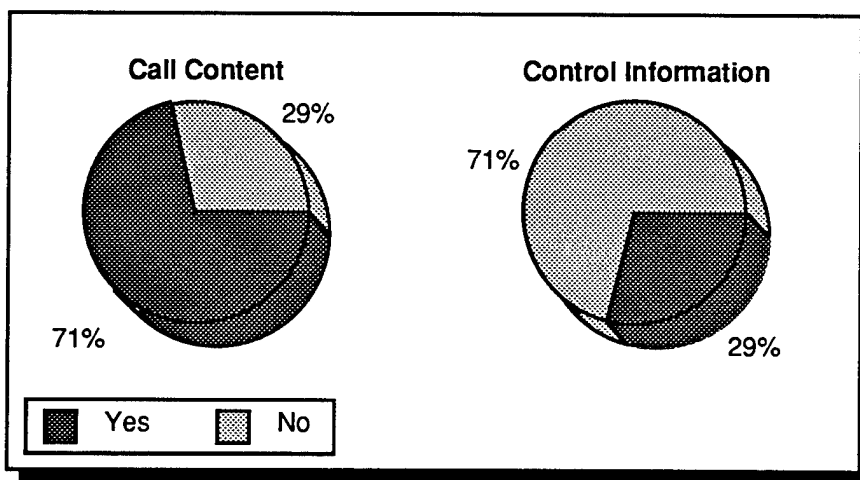
Truly secure cordless telephone systems are unavailable (note the absence of STU-III products in Exhibit 4-13). Upcoming FCC decisions, expected to standardize digital cordless telephones, may help open the market and spur demand for such devices; however, STU-III technology might be too bulky for inclusion in a cordless telephone. Larger markets could ultimately justify the development of secure cordless phones and additional security services.

# **EXHIBIT 4-11** **Security Services for Cordless Telephones**



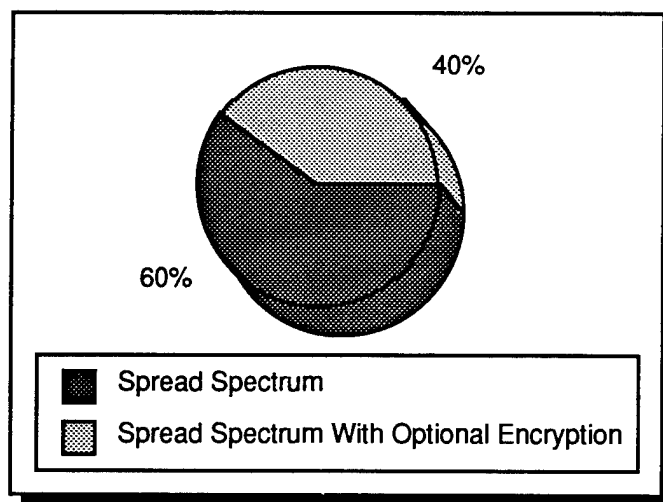
03.134.93-4-28

# **EXHIBIT 4-12** **Cordless Telephone—Types of Information Protected**



03.134.93-4-29

**EXHIBIT 4-13**  
**Cordless Telephone—Methods of Protecting the Wireless Channel**



03.134.93-4-30

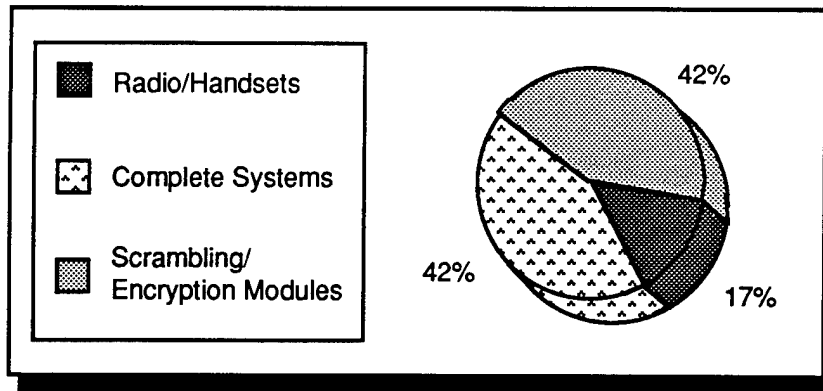
#### **4.4 LAND-MOBILE RADIO**

Unprotected analog land-mobile radios are extremely susceptible to interception and eavesdropping; any individual using a commercially available radio scanner can simply tune to the appropriate frequency and listen in. Business professionals and government groups (e.g., law enforcement agencies) that use these unsecure devices run the risk of having sensitive conversations unnecessarily exposed to the public. To provide the requisite protection, a wide range of manufacturers' products are available to satisfy most security and financial concerns.

Secure land-mobile products generally fall into one of three categories: scrambling/encryption modules designed to retrofit other manufacturers' radios; matched radio/handset pairs; and complete systems that integrate the radios, handsets, and repeaters with optional key management capabilities. Exhibit 4-14 illustrates a relative balance between low (modules), middle (radio/handsets), and high-end (complete systems) land-mobile products. Consequently, end users benefit by having a varied selection at their disposal.

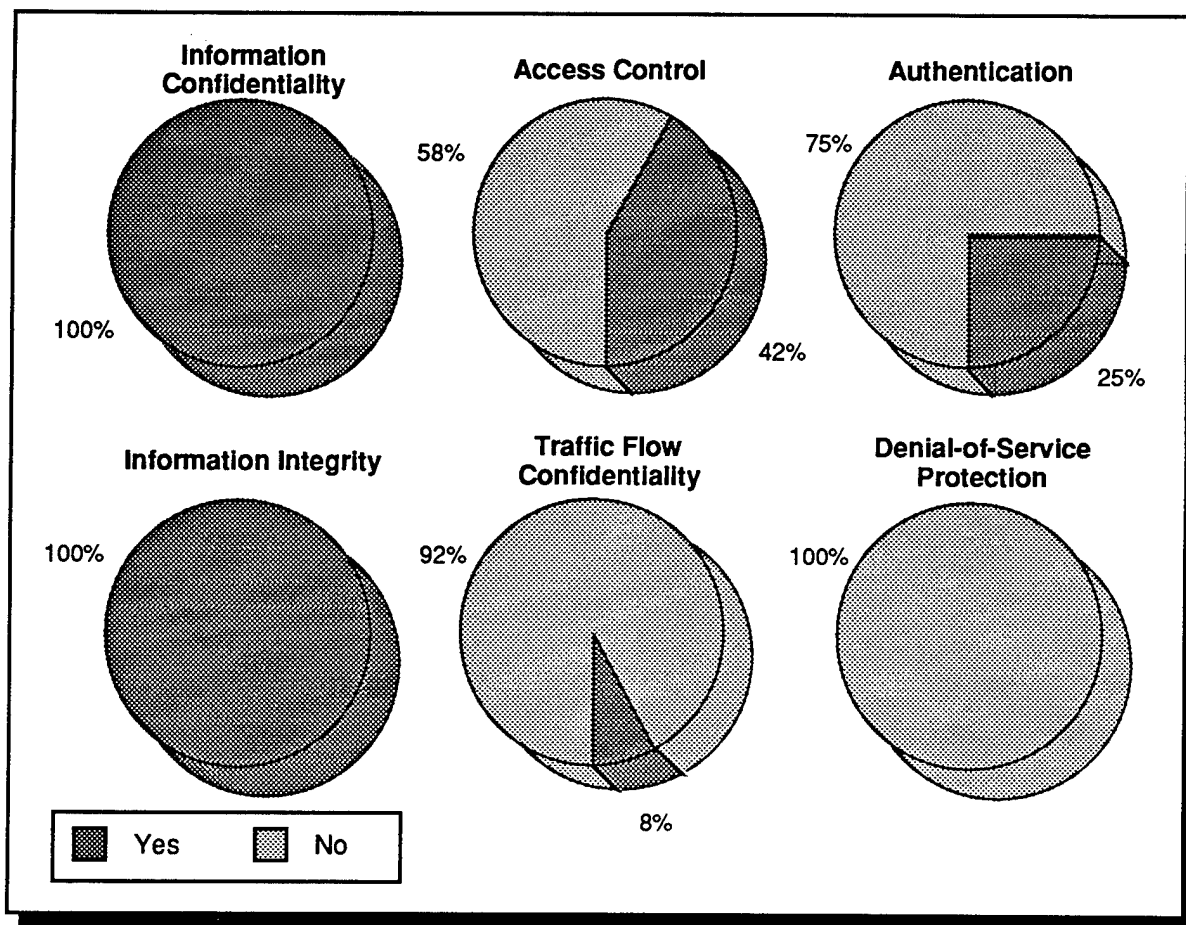
Because the majority of land-mobile products support some form of encryption, information integrity and information confidentiality services are universally available in the reviewed products, as shown in Exhibit 4-15. Authentication, through PINs or

**EXHIBIT 4-14**  
**Types of Land-Mobile Radio Products**



03.134.93-4-24

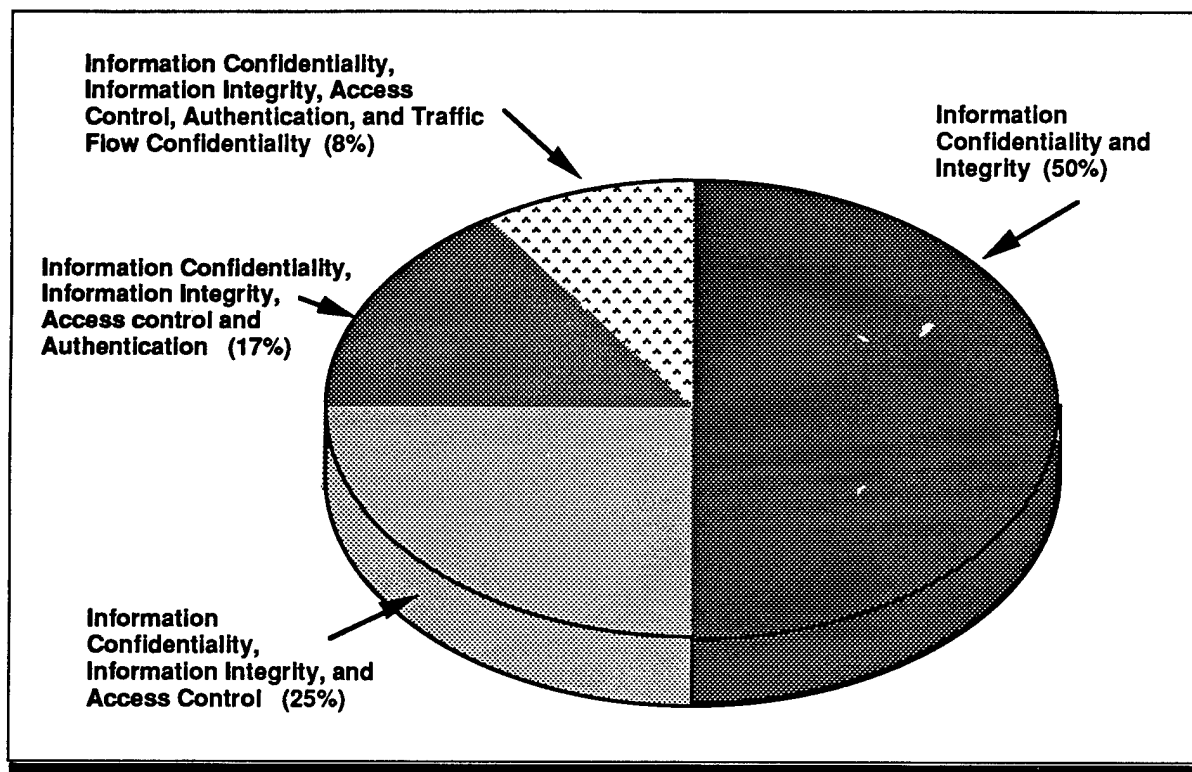
**EXHIBIT 4-15**  
**Security Services for Land-Mobile Radio**



03.134.93-4-25

user codes, and access control, generally in the form of a dispatcher-controlled remote kill function, are less common. Traffic flow confidentiality is supported in the only non-encryption-based product by use of a proprietary frequency-hopping technique. Exhibit 4-16 illustrates the distribution of security services available in the surveyed products.

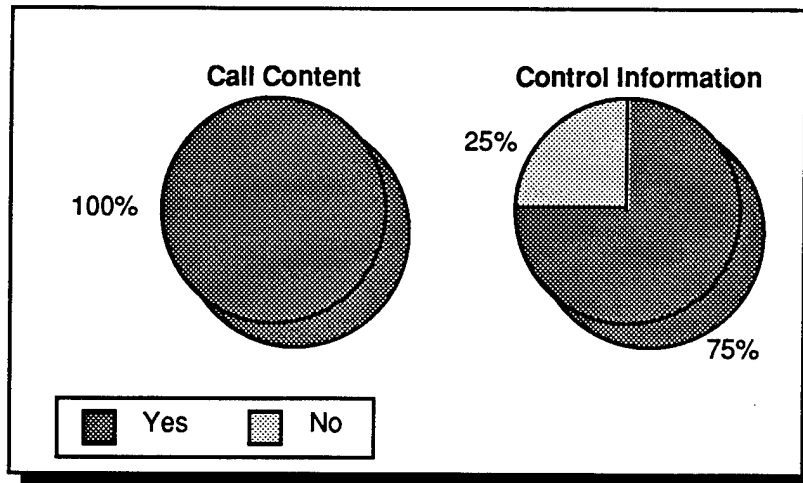
**EXHIBIT 4-16**  
**Land-Mobile Radio—Distribution**  
**of Security Services**



03.134.93-4-32

The objective in using land-mobile security products is to safeguard user conversations from unintended eavesdropping. Consequently, as Exhibit 4-17 shows, all of the products protect call content. Furthermore, since control information is usually passed in-band, it often undergoes the same security measures as the call content.

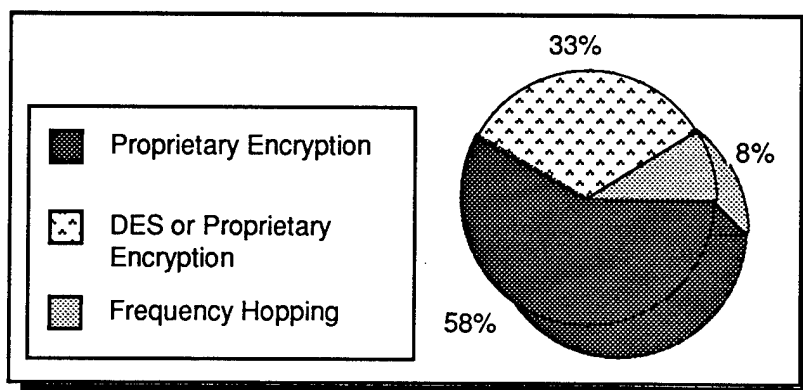
**EXHIBIT 4-17**  
**Land-Mobile Radio—Types of Information Protected**



03.1334.93-4-26

As stated earlier, most of the reviewed products protect communications with encryption-based methods except for the only nonencrypted product, which uses frequency-hopping (see Exhibit 4-18). Customers may choose, however, between DES and the proprietary encryption scheme. By providing multiple encryption schemes, manufacturers allow the customer to decide whether to interoperate with systems based on federal standards or receive additional security that some of the proprietary systems provide.

**EXHIBIT 4-18**  
**Land-Mobile Radio—Methods of Protecting the Wireless Channel**



03.134.93-4-27

The level of security in the land-mobile products reviewed is generally sufficient for the intended user audience (i.e., Government and commercial users who desire privacy for sensitive communications). These products, however, do not provide sufficient protection for classified information broadcast by land-mobile radios. These products should not be considered for classified missions.

## **4.5 MOBILE SATELLITE SYSTEMS**

Wireless access to satellite service, as described in this report, refers to the ability of the individual user to access a satellite directly, rather than to join a multiplexed data stream with other users through an earth station. This direct access may be through a relatively large terminal, such as the shipboard devices used for accessing some satellite services, luggage-sized terminals that are transportable, or handheld devices planned for Low Earth Orbit (LEO) satellites. Other miniaturized terminals can be used for global positioning, such as Radio Determination Satellite Service, and messaging services. Because none of the positioning and messaging services have any associated security, they have not been included in this analysis.

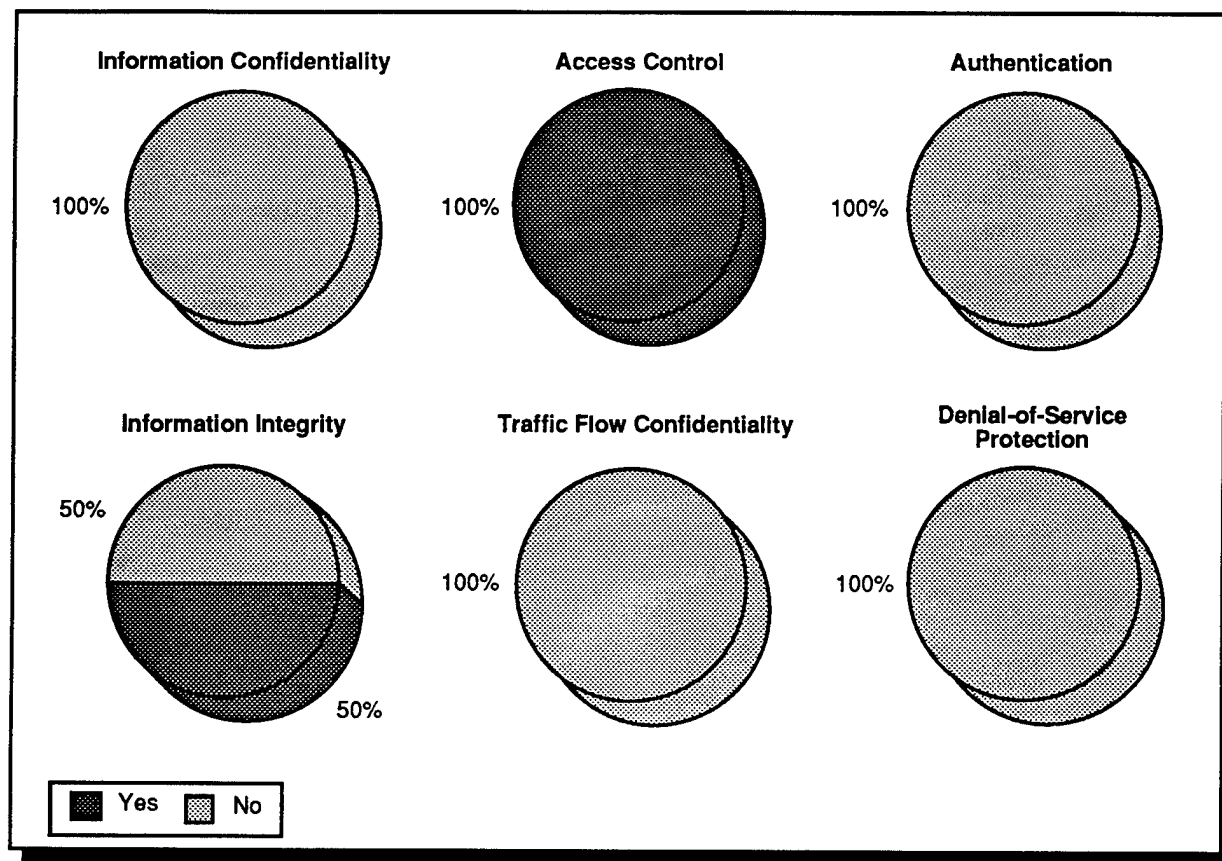
Satellite services, as analyzed in this report, are based upon two types of satellite systems: LEO and Geostationary Earth Orbit (GEO). The LEO systems include "little LEOs" that will provide messaging services and "big LEOs" that will provide duplex voice, data, messaging, and global positioning service. Big LEO systems are oriented toward supplementing access to cellular radio service. The analysis presented below separates GEO systems from LEO systems, as each system has unique characteristics that should be examined separately.

### **4.5.1 GEO Mobile Satellite Systems**

GEO mobile satellite systems serve only as conduits for information being transmitted over their channels; no additional services are provided over the link. Exhibit 4-19 reflects this fact. Some GEO systems use analog transmission techniques, while others use digital transmission techniques; hence, not all GEO systems provide information integrity security service. However, all GEO systems use access control procedures to validate the identity of terminals and ensure that unauthorized users and terminals cannot access the system.



### EXHIBIT 4-19 Security Services for GEO Satellite Systems



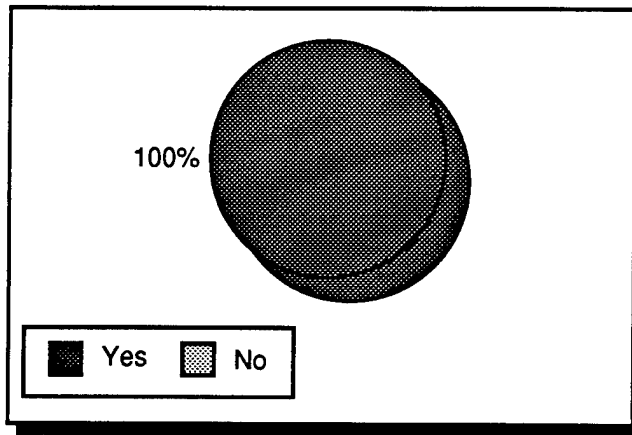
03.134.93-4-09

Although the GEO mobile satellite systems do not provide any information confidentiality, they can pass signals protected by an end-to-end privacy system. As shown in Exhibit 4-20, all GEO systems can pass STU-III signals. A user must hook a STU-III desk phone into a special adapter on the mobile terminal to take advantage of the protection afforded by the STU-III. No other end-to-end privacy systems are available for use with GEO satellite systems.

#### 4.5.2 LEO Mobile Satellite Systems

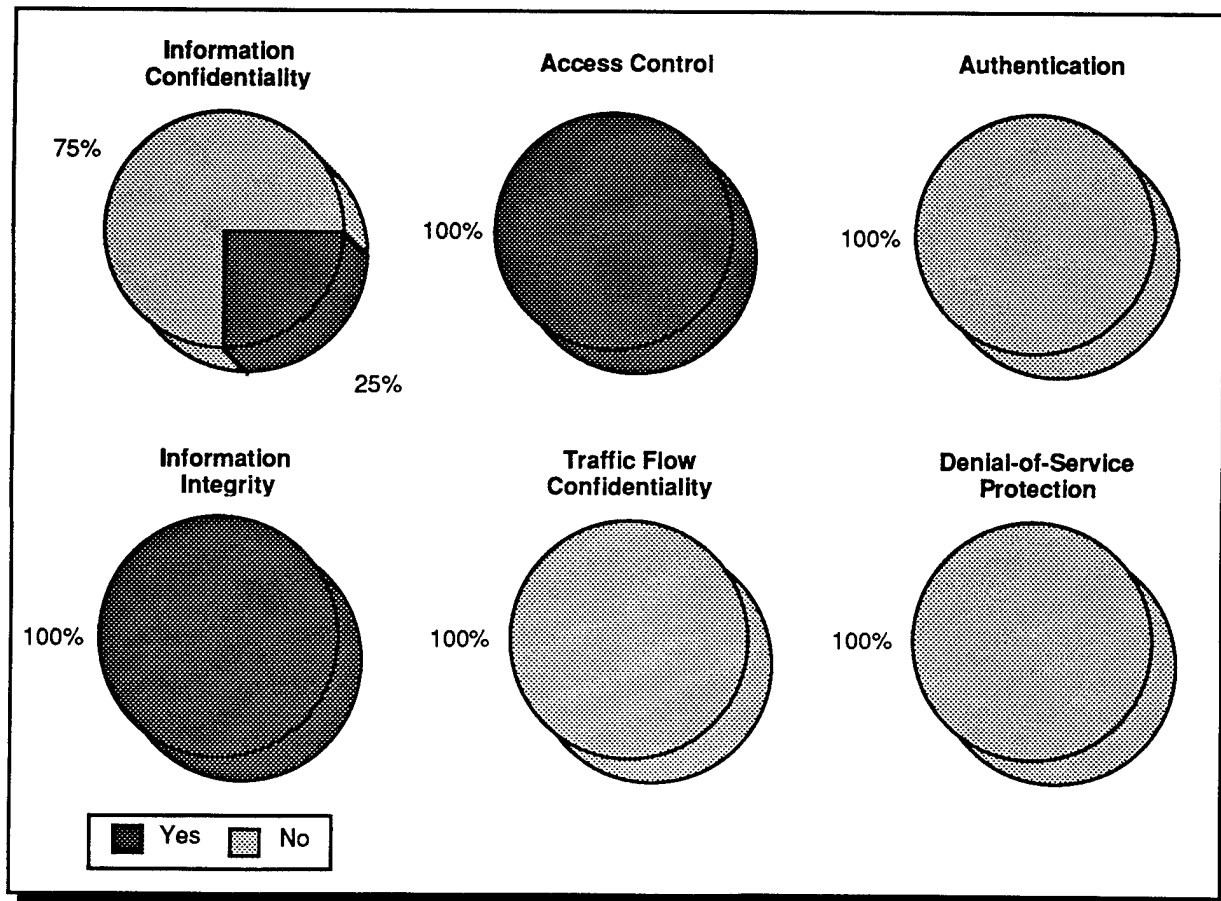
LEO mobile satellite systems are different from GEO satellite systems, especially with respect to privacy and other security measures. Some LEO systems use spread-spectrum techniques for transmission to and from the satellite; therefore, they provide some degree of privacy. Exhibit 4-21 illustrates these points. As noted before, spread spectrum was not designed with privacy as its primary focus; therefore, the privacy

**EXHIBIT 4-20**  
**GEO Satellite Systems—STU-III Compatibility**



03.134.93-4-10

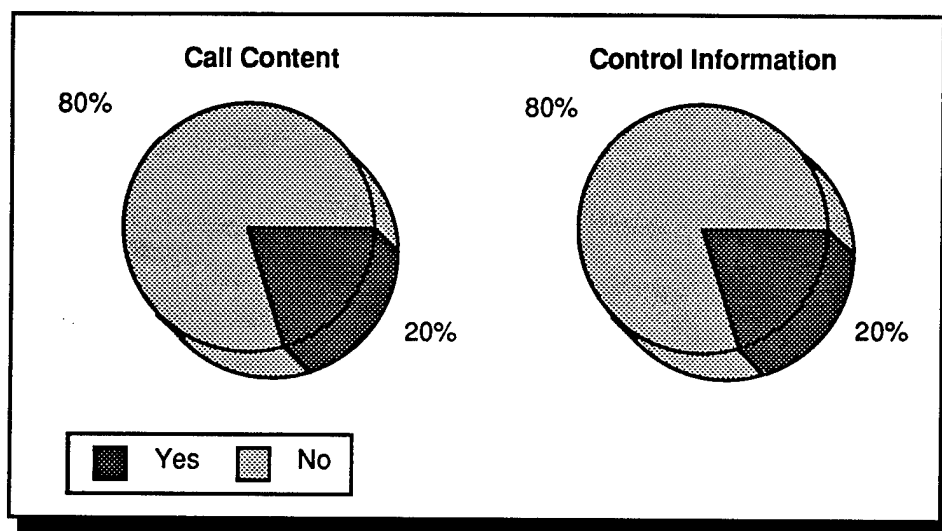
**EXHIBIT 4-21**  
**Security Services for LEO Satellite Systems**



03.134.93-4-11

inherent in spread-spectrum transmissions should not be trusted as the sole measure of privacy for NS/EP use. Due to the nature of the spread-spectrum transmissions, the call content and control information for these LEO satellite systems are protected from casual monitoring; Exhibit 4-22 shows the proportion of the products that provide this protection.

**EXHIBIT 4-22**  
**LEO Satellite Systems—Types of Information Protected**



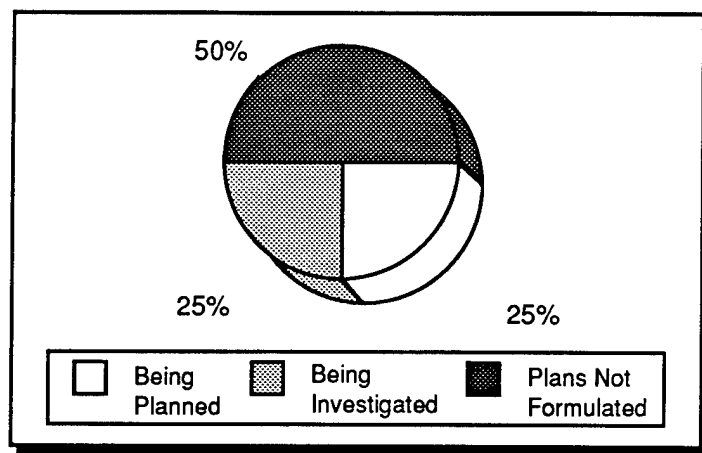
03.134.93-4-12

Some LEO service providers are planning to provide some STU-III interface in the future. Exhibit 4-23 shows the status of STU-III compatibility on various LEO satellite systems. Although approximately 50% of LEO system developers have not formulated plans for STU-III compatibility, they are aware of the potential demand for interoperability with STU-III and may address this concern soon. As with the GEO satellite systems, users wishing privacy on the wireless satellite channel must supply their own end-to-end privacy solution if they are dissatisfied with the protection afforded by spread spectrum.

#### 4.6 PAGING

As a commercial service, electronic paging offers limited information security to service subscribers. The extent of the security is generally confined to PINs and identifier codes built into the pagers themselves. Some carrier systems use PINs to authenticate the user before over-the-phone message retrieval may begin. This is the

**EXHIBIT 4-23**  
**LEO Satellite Systems—STU-III Compatibility**



03.134.93-4-13

same function PINs provide in automatic teller machines and telephone calling cards. Identifier codes, known as “cap” codes, enable delivery of a message only to the intended terminal. For example, the paging service carrier broadcasts all messages intended for a specific geographic area while individual pagers monitor the broadcasts. When the pager recognizes a message containing its “cap” code, the pager retrieves that message and acts according to the predefined pager functions (e.g., beeping or displaying a message on an alphanumeric readout).

Security procedures for paging appear unlikely. According to service providers, there has been almost no demand for any type of secure paging device and they do not foresee any demand in the near future. Commercial paging service exists as an unsecured communications technology with limited privacy.

#### **4.7 WIRELESS LOCAL AREA NETWORKS**

Wireless LANs are designed to provide flexible access to users who often reorganize and to users in spaces difficult to wire. Consequently, the systems can exist as either an add-on system to an existing wireline LAN or as a stand-alone LAN. In most cases, the wireless link between the workstations is 20–200 feet, although there are provisions for outside links and bridges of up to 3 miles. Some wireless LANs use infrared transmission. Vendors of these LANs claim that, because the transmission path is entirely within the sight of the user, it is very secure. Because the signal is not

encrypted or otherwise modified in these systems, infrared LANs are not considered able to provide information protection and were not included in this analysis.

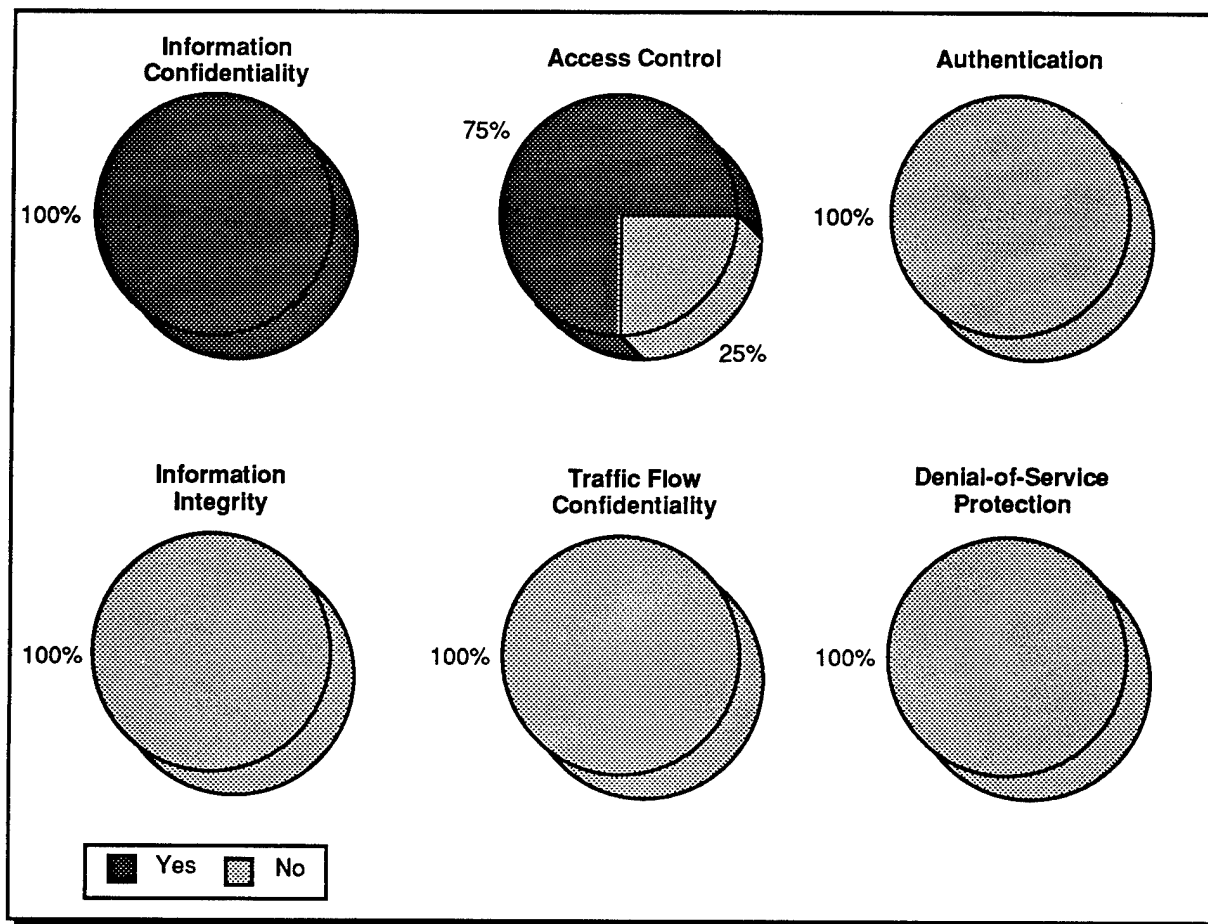
Wireless LANs, in general, provide some basic security services, as illustrated in Exhibit 4-24, and described below:

- **Information Confidentiality.** All but one of the systems analyzed operate in the 902–928 MHz band, which does not require FCC licensing if the power is kept low. Vendors implement this requirement by using spread-spectrum transmission. The effect of this choice is to provide a minimal level of information confidentiality. In addition, half the vendors provide the option for encryption of the information using either a proprietary chip or one based on the National Institute of Standards and Technology (NIST) DES.
- **Access Control.** All systems provide access only to those devices registered to communicate over the network. The network administrator maintains the file of authorized devices. Additionally, networks can be segmented according to the access codes assigned to the end terminals. Devices on these segments can communicate with other segments only through bridges. This ability to segment affords an additional layer of protection for the users on individual segments.
- **Authentication.** No vendors provide authentication because they claim that it is a function of the application layers and that wireless LAN service is provided only at the physical and Media Access Control (MAC) layers.
- **Information Integrity, Traffic Flow Confidentiality, Denial-of-Service Protection.** None of the LANs reviewed provides this sophisticated level of security.

Exhibit 4-25 shows the types of information protected. Many of the LANs reviewed provide some message content protection through the use of spread-spectrum transmission. Some of the LANs reviewed do not use spread-spectrum transmission, although they provide an optional encryption chip.

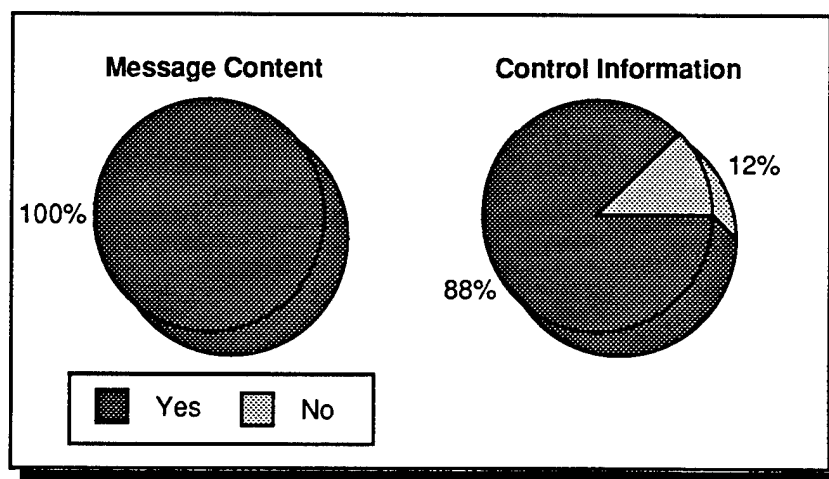
As shown in Exhibit 4-26, the vendors offer considerably different means of protecting the information flow. Half of the manufacturers rely only on spread-spectrum techniques. Of those vendors that provide an encryption option, half use a proprietary algorithm and half use a DES-based chip.

**EXHIBIT 4-24**  
**Security Services for Wireless LANs**



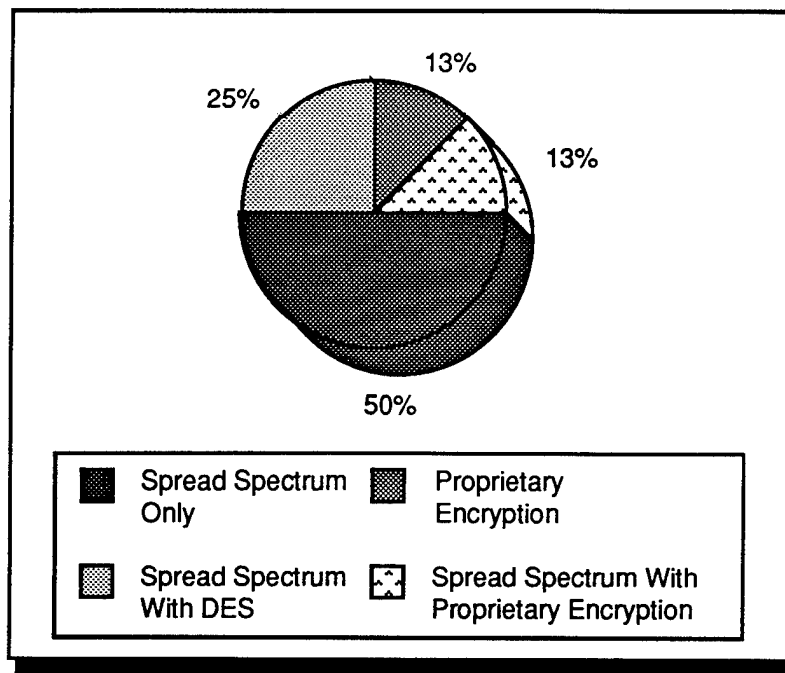
03.134.93-4-14

**EXHIBIT 4-25**  
**Wireless LANs—Types of Information Protected**



03.134.93-4-15

**EXHIBIT 4-26**  
**Wireless LANs—Methods of Protecting the Wireless Channel**



03.134.93-4-16

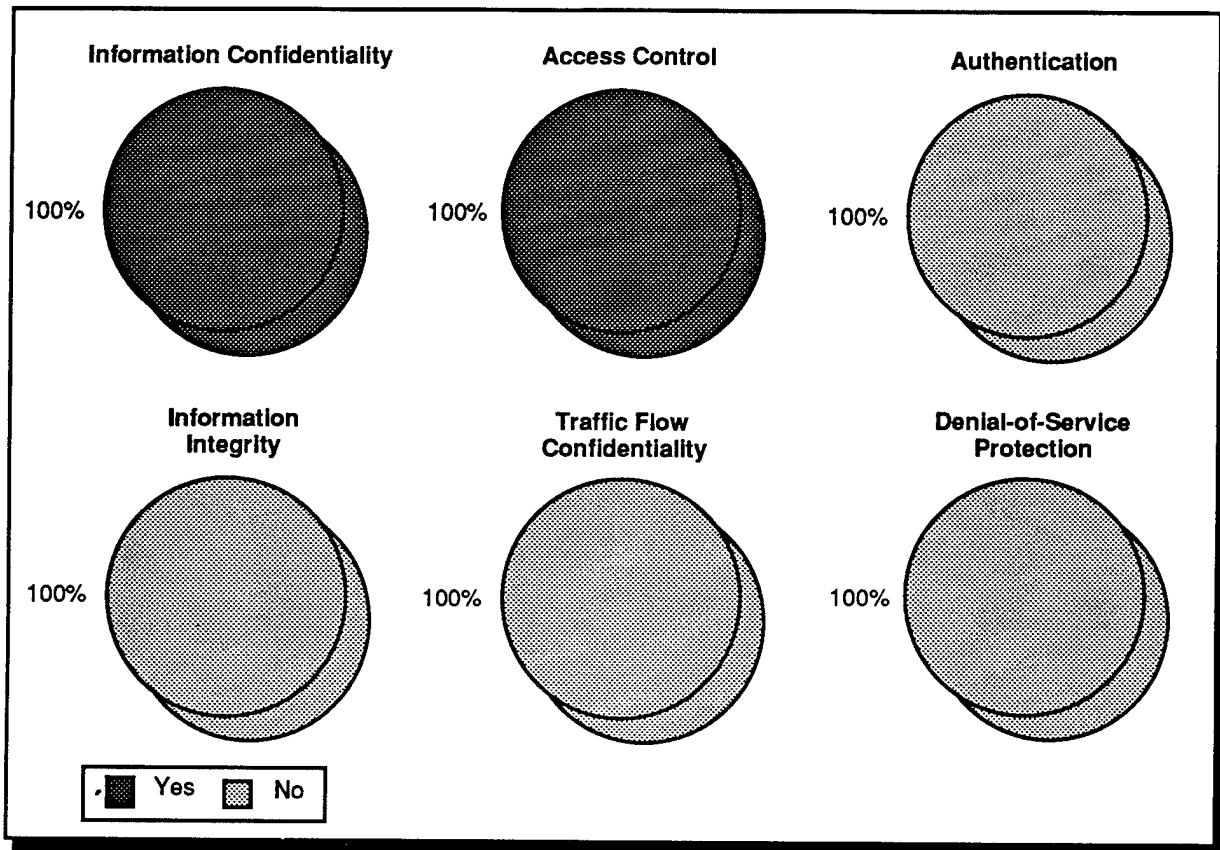
End-to-end protection of information is possible only if both users are on the wireless LAN. Spread-spectrum protection, of course, applies only to the wireless portion of the link between users. In hybrid wireless/wireline systems, encryption covers only that part of the link controlled by the wireless system.

#### **4.8 WIRELESS PRIVATE BRANCH EXCHANGES**

The devices known as wireless PBXs provide only wireless access to existing PBX or Centrex users. The PBX functionality extends into a cellular type of system constructed within a well-defined area, usually inside a corporate facility, and sometimes covering the immediate vicinity outside as well. Exhibit 4-27 shows the security services provided by the wireless PBXs surveyed.

Wireless extensions to PBXs are uncommon, and few provide security services. In at least one case, the optional proprietary chip advertised as providing security has not yet been implemented. In those cases where protection is available as a result of either the spread-spectrum transmission or an encryption chip, the wireless link is the

**EXHIBIT 4-27**  
**Security Services for Wireless PBXs**



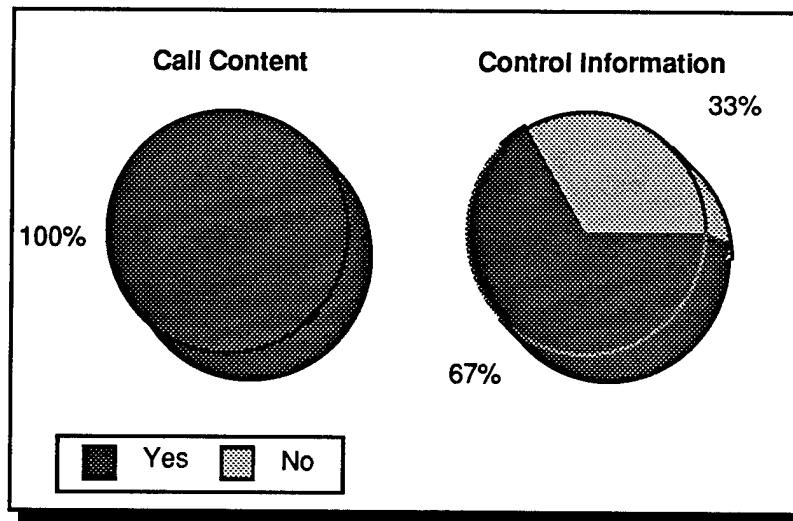
03.134.93-4-17

only part of a call that is protected. Even when the call is between two users in the same wireless system, the call content loses its protection when it is sent to the PBX for switching. The call is reprotected when it is again placed on a wireless link. Another system employs a spread-spectrum CDMA technique that effectively increases the level of privacy. As shown in Exhibit 4-28, privacy is provided for call content; the spread-spectrum wireless PBXs also protect the control information.

All systems provide access only to those devices registered with the system. Because the system administrator maintains the file of authorized devices, access control is strong. Only one system provides authentication; however, it does not protect message content and therefore was not included in the analysis. Generally, the position of the vendors was that authentication was a service appropriate for the PBX (e.g., by



**EXHIBIT 4-28**  
**Wireless PBXs—Types of Information Protected**



03.134.93-4-18

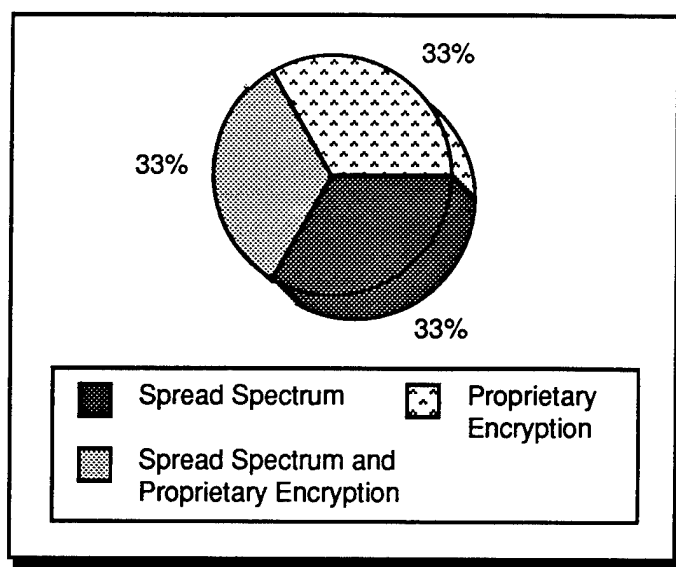
the use of PINs) and not for the wireless access system. Wireless PBXs do not support information integrity, traffic flow confidentiality, and denial-of-service protection.

Exhibit 4-29 shows the different methods used to protect the wireless link. Of those systems that provide information confidentiality, most depend on spread-spectrum transmission to provide the protection. Additionally, one system employs CDMA; its manufacturer asserted that the coding associated with this access technology is probably as effective a means of protection as the coding in the spread spectrum. These systems, of course, protect the control information as well as the call content. One of these systems will provide an optional proprietary encryption chip in the future. Another system does not provide the protection of spread spectrum but does include an optional proprietary encryption chip.

#### **4.9 WIRELESS SUBSCRIBER LOOPS**

Wireless subscriber loops provide alternative wireless access to the PSN, much like cellular radio and other wireless services. Wireless subscriber loops often replace the wireline link from a telephone company's central office to the homes or offices of its subscribers. Regular analog phones are connected to a transceiver that communicates

**EXHIBIT 4-29**  
**Wireless PBXs—Methods of Protecting the Wireless Channel**



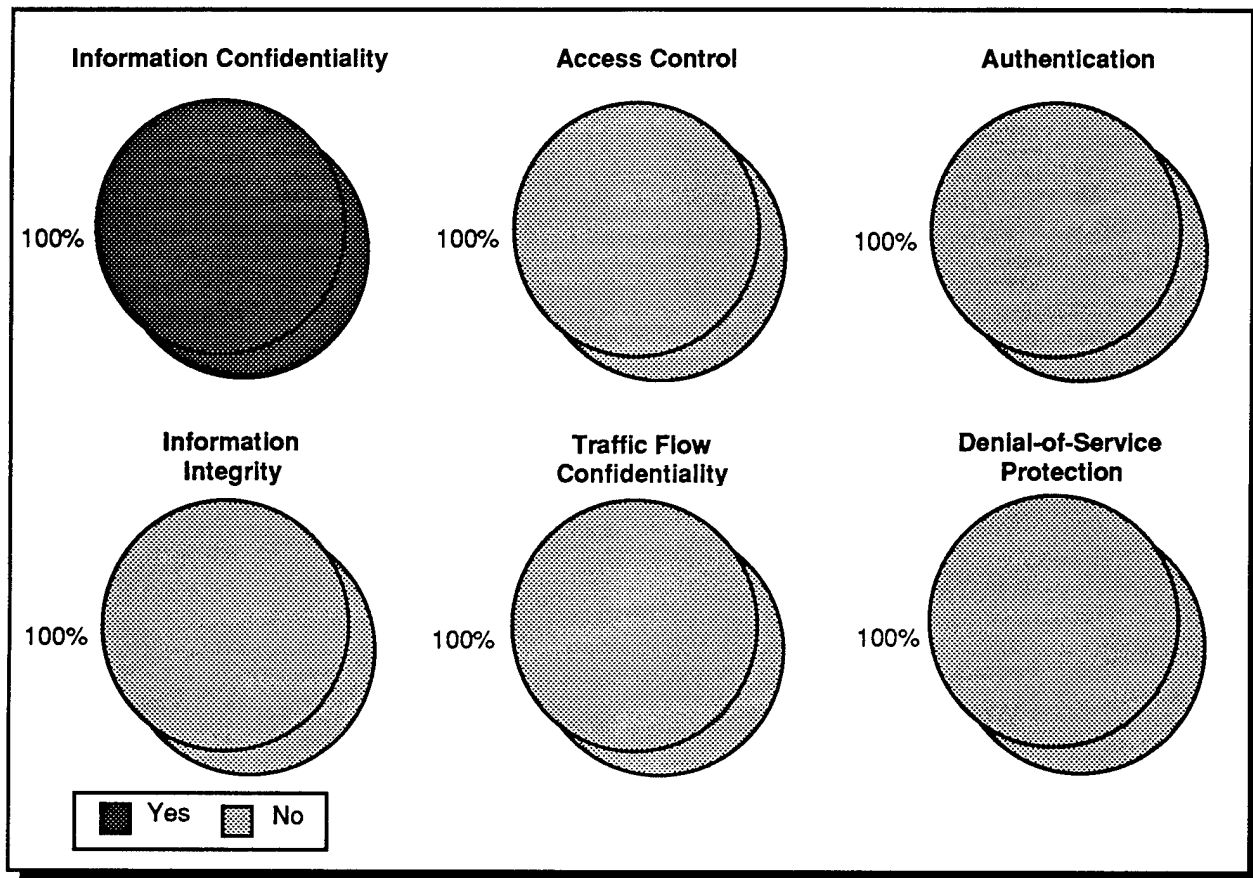
03.134.93-4-19

with a base station connected to the central office. The links will carry any traffic that is normally passed over standard analog phone lines, such as voice and low-speed data.

Because wireless subscriber loops are intended as a link connection without providing any additional services, manufacturers of wireless subscriber loops have not designed any additional security measures into their products (see Exhibit 4-30). Some digital wireless loops provide weak information confidentiality through means not designed specifically for privacy but to maximize bandwidth efficiency. In general, wireless subscriber loops are intended for use as point-to-point or point-to-multipoint communication links.

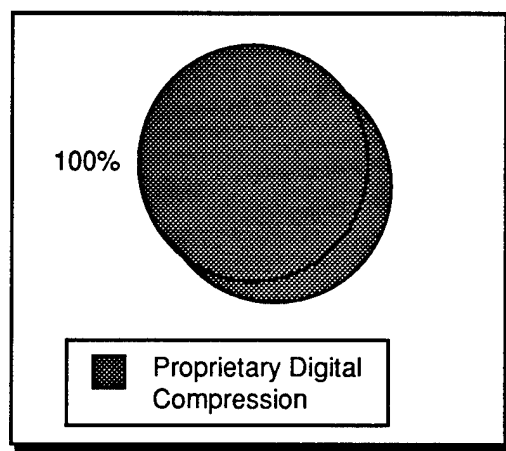
In some digital wireless loops, the manufacturers employ a proprietary compression scheme, as shown in Exhibit 4-31. This approach can provide very limited privacy from casual eavesdropping or monitoring, as shown in Exhibit 4-30. Any sophisticated eavesdropper could readily obtain the transmitted information with the proper monitoring equipment. Analog wireless subscriber loops do not use a digital compression scheme on their transmissions; therefore, the transmissions are not protected in any way.

# **EXHIBIT 4-30** **Security Services for Wireless Subscriber Loops**



03.134.93-4-20

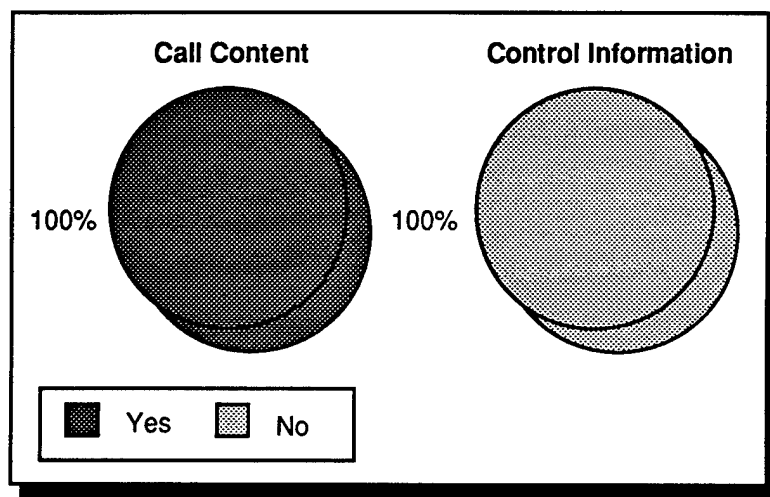
# **EXHIBIT 4-31** **Wireless Subscriber Loop—Methods of Protecting the Wireless Channel**



03.134.93-4-22

Exhibit 4-32 shows the types of information protected by data compression schemes. Often, wireless loops utilize both in-band and out-of-band signaling to pass control information. The out-of-band signaling information is not "protected" by the compression algorithm; therefore, some location data passed on the control channel may be subject to eavesdropping.

**EXHIBIT 4-32**  
**Wireless Subscriber Loop—Types of Information Protected**



03.134.93-4-21

If wireless subscriber loop customers need secure transmission capabilities, they should provide their own end-to-end solution. Often, this can be done with the same equipment used in the wireline environment. One example that would satisfy NS/EP requirements is a STU-III. Most wireless loops, whether analog or digital, can pass STU-III traffic. There are other end-to-end desktop security solutions, but they may not satisfy all of the security requirements of a given NS/EP mission. A discussion of these products is outside the scope of this TIB.

## 5.0 FINDINGS

## 5.0 FINDINGS

This TIB shows a wide variation in applied security services among various wireless services. Some wireless services are only link services that provide little security. Others have a relatively mature subscriber base and are beginning to address subscribers' needs for privacy and additional security. This chapter summarizes the findings of the analysis presented in Chapter 4 and some of the implications of these findings.

- *Six security services are critical for providing complete security in the wireless environment: information confidentiality, information integrity, access control, authentication, traffic-flow confidentiality, and denial-of-service protection.* None of the products surveyed provides all six security services. Further analysis of the NS/EP wireless services security environment may show, however, that some of these services may be optional.
- *Information confidentiality, also referred to as privacy, is the most common security service and is provided in the vast majority of surveyed projects.* Several techniques provide privacy, although not all were designed with privacy as a primary concern. These techniques include digital compression, spread-spectrum transmissions, proprietary scrambling and encryption algorithms, NIST-approved encryption algorithms (e.g., DES), and National Security Agency (NSA)-approved algorithms (e.g., STU-III). With digital compression, privacy depends on the monitoring party's not knowing the algorithm, which provides some protection to transmitted information. With spread-spectrum transmission techniques, privacy depends on the monitoring party's not having the pseudorandom codes.
- *Air-to-ground telephone service uses digital compression schemes as a bandwidth compression scheme, thereby affording a minimal level of privacy to the information.* This privacy can be easily compromised by a receiving party that knows the compression algorithm. *All air-to-ground telephone service providers are considering or implementing STU-III interfaces on their networks.* The STU-III interface can be installed for requesting parties on a case-by-case basis.
- *Privacy seems to be the primary security concern of cellular subscribers, and all products surveyed provide some level of information confidentiality through techniques ranging from spread-spectrum transmissions to STU-III terminals.* Some cellular products also provide other security services, such as authentication and access control. Cellular radio service has a large subscriber base that has a growing need to protect the privacy of conversations. The spread-spectrum techniques used in the new generation of dual-mode cellular radios are being marketed as providing adequate privacy protection for subscribers. These techniques, however, may not suffice for NS/EP users.

- *The more recent generations of cordless telephones support various privacy techniques, although cordless telephone technology is historically not a secure technology. CT-2Plus and CT-3 support proprietary encryption algorithms, while spread-spectrum cordless phones may offer increased levels of privacy. Furthermore, it should be noted that the surveyed CT-2Plus and CT-3 products do not include the encryption modules to protect the wireless link.*
- *Privacy and information integrity are the primary security concerns of land-mobile radio users; some systems also offer access control and authentication procedures to system users. Land-mobile radio products are a well-established segment of the wireless communications market. Almost all land-mobile radio products use some type of encryption algorithm to protect transmitted information. Land-mobile products do not provide access to the PSN and are usually used to establish local radio networks for communication between mobile users. Land-mobile radio was one of the first wireless technologies to be developed and used extensively, especially by emergency personnel.*
- *Mobile satellite systems themselves do not provide added privacy over the wireless link, except for privacy provided on some spread-spectrum links; however, many systems support STU-III connectivity to user terminals for communication into the PSN. Mobile satellite systems serve as link services, passing information derived from earth stations connected to the PSN or cellular networks or mobile terminals carried by the subscriber. When the digital transmissions of the service are used, information integrity and access control measures ensure that registered users and terminals can access the satellite.*
- *There is no demand for privacy or security for paging service. No paging service providers offer any devices for privacy or security of paging transmissions because user groups have not expressed a desire for a secure paging devices.*
- *Some wireless LANs use spread spectrum or DES chips to provide privacy on the wireless links; access control measures control the reception of data at specified network nodes. Privacy of data transmitted on wireless LANs is a major concern of wireless LAN users. In response, manufacturers have been implementing encryption schemes to protect information broadcast on wireless LANs.*
- *Most wireless PBXs use spread-spectrum transmissions; some also use a proprietary encryption module to supplement the privacy inherent in spread spectrum. Access control is used to prevent unauthorized terminals from accessing and using the system. Currently, wireless PBXs must be attached to a standard PBX; wireless PBXs can only provide supplemental service through the PBX. Some terminals used for wireless PBXs are also used in cordless telephone systems.*

- *The privacy provided by wireless subscriber loops is a secondary effect of the digital compression scheme used primarily for bandwidth efficiency. Wireless subscriber loops serve only as an alternative access method to the PSN and provide only link services.*
- *Very few of the products surveyed have been submitted to the Government for accreditation and compliance testing. Standards have been established for DES algorithms and STU-III products, the latter being tightly controlled by NSA. Commercially available security services for wireless communications that do not meet Government levels of acceptability are of limited usefulness to NS/EP users.*
- *The security services and mechanisms commercially available for most wireless communications do not provide adequate security or privacy protection against the classic and accepted threats to the PSN (hence to the NS/EP telecommunications infrastructure). The threats to the PSN include collection by foreign intelligence, unconventional threats (such as warfare, terrorism, sabotage activity, and electronic intrusion or hackers), electronic warfare, and offensive warfare systems (Ref. 7). Most products surveyed for this TIB, with the exception of Type 1 STU-III products, were not designed to protect against these threats.*
- *The use of commercially available security services for wireless communications should be considered only for sensitive-but-unclassified information. The algorithms used for most commercial security mechanisms have not been approved by NSA for protecting classified Government information. General public users create most of the demand for commercially available security services for wireless communications, and non-Government-approved algorithms satisfy the commercial demand. For situations where the same NS/EP users exchange only sensitive-but-unclassified information via wireless communications, the acquisition of a commercially available security mechanism may be cost-effective. The alternative is to acquire and use Government-approved security services, which tend to be more costly and complex and provide services that may never be used.*
- *The minimum security objectives for wireless communications should be (1) to prevent inappropriate access to PSN network services and features, (2) to detect unauthorized access, and (3) to plan for an overarching security architecture that includes all wireless means. These objectives are commensurate with the assumed risks: diminution of the operational effectiveness of NS/EP personnel, loss and misuse of Government information, and unauthorized access to or modification of the information carried by wireless means.*
- *Uncontrolled use of commercially available security services for wireless communications may create islands of NS/EP users within the NCS whose systems are incompatible with larger systems. NS/EP users can acquire and use commercially available security mechanisms and services unless prohibited from doing so by policy and guidance. Users of these*



mechanisms and devices may create interoperability problems, however, when communicating with NS/EP users that do not have compatible security support.

- *The NCS should establish a method to control the configurations and use of security services or mechanisms employed by NS/EP users. The objective of the OMNCS should be to reduce the inventory of available security services or mechanisms to one common set for NS/EP use, eliminating the possibility of isolated islands of NS/EP users with incompatible secure terminals.*
- *Security services or mechanisms for wireless communications that interface with the PSN need to be at least as strong as the security protection provided by PSN service providers. All security services or mechanisms employed by NS/EP users should be compliant with the overall security objectives defined in the NCS target architecture. Wireless communications can provide a vulnerable "backdoor" extension to PSN services and components.*
- *Local link security services, such as encryption, are more applicable to cordless telephones, wireless PBXs, and wireless LANs. For wireless extensions that are inherently more resistant to intentional or unintentional intrusion because of their somewhat controlled operating surroundings, local link security services may be the most cost-effective solution. A localized threat assessment will determine the adequacy of local link security services.*
- *Due to the large number of different service providers in wide-area services, such as cellular radio, end-to-end security solutions may be more cost-effective than coordinating link security solutions with individual service providers. Installing link security services in multiple networks to allow nationwide secure communications for NS/EP users can become extremely expensive. Implementation of end-to-end security solutions that can pass through a targeted service type, such as cellular radio, may be more cost-effective.*
- *Joint Government and industry action is needed to address the NS/EP security requirements for wireless communications. This study indicates that there is little demand for commercial-off-the-shelf wireless security services that satisfy Government security requirements or provide protection in the PSN. Together, Government and industry could define and relate NS/EP security requirements to these vendors. The OMNCS should develop and publish standards and guidelines for the use of security services for wireless communications.*
- *Research and studies are needed to determine the nature and extent of the vulnerabilities of wireless communications and to develop cost-effective solutions for providing security and privacy of sensitive Government information transmitted via wireless communications. This recommendation is based on an assumed threat to wireless communications. An accurate and complete security architecture cannot be developed without a comprehensive, Government-approved threat assessment.*

- *The OMNCS should develop a security architecture based on end-to-end protection to enhance network security.* The PSN is increasingly reliant on computer networks for timely, reliable, accurate, and secure dissemination of information. Network security requirements include protecting traffic from disclosure to unauthorized persons, detecting unauthorized modification of network traffic, and alerting security officials of attempts by unauthorized persons or processes to masquerade as legitimate network participants. End-to-end security services that provide encryption, integrity encoding, and digital signature enforce the system security policies and control access to the network resources. Cellular, satellite, land-mobile radio, and personal communications networks are best supported by end-to-end security services.
- *The OMNCS needs to continue its participation in wireless and security standards-making bodies to ensure that standards are being developed that support NS/EP requirements for security and privacy.* The OMNCS can promulgate NS/EP requirements for security services for wireless communications to ensure that industry knows the Government will acquire or use only products that comply with its requirements. The OMNCS should continue to participate in at least the Integrated Services Digital Network (ISDN) Users' Forum, the Telecommunications Industry Association (TIA) Committee TR45 for Digital Cellular, the American National Standards Institute (ANSI) T1P1 and T1S1 Subcommittees, and appropriate land-mobile radio activities. The objective is to influence the processes for ensuring common, uniform, and transparent features within the various wireless networks necessary to support the interoperable information security component of the NCS target architecture.

## ACRONYMS AND ABBREVIATIONS

## ACRONYMS AND ABBREVIATIONS

|          |                                                                    |
|----------|--------------------------------------------------------------------|
| ANSI     | American National Standards Institute                              |
| Bellcore | Bell Communications Research                                       |
| CB       | Citizen Band                                                       |
| CCIR     | International Radiocommunications Consultative Committee           |
| CDMA     | Code Division Multiple Access                                      |
| CFR      | Code of Federal Regulations                                        |
| CT       | Cordless Telephone                                                 |
| CT-2     | Second-Generation Cordless Telephone                               |
| CT-3     | Third-Generation Cordless Telephone                                |
| DES      | Digital Encryption Standard                                        |
| FCC      | Federal Communications Commission                                  |
| FDMA     | Frequency Division Multiple Access                                 |
| FM       | Frequency Modulation                                               |
| FPLMTS   | Future Public Land Mobile Telecommunications System                |
| kb/s     | Kilobits per Second                                                |
| kHz      | Kilohertz                                                          |
| LAN      | Local Area Network                                                 |
| LEO      | Low Earth Orbit                                                    |
| MAC      | Media Access Control                                               |
| MHz      | Megahertz                                                          |
| MSC      | Mobile Switching Center                                            |
| MSS      | Mobile Satellite Systems                                           |
| NCS      | National Communications System                                     |
| NIST     | National Institute of Standards and Technology                     |
| NS/EP    | National Security and Emergency Preparedness                       |
| NSA      | National Security Agency                                           |
| NSTAC    | National Security Telecommunications Advisory Committee            |
| NT       | Office of Technology and Standards, National Communications System |
| OMNCS    | Office of the Manager, National Communications System              |
| PBX      | Private Branch Exchange                                            |

|         |                                         |
|---------|-----------------------------------------|
| PCM     | Pulse Code Modulation                   |
| PIN     | Personal Identification Number          |
| PSN     | Public Switched Network                 |
| RF      | Radio Frequency                         |
| STU-III | Secure Telephone Unit, Third Generation |
| TIA     | Telecommunications Industry Association |
| TIB     | Technical Information Bulletin          |

## REFERENCES

## REFERENCES

1. Dean, R., *NSA's View of Wireless Standards*, presentation to the National Security Telecommunications Advisory Committee (NSTAC) Wireless Task Force, 16 June 1992.
2. NSTAC, *Final Report of the Network Security Task Force*, July 1992.
3. Haykin, S., *Communications Systems*, John Wiley & Sons, Inc., New York, 1983).
4. *Roget's II*, F. deM. Vianna ed., Houghton Mifflin Company, Boston, 1980).
5. Beker, H. J., and Piper, F. C., *Secure Speech Communications*, Academic Press, Inc., Orlando, Florida, 1985).
6. Telephone interview with Ted Lee, Bell Communications Research Inc., January 1993.
7. OMNCS, *Status Report on the Development of the Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications*, 1 December 1992.

## GLOSSARY



## GLOSSARY

**Access Control.** A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs and/or to obtain data from, or place data onto, a storage device (Ref. 1 and Ref. 4). For example, access control applies to determining whether a wireless terminal is a legitimate terminal in a given wireless network.

**Air-Ground Radiotelephone Service.** A public radio service between a base station and airborne mobile stations (Ref. 1). Subscriber service is obtained through the airborne mobile station.

**Authentication.** The process of verifying the identity of a user, terminal, application program, or service provider. This is a security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission message or originator (Ref. 1).

**Cellular Radio System/Service.** A radio system providing wireless service to a mobile subscriber. Low power, limited range, interconnected transmitters provide coverage over small areas (cells). Such a system allows frequencies to be reused economically in non-adjacent cells and provides service to multiple users within the cell. The system will hand off subscribers as they move between cells at automotive speeds. Cellular systems provide access to and egress from the Public Switched Network (PSN), and calls may be switched within the cellular system or forwarded through a controller to the PSN for completion.

**Confidentiality.** Assurance that information is protected against disclosure to unauthorized persons, programs, or systems (Ref. 4).

**Cordless Telephone System.** A communications system consisting of two transceivers, one a base station that connects to the PSN and the other a mobile handset unit that communicates directly with the base station (using radio frequency [RF] transmission) (Ref. 4). There are four technologies currently supporting cordless telephones:

- **CT-1** (Cordless Telephone, first generation) provides analog transmit-only service from the handset.
- **CT-2** (Cordless Telephone, second generation) provides digital frequency division multiple access, and *permits* two-way telephone communications. Not all CT-2 implementations support two-way communications.
- **CT-2Plus** permits encryption and faster call setup, in addition to normal CT-2 service.
- **CT-3** (Cordless Telephone, third generation) is a proprietary time division, multiple access scheme based on Digital European Cordless Telecommunications (DECT), which supports encryption.

**Cover.** To convert the transmitted waveform into an unusable form by means of communications and information security and cryptographic techniques (Ref. 1).

**Data Encryption Standard (DES).** A cryptographic algorithm for the protection of unclassified computer data, issued as Federal Information Processing Standard Publication 46-1 and intended for public and Government use (Ref. 1).

**Denial of Service.** The prevention of authorized access to system assets or services, or the delaying of time-critical operations (Ref. 4).

**Eavesdropping.** The unauthorized interception of information-bearing emanations through the use of methods other than wiretapping (Ref. 1).

**Encipher.** To convert plain text into a form unintelligible to untrusted individuals or processes by means of a cipher system (Ref. 1).

**Encode.** To convert data by the use of a code, frequently one consisting of binary numbers, in such a manner that reconversion to the original form is possible (Ref. 1).

**Encrypt.** To convert plain text into a form unintelligible to untrusted individuals or processes by means of a crypto system<sup>1</sup> (Ref. 1). Encryption also supports authentication and may support information integrity and access control.

---

<sup>1</sup>The meaning of the term "*encrypt*" is similar to that of the terms "*encipher*" and "*encode*."

**Hacker.** A computer enthusiast with the drive to master the computer and computer systems, a term often associated with computer criminal (Refs. 2 and 5).

**Information Integrity.** Assurance that information, data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems (Ref. 2).

**Information Security.** The protection of information from unauthorized modification, destruction, or disclosure resulting from all measures designed to deny to unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study (Ref. 1).

**Intrusion.** The act of joining a communications circuit without permission or authority, usually with the intention of causing a distraction or disrupting communications.

**Land-Mobile Radio.** A mobile service between base stations and land-mobile stations or between land-mobile stations. A mobile station is capable of surface movement within the geographical limits of a country or continent (Ref. 1).

**Masquerading.** Assuming the identity of another party that has authorization to perform operations not authorized for some parties (Ref. 3).

**Mobile Satellite Systems/Service.** Systems/services that allow subscribers direct access to a satellite. Mobile satellite systems/services range from fixed GEO satellite service to individuals to service from nonstationary, LEO satellites.

**Monitoring.** The unauthorized observation of information passing between users over a communications channel.

**Paging Service.** A one-way wireless radio service to provide a message to the subscriber. The subscriber's receiver is usually no larger than a package of cigarettes. In very elementary systems, the alert may be a "beep" to trigger a pre-defined response, such as to telephone a base office. In more flexible systems, a short message may be transmitted to the subscriber.

**Phone Phreak.** A telephone system hacker. The phreak's primary interest appears to be mastery of the system complexities rather than completion of a free call (Ref. 2). Phone phreaks, as opposed to petty phone thieves, "explore the system" for the sake of "intellectual" challenge (Ref. 5).

**Privacy.** The ability to control or influence access to user information and protect such information from disclosure (Ref. 3).

**Public Key Encryption.** An asymmetric encryption system in which each subscriber has a pair (public and private) of keys. The public key is made available for others to use when communicating with the subscriber and is obtained from a certification authority trusted by the key owner. The subscriber, upon receiving a message, decrypts the message with the private key.

**Scramble.** To modify a transmitted digital signal by altering the order of the bits or to modify an analog signal by distorting the waveform.

**Secure Telephone Unit (STU).** A U.S. Government-approved telecommunications terminal designed to protect the transmission of sensitive or classified information in the voice, data, and facsimile modes (Ref. 1). The current model is the third generation of STU products (STU-III).

**Security.** The condition achieved when designated information, material, personnel, activities, and installations are protected against espionage, sabotage, subversion, and terrorism as well as against loss or unauthorized disclosure. The term is also applied to those measures necessary to achieve this condition (Ref. 1).

**Spread Spectrum.** A signal-structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy and increasing the immunity of spread-spectrum receivers to noise and interference. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wide band of frequencies. The receiver correlates the signals to retrieve the original information signal (Ref. 1).

**Tetherless Channel.** An unrestrained, unlimited communications channel.

**Traffic Flow Analysis.** The analysis of traffic and signaling patterns over time, in the hope that pattern changes may indicate identifiable changes in operations or provide intelligence about a target individual or organization.

**Unbounded Channel.** Having no bound, unlimited in extent, degree, or quantity; unchecked, uncontained, unrestrained; having no ends or limits.

**Wireless.** Communications that use an unbounded and tetherless channel to propagate information signals through free space and atmosphere in the form of electromagnetic radiation.

**Wireless Local Area Network (LAN).** A data system that provides wireless access to a wireline LANs or can operate as a stand-alone LAN.

**Wireless Private Branch Exchange (PBX).** A system that provides two-way wireless access to an existing PBX. The systems do not perform any switching and add no features to those provided by the PBX.

**Wireless Subscriber Loop.** A wireless means of access to and egress from PSN services. Wireless subscriber loops provide a link to the central office and perform no other telecommunication services.

**Wireless Communications.** Communications that use a wireless channel rather than transmission lines or optical fiber. Users of wireless communications are generally mobile, from foot-speed to airborne-speed users.

## REFERENCES

## REFERENCES

1. Dean, R., *NSA's View of Wireless Standards*, presentation to the National Security Telecommunications Advisory Committee (NSTAC) Wireless Task Force, 16 June 1992.
2. NSTAC, *Final Report of the Network Security Task Force*, July 1992.
3. Haykin, S., *Communications Systems*, John Wiley & Sons, Inc., New York, 1983).
4. *Roget's II*, F. deM. Vianna ed., Houghton Mifflin Company, Boston, 1980).
5. Beker, H. J., and Piper, F. C., *Secure Speech Communications*, Academic Press, Inc., Orlando, Florida, 1985).
6. Telephone interview with Ted Lee, Bell Communications Research Inc., January 1993.
7. OMNCS, *Status Report on the Development of the Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications*, 1 December 1992.