Report of the November 1993 Joint Experts Meeting on Privacy and Authentication for Personal Communications Services Sponsored by Telocator, TR 46, and T1P1

Nov. 8-12, 1993, Phoenix, AZ

Leon S. Scaldeferri
Office of Information Security Research[1]
NSA, R22
9800 Savage Rd.
Ft. Meade MD 20755-6000

(301) - 688 - 0293 /0289[fax]
em: lsscald@alpha.ncsc.mil

1. Opinions expressed in this paper are those of the author and do not represent the opinions or position of the FWUF or NSA.

Report of the November, 1993 Joint Experts Meeting on Privacy and Authentication for personal Communications Services

Telocator, TR 46, and T1P1

November 8-12, 1993

Phoenix, AZ

(extraction and summarization of final report)

1. Background:

Personal Communication Service (PCS) provides the freedom of mobility to users. However, this mobile nature of PCS implies network and service capabilities that subject users and service providers to certain risks. This joint experts meeting was held to explore the risk faced by users and service providers, to determine specific requirements to address these risks, and where possible, to propose methods to meet these requirements.

2. Purpose:

The report was offered to standards organizations, manufacturers, and other interested parties for use in developing detailed standards guiding equipment design and meeting general communications needs.

3. Objectives:

a. Determine the authentication scheme for wireless access to PCS.

b. Establish the minimum level of privacy required for wireless access to PCS.

c. Establish the minimum interoperability requirements for intersystem PCS authentication and privacy.

d. Establish recommendations for privacy and authentication operations needs, including service activation, fraud detection and recovery, and law enforcement.

4. Assumptions:

A list of assumptions were generated which have possible impact on the PCS security architecture. The assumptions were primarily based on the Future Public Land Mobile Telecommunications System (FPLMTS). Briefly the assumptions are as follows;

Near-team availability is a critical factor, based on ambitious FCC timetable.

PCS will be provided in a multi-network-operator and multi-service-provider environment.

PCS will be operated across international and national network boundaries with international and national roaming capabilities.

PCS will have an open architecture, based on Intelligent Network (IN) and Telecommunication Management Network (TMN) concepts.

PCS supports UPT personal mobility.

PCS will provide a variety of services with a range of bit rates.

PCS will provide a range of terminal types.

PCS users and terminals are logically identified with different unique identities.

A PCS user has a service profile, to which he has direct but limited access.

PCS subscribers are allowed to "roam" even within their "home" geographic area.

A PCS handset may be exported anywhere.

The following sections provide a summary of the agreements at the meeting.

5. Objective a: Authentication

This objective addresses the need to protect user and service providers against fraudulent use of services while meeting user and service provider needs. The charge for this meeting was to determine a specific recommendation for the authentication procedures for PCS. A summary of the recommendations follow;

Initially provide support for Secret Key authentication, e.g. IS-54/Is-95, GSM.

Signalling and control should be flexible enough to support Public Key.

Further work should be done on Public Key.

Consideration should be given to implementing a Key Management Center/Authentication Center.

A table was prepared which compared alternative authentication and key agreement systems.

6. Objective b: Privacy

This objective addresses the need to provide privacy for PCS users' call-related information. Work in this area focused on the determination of an acceptable level of privacy for PCS users and the review of schemes which would provide this level of privacy. Related issues, such as complexity and export restrictions, were discussed. Some of the recommendations on privacy were;

Privacy of the air link should be maintained even during handover between service providers.

Air interface privacy is requires at all times to protect both the signalling and bearer channels.

The air interface privacy algorithm should be better than the IS-54 algorithm.

The encryption method should be capable of being upgraded.

The encryption method should maintain bit and frame count integrity.

A uniform method of synchronous voice and data privacy should be applied to all PCS systems, to ease export issues.

All Federal requirements for support of end-to-end encryption should be instituted in the first generation of PCS systems.

The PCS service provider should provide an indication to the PCS user when over-the-air privacy is not being provide.

All PCS systems should employ a method of disabling encryption, export issue.

7.Objective c: Interoperability

This objective was to establish the minimum interoperability requirements for inter-system PCS authentication and privacy. Interim standard IS-41 addresses intersystem hand-off and roaming for cellular systems. The work effort for this objective was to determine what analogous interoperability functions would be required to support PCS authentication and privacy schemes, and the potential network and operations impacts of these functions. Issues addressed included the impact of key exchange requirements, also;

Transfer and management of privacy and authentication information.

Global Service Mobility

Interoperability between public and private PCS services

Fraud management

Emergency services

Users Identity Modules/Terminal identity

8. Objective d: Operations Needs

This objective was to establish recommendations for privacy and authentication operations needs, including service activation, fraud detection and recovery, and law enforcement.

9. Summary:

PCS authentication and privacy considerations have been addressed; many decisions and recommendations have been reached. Some of the highlights of these decisions are;

a. A secret key authentication and privacy mechanism should be standardized for PCS applications in the near term.

b. A public key authentication and privacy mechanism should be standardized for PCS applications for use later in the PCS deployment cycle.

c. PCS key distribution mechanisms should be implemented with expectations of a minimum level of service activation training and experience.

d. The bearer channel privacy mechanism should be sufficiently robust to resist intrusive loss of privacy for a minimum acceptable time period. Further study is recommended on a comparable objective measure of privacy for PCS calls.

e. Authentication mechanisms must be air interface independent.

f. Access to emergency provider notification systems must be provided in a manner compatible with operational expectations of the emergency provider systems.

g. Interoperability of Public and Private PCS systems should allow handover of (approved) active calls.

h. Authentication of users should be by a User Identity Module (UIM) which is physically separable from a Wireless Access Terminal. The UIM should adopt an existing standard for personal identification devices. Users are required to authenticate themselves to the UIM by means of a PIN or equivalent.

Attachments:

1. List of Contributions and Reference Documents.

2. List of Attendees.

CONTRIBUTIONS AND REFERENCE DOCUMENTS LIST

Contributions

JEM/93-001
Title:Cryptographic or Privacy & Authentication Requirements for PCS
Author: Joe Wilkes, AT&T

JEM/93-002
Title: Users Perspective of PCS Security, User Services and Security Architecture
Source: Federal Wireless Users Forum: Contact: Leon Scaldeferri (NSA)

JEM/93-003
Title: Parameter Recommendations for PCS Real-time Encryption
Author: Dan Brown, Motorola

JEM/93-004
Title: Recommendation for Synchronous-Mode Encryption
Author: Dan Brown, Motorola

JEM/93-005
Title: A Method of Authentication & Key Agreement for PCS
Author: Dan Brown, Motorola

JEM/93-006
Title: Protocol for PCS Security-Related Wireless Access
Author: Dan Brown, Motorola

JEM/93-007
Title: Law Enforcement Requirements for the Surveillance of Electronic Communications
Source: Electronic Communications Services Providers Committee (ECSP), ATSI: Contact: Jeff Kushan; (Presented by Neil Knight, U S West Communications and David Worthley, FBI)

JEM/93-008
Title: Selected Responses to the Canadian Government Call for comments of Proposed Telecommunications Privacy Principles.
Source: Stentor Telecom Policy, Inc.; Contact: Claude Parent

JEM/93-009
Title: Statement of Policy on Privacy & Telecommunications
Source: State of New York Public Service Commission; Contact: Claude Parent

JEM/93-010
Title: Guidelines on Protection of Privacy & Transborder Flows of Personal Data
Source: OECD; Claude Parent

JEM/93-011
Title: Comparison of Authentication & Key Agreement Protocols for PCS
Author: Mike Beller, Bellcore

JEM/93-012
Title: Proposed Authentication & Key Agreement Protocol for PCS
Author: Mike Beller, Bellcore

JEM/93-013
Title: Comments on Threat Analysis & Smart Cards
Author: Phil Porter, Bellcore

JEM/93-014
Title: Handset Features Relating to Fraud Control & Privacy
Author: Robert S. Powers, MCI Telecommunications

JEM/93-015
Title: Subscriber Authentication & Voice Privacy, JEM Report 4-6 March 1991, Denver, CO
Source: JEM (TIA and ECSA)

JEM/93-016
Title: Proposed Draft Technical Report:
Privacy & Authentication Objectives for Wireless Access To Personal Communications

JEM/93-017
Title: Presentation: Task Group 8/1 Working Group Status Report, ITU, Oct. 1993; Security Principles for FPLMTS (FPLMTS.SCRT)
Source: ITU; Contact: Mark Hosford, ATT

JEM/93-018
Title: Presentation: Introduction to PCS
Author: Carl Bedingfield, BellSouth

JEM/93-019
Title: Presentation: PCS Authentication and Privacy: Brief Overview of History and Technology
Author: Dr. Richard Levine, Beta Scientific Laboratory

JEM/93-020
Title: Presentation: Privacy in Telecommunications - the Canadian Experience
Author: Claude Parent, Stentor Resource Centre

JEM/93-021
Title: Presentation: Government Escrow
Author(s): Cliff Brooks & McNulty, NSA

JEM/93-022
Title: Presentation: Authentication and Privacy Requirements
Author: Herb Calhoun, Motorola, FWRDC

JEM/93-023
Title: User Needs for Privacy & Authentication in 1800 MHz Personal Communications Services
Author: Telocator Technical & Engineering Committee

JEM/93-024
Title: TSB-51 (IS-41 Rev. C) TSB Published Authentication, Signaling, Message Encryption and Voice Privacy; PN 2254/November 1992.
Source: Mark Hosford, AT&T Communications

JEM/93-025
Presentation: Draft Recommendation - Security Principles for FPLMTS
Source: Mark Hosford, AT&T Communications

JEM/93-026
Presentation: GSM Security
Source: Charles Brookson, British Telecom

JEM/93-027
Presentation: A Current Perspective of Cellular Fraud
Source: Robert Jueneman, GTE Laboratories

JEM/93-028
Title: TIA P/N 3098, Annex A, Emergency Services Models (Balloted Version Nov. 1993)
Source: Mark Hosford, AT&T Communications

JEM/93-029
Title: Minimizing Unauthorized Penetrations of Personal Communications System Network Components
Source: Dick Brackney, National Communications System

JEM/93-030
Title: Viewgraphs from presentation on contributions 011 and 012
Source: Milt Anderson, Bellcore

JEM/93-031
Title: GSM Security Information (Supplement to contribution 026)
Source: Charles Brookson

Additional References

Draft ITU-T Recommendation F.115 "Operational and Service Provisions for FPLMTS", January, 1993.

ISO 7810:1985, "Identification cards - Physical characteristics"

ISO 7811-1:1985, "Identification cards - Recording technique - Part 1: Encoding"

ISO 7811-3: 1985, " Identification cards - Recording technique-Part 3: Location of encoded characters"

ISO 7816-1:1987, " Identification Cards - Integrated circuit(s) cards with contacts, Part1: Physical characteristics"

ISO 7816-2: 1988, "Identification cards - Contacts, Part 2: Dimensions and locations of the contacts"

ISO 7816-3: 1990, "Identification cards - Contacts, Part 3: Electronic signals and transmission protocols"

PT EN 726-3: "Terminal Equipment (TE); Requirements for IC Cards and terminals for telecommunications use Part 3: Application for independent card requirements"

PT EN 726-4: "Terminal Equipment (TE); Requirements for IC Cards and terminals for telecommunications use Part 4: Application independent card related terminal requirements"

ATTENDANCE

Milton M. Anderson	Bellcore
Carl Bedingfield	BellSouth Telecommunications
Marie-Clair Behar	EDS -Personal Communications Division
Mike Beller	Bellcore
Chris Bennett	c/o PCSI
Dick Blake	Siemens Stromberg-Carlson
Richard C. Brackney	National Communications System
Charles Brookson	British Telecom
Dan Brown	Motorola Inc.
William Burr	NIST
Herb Calhoun	Motorola
Lynn A. Carlson	GTE Mobilnet
Gilbert Chien	Ericsson Network System
Christopher Clanton	Motorola
Jeff Crollick	GTE Telecommunications Services
Brian Daly	AG Communication Systems
Walter Fairclough	Bell SYGMA
Michael Gundlach	Siemens OEV EA A32
Dr. A. Roger Hammons Jr.	Hughes Network Systems Inc.
William Heger	Siemens AG
Mark Hosford	AT&T
Eric Johnson	DOD/NSA
Clayton Joyce	Omnipoint
Robert Jueneman	GTE Laboratories
John Kimmins	BELLCORE
Neal J. King	ROLM, Siemens Company
Neil Knight	US West Communications
Mark Koro	Dept. of Defense-NSA
Frank LaPorta	AT&T Communications
Richard Levine	Beta Scientific La
Wayne McCoy	NIST
S. Brent Morris	N.S.A.
Doug O'Neil	BellSouth
Jim Papadopoulos	NYNEX
Claude Parent	Stentor Resource Centre Inc.
P. T. Porter	Bellcore
Robert S. Powers	MCI Telecommunications
Larry Puhl	Motorola
Christopher Redding	US Dept. of Commerce NTIA/ITS
Dr. Arthur Ross	Qualcomm Incorporated
Mary Ruhl	NIST
Ronald D. Ryan	Northern Telecom, Inc.
Leon S. Scaldeferri	National Security Agency R22
Amy Stephan	Telocator
William R. Tisdale	American Mobile Satellite Corp.
Els Van Herreweghen	IBM Research Zurich
Micheal Walker	Skynet
Michael Wiener	Northern Telecom
Mark Wells	Nokia Mobile Phones
Michelle Wignall	Dept. of Defense
Dr. Joseph Wilkes	AT&T Bell Laboratories
Paul K. Wilkinson	Audiovox Cellular Communications
Larry Wilson	US DOD
Desmond Wood	Northern Telecom
David Worthley	FBI