Individual Management of Personal Reachability in Mobile Communication

Martin Reichenbach[1], Herbert Damker[1], Hannes Federrath[2], Kai Rannenberg[1]
[1]University of Freiburg, Institute for Informatics and Society,
Department of Telematics, Friedrichstr. 50, D-79098 Freiburg, Germany
Phone: +49-761-203-4931, Fax: +49-761-203-4929
E-Mail: {marei, damker, kara}@iig.uni-freiburg.de
[2]Dresden University of Technology, Institute for Theoretical Informatics,
H.-Grundig-Str. 25, D-01062 Dresden, Germany
Phone: +49-351-463-8470, Fax: +49-351-463-8255
E-Mail: federrath@inf.tu-dresden.de

Abstract

This paper describes a concept for controlling personal reachability while maintaining a high degree of privacy and data protection. By easy negotiation of their communication requests users can reach others without disturbing the called partners and without compromising their own privacy.

Reachability management can strengthen the called subscriber's right to self-determined communication without violating the callers' interests in protecting their personal data.*

Keywords

Security and Protection; Communications Applications

---

* Parts of this work are funded by the Gottlieb Daimler and Karl Benz Foundation (Ladenburg, Germany) as part of its Kolleg "Security in Communication Technology".

Published in:
Louise Yngström, Jan Carlsen (ed.): **Information Security in Research and Business**; IFIP TC11 13th international conference on Information Security (SEC '97), 14 - 16 May 1997, Copenhagen, Denmark, ISBN 0 412 81780 2, p. 164 - 174, Chapman & Hall, London • Weinheim • New York • Tokyo • Melbourne • Madras, May 1997

1 PERSONAL REACHABILITY MANAGEMENT AND MULTILATERAL SECURITY

Current opportunities for mobile communication increase the technical reachability of users. This, of course, endangers their right to self-determined communication. Persons, who need to be available for professional reasons, are particularly affected. Their need of personal mobility and technical availability rises. Frequently they are without a secretary's support. Some people even have to fear annoying and harassing calls in their private life.

The increased technical availability necessitates a new class of services in order to facilitate the self-control of one's personal reachability – **personal reachability management** (cf. 1.1).

As the interests of different parties participating in communications differ, personal reachability management is a telecommunication-area example for multilateral security (cf. 1.2 and 1.3). It's prototype implementation is going to serve as the basis for a trial to demonstrate the concepts of multilateral security and to examine their relation to the users' needs (cf. 1.4).

1.1 What is "Personal Reachability Management"?

Subscribers are able to control their personal reachability through the technical support provided by their personal Reachability Management System.

During the signalling phase of a call the caller transmits information concerning the nature and content of his communication request (cf. 2.1). Before the subscriber being called – the "callee" – is personally contacted, this communication request is evaluated and negotiated by his Reachability Management System.

Subscribers are able to configure their reachability easily for different situations. The situations may arise from daily life or requirements of the work environment.
By supporting these new services personal reachability management offers a high degree of security and privacy to the users.

1.2 Multilateral Security, Data Economy and Careful Allocation

A lot of the early security approaches (e.g. [USA_DOD85]) are focused on the protection of system owners and operators only. Frequently the security of users and subscribers has been neglected. The term **multilateral security** [Ranne94] is therefore used here to describe an approach aiming at a balance between the different security requirements of different parties.

In particular, respecting the different security requirements of the parties involved implies renouncing the commonly used precondition, that the parties have to trust each other, and especially renouncing the precondition, that the subscribers have to place complete trust into the service providers. Consequently, each party must be viewed as a potential attacker on the other and the safeguards have to be designed accordingly.

The following list gives some examples of different security requirements of different parties:

- Subscribers deserve protection from others, especially network operators or service providers, monitoring their communication activities (confidentiality, especially unobservability and message content confidentiality).

- Providers deserve protection from fraud, e.g. through unpaid and unaccountable calls, for which no subscriber takes responsibility (accountability, especially non-repudiation).
- Network operators deserve protection from sabotage, endangering the use of their systems (integrity and availability).
- Subscribers deserve protection from harassing calls, for which no one takes responsibility (accountability, especially non-repudiation).

The best design strategy to fulfil the confidentiality requirements is the **avoidance of data**, e.g. in communication protocols. In this context, data that do not exist or are not transmitted, need no protection from unauthorized use. Since identification data, for instance, are frequently needed for accountability purposes, complete data avoidance is rarely possible. Nevertheless the strategy of **data economy** (i.e. to avoid data, wherever possible) is worthwhile, because it reduces the expenditure for data protection.

Another helpful design strategy in order to reduce the risk of misuse is the strategy of **careful allocation**. This means especially to give the storage and the processing of data into the control of those who require the confidentiality.

1.3 Reachability Management as an Example for Multilateral Security

Personal reachability management can be viewed as an example for multilateral security as well as for the design strategies of data economy and careful allocation.

The need for multilateral security comes from the different interests of callers and callees. Callees are interested in avoiding a possible disturbance, e.g. by getting more information on an arriving call before answering it. On the other side callers are frequently interested in protecting their anonymity and in keeping their communication request confidential.

The following examples illustrate these issues and show which facets of security could be important in different situations:

- In order to avoid disturbance a medical woman or nurse in a nocturnal stand-by service is not interested in every call which might arrive at night. She wants to be reachable for emergency calls and perhaps also for near relatives or friends, for whom she would get up even at night. Potentially she wants to defend herself from annoying calls. Accordingly, her Reachability Management System will request the identity or function information from the caller before ringing the bell (and disturbing her sleep). Protection from transmission errors and from callers, pretending to be someone else, requires the integrity of the call information and the accountability of the call.
- The staff of a welfare centre as well as mobile social workers may use a Reachability Management System to ease their work during rush periods. The clients of welfare centres which handle socially taboo topics like AIDS, alcoholism, venereal disease or indebtedness generally want to stay anonymous. Often this anonymity is a prerequisite for an open and really helpful consultation. The client must therefore be able to contact the welfare centre anonymously. It must be guaranteed that, in fact, no identity information is transmitted. If the consultation can take place anonymously, but not free of charge, it must be possible to call under a pseudonym.

Providing a satisfying degree of both confidentiality and accountability of callers is not a simple task. Current caller identification mechanisms allow either, that callees protect them-

selves by forcing the callers to show their identity (to give some accountability to a call), or they allow, that callers stay anonymous (thus protecting their confidentiality).

Some systems allow calling users a per-call choice whether to show their identification or not, but even then the called users have no instrument to differentiate calls, before they are disturbed. Their only way to get some information about an incoming call is to look for the caller identification. This way the callers are forced to show this identification and lose their anonymity, even when other means would be more appropriate (cf. 2.1).

Personal Reachability Management is a more flexible approach allowing the caller and the callee to exchange only the information, that is really needed. This economical use of data enables the transmission of less personal data, which deserves to be protected.

The data arising in the context of personal reachability management are extremely sensitive: some of them describe callers' and callees' current situations, some (e.g. the programmed reaction to incoming communication requests) contain information on personal attitudes towards other people. Information like this may even be protected by the privacy regulations of some states. It must be allocated carefully and has to be protected from all potential communication partners as well as from third parties, such as service providers. The personal reachability data and programmes should therefore be located at a place, where those users, whose data are processed, can control them (cf. 2.2).

While the personal Reachability Management System can be seen as a prime example for the implementation of multilateral security both in a telecommunication terminal and on the application level, complementary work is needed on network and network infrastructure levels. Examples of techniques aimed at multilateral security on those levels can be found in [Chaum85, KFJP96, MS95, Pfitz93, PW87 and PPW91].

1.4 Demonstrating and Examining Multilateral Security

The personal reachability management prototype is currently being developed in the (virtual college) project "Security in Communications", mainly sponsored by the independent Gottlieb Daimler and Karl Benz Foundation, Ladenburg, Germany.

On one hand this prototype serves as an example demonstrator for the implementation of multilateral security in communication technology. On the other hand it will be examined in laboratory experiments and in trials. These trials are based on the simulation study method [KS95] and on cases occurring in the daily work of actors in the public health service, e.g. mobile nursing.

The trials will examine the subscribers' requirements for security and trustworthiness in the context of using telecommunication devices and networks. The prototype therefore has to contain additional security mechanisms (authentication, trusted services, user-to-user-encryption) or to provide at least a demonstration of their operation.

2 DESIGN OF THE REACHABILITY MANAGEMENT SYSTEM

According to the strategies aiming at multilateral security the main design aspects of the Reachability Management System are the communication context and the representation of urgency (cf. 2.1) as well as the secure data processing and storage (cf. 2.2). To ease the demon-

stration of multilateral security, a special effort has been placed into the usability and the user interface of the prototype (cf. 2.3).

2.1 The Communication Context and the Representation of Urgency

This chapter describes the central idea enabling multilateral security in a call situation - the careful modelling of the **communication context**. The communication context illustrates a communication request (respectively a proposal) or a currently existing communication between two (or more) partners. The communication context is transmitted as a whole or in parts during the signalling phase and is the object of the arrangement between the reachability managers involved.

The connection with the called subscriber will only be established if the negotiated communication context has fulfilled certain conditions. If not, the reachability manager is capable of offering a variety of reactions, for example storing a message, or diverting a call to another person.

A communication context contains information about:

- how the communication partners are acquainted with each other (anonymous, by a pseudonym, with their real identity);
- the intention of the communication request;
- the urgency of the communication request;
- the manner of communication (the kind of service involved);
- the existing security requirements;
- the mechanisms used to ensure the actual communication.

Of particular significance is the way the urgency of a communication request is represented. Consistent with the interpersonal negotiation of reachability, a technical system should provide a multitude of options. The subscribers to the Reachability Management System can provide details about the subjective urgency or a reference.

Possible options are:

- The **assertion of urgency**: The caller indicates a certain degree of urgency while he is trying to get hold of someone. This assessment may be very subjective.
- The **specification of a function**: The caller can give details about the reason for his call, about his position, or even his qualification. He may, for instance, call as a member of a particular project or company. This specification may be digitally certified.
- The **specification of a subject**: This specification may only be evaluated by the reachability manager when a prearranged list of possible topics exists.
- The **provision of a reference**: The caller mentions the recommendation of a third person. This might be accomplished by means of a certificate issued by this third person. If the called subscriber knows the third person, he may use this recommendation as a criterion for evaluating the communication request.
- The **presentation of a voucher**: The voucher differs from the reference in that it has been issued by the called subscriber himself. It may increase the chance of a return call.

- **Offering a surety**: In order to emphasize the seriousness of his communication request and his statement of urgency, the caller may remit to the called subscriber a (possibly negotiated) amount as a surety. If the called subscriber does not agree with the caller's evaluation of the urgency of his call, he has the potential to withhold this amount or remit it to a public welfare institution, or a similar organisation.

In the personal configuration of his Reachability Management System the subscriber determines the different kinds of reactions to incoming calls (respectively communication requests). He defines, which information the Reachability Management System will request from the caller in order to evaluate the communication request. A likely example will be that the called subscriber's Reachability Management System requests the identification or a surety from an unidentified caller.

2.2 Secure Data Processing and Storage

The configuration of the Reachability Management System demands a high degree of confidence. The user entrusts very sensitive personal data to a technical system, e.g. the information when he can be reached and which persons he wants to communicate with.

This requires:

- Processing and storage in a trustworthy and personal environment: Because the data should also be protected against third parties, such as service providers and network operators, the Reachability Management System can't be implemented as a purely network service (cf. 1.3).
- Protection against malicious investigation: The process of negotiation between the reachability managers should be arranged such that even repeated requests reveal no information about the personal configuration of any subscriber's reachability. It should be possible to discover attempts to gain such information.
- Protection from unintentional revelation of personal information or financial values such as sureties: This requirement should particularly be considered while designing the user interface of the Reachability Management System.
- The user's ability to audit the system: At all times the user should be able to control, change or delete all the information stored in his Reachability Management System. In particular, there should no data be stored in the Reachability Management System which would allow third parties to reconstruct the subscriber's communication behaviour if the reachability manager is lost.

It is essential to secure the communication and negotiation between two Reachability Management Systems according to the objectives of multilateral security. The confidentiality of transferred data can be guaranteed by point-to-point-encryption. Anonymity and unobservability may only be achieved by an appropriate underlying network infrastructure (cf. 1.3 and [KFJP96, Pfitz93]). In order to support these tasks, the Reachability Management System fulfils security functions, like managing information regarding the subscriber's location in a mobile communication network [Hetsc93, MS95].

Reachability managers have to function correctly even in the case of abuse or attack: The integrity and, if necessary, the accountability of the data transferred with a communication request have to be guaranteed. In order to fulfil these requirements the user has to supply evi-

dence of the authenticity of his identity information by delivering a digital signature or a certificate.

To a certain extent the topic is related to access control systems (controlling the access to a called person's private sphere) and to value transfer systems. A value transfer system passes on values like “Reachability Rights”, e.g. references and vouchers in a secure way. In order to confirm the declaration of urgency by means of a surety the transfer of a value is also needed.

2.3 Usability and the User Interface

Reachability management constitutes an extension to the service offered by a normal telephone. Some additional effort is required in usage, because the user has to assign additional specifications about the urgency of his call (over and above the information regarding which communication partner he wants to get hold of).

Standardized call templates reduce this effort by delivering default values, e.g. “normal” urgency, or the delivery of a small surety. As the Reachability Management System gives the opportunity to access a subscriber directory the effort may be reduced even more.

Furthermore, each subscriber is reachable under exactly one address, no matter where or in which situation he is.

The task of the user interface is to support the user while formulating his communication requests, presenting the actual communication context and configuring his reachability. It should also be possible to change the user's status.

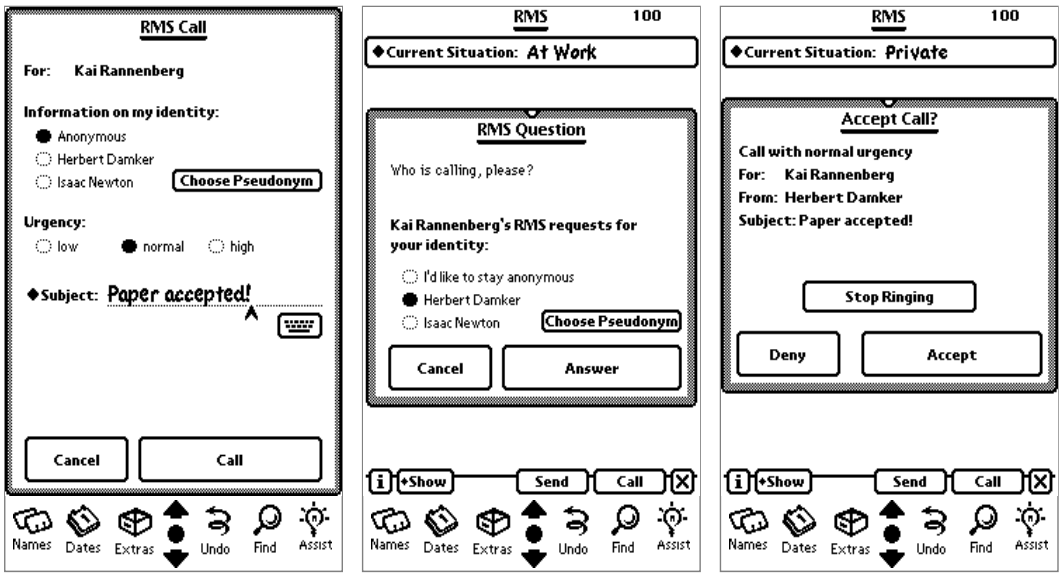

Figure 1 Reachability Management Dialogues on the Newton MessagePad™

Figure 1 shows three of these dialogues on the Newton MessagePad™(formulating a communication request, a question from the called subscriber’s Reachability Management System and the display of an incoming call).

3 TECHNICAL IMPLEMENTATION OF THE REACHABILITY MANAGEMENT SYSTEM

3.1 Hardware Architecture

The implementation of the Reachability Management System involves two components.

The “personal communication assistant” serves as a trustworthy personal environment. While building communication requests it supports the caller by delivering a subscriber directory. On the other side it signals incoming calls and messages to the called subscriber. The sensitive reachability information is stored in this component.

The mobile part of the reachability manager is complemented by a “stationary subscriber station”. This component is localized, for example, at the subscriber's home or office, accepting all the communication requests for the user and, should the occasion arise, forwarding them to the user's personal communication assistant. The stationary subscriber station performs additional functions of the Reachability Management System, which can't (yet) be implemented by a mobile device, for example, the recording of speech messages.

Within the scope of this project the personal communication assistant will be based on a Newton Message Pad™ with demonstrator functionality.

The stationary subscriber station is being implemented on a Personal Computer, connected to the fixed network via ISDN (Integrated Services Digital Network). The communication between the personal communication assistant and the stationary subscriber station takes place over the cellular mobile communication network GSM (Global System for Mobile communication).

3.2 Functional architecture

Figure 2 shows the functional structure of the Reachability Management System (both personal communication assistant and stationary subscriber station). The Reachability Management System consists of three functional units: the user interface, the core machine and the communication services.

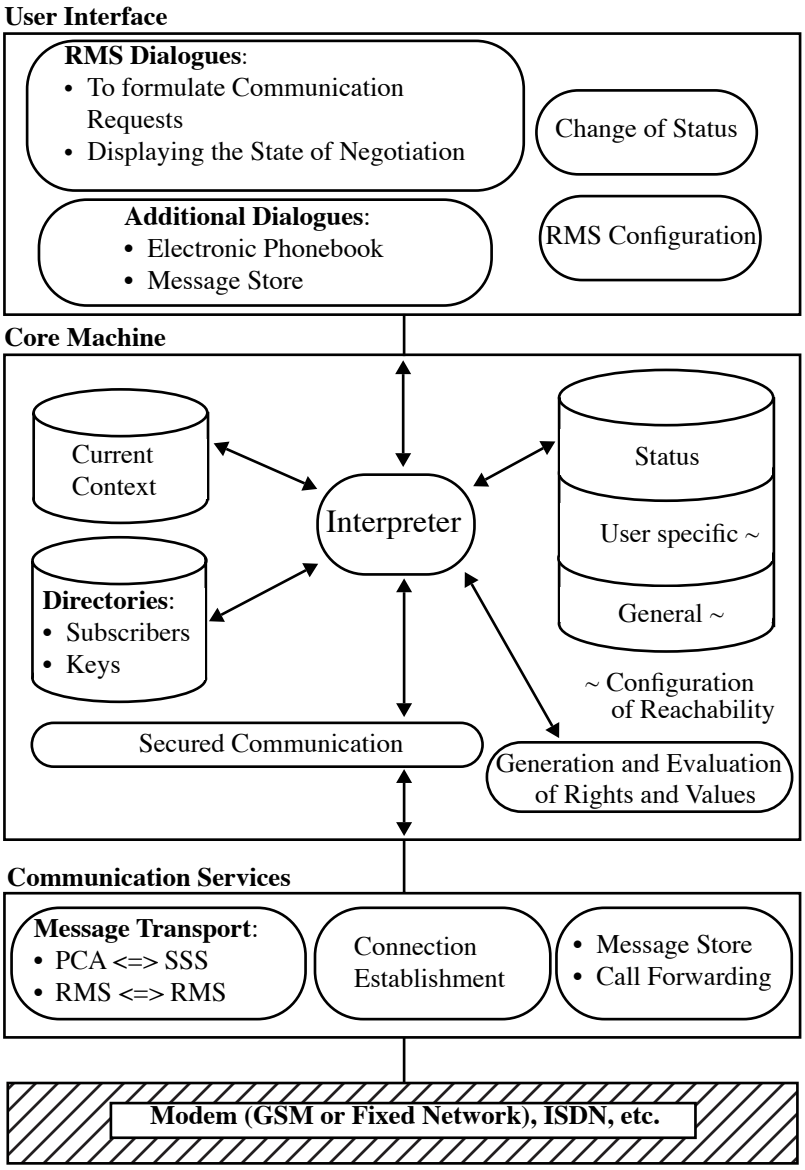

Figure 2 Functional Architecture of the Reachability Management System (RMS - Reachability Management System, PCA - Personal Communication Assistant, SSS - Stationary Subscriber Station).

4 THE CORE MACHINE

The core machine is the central technical part of the Reachability Management System. It evaluates the current communication context. This context is set up using the subscriber's specifications, as well as the data transmitted from the communication partner. The rules of evaluation come from three different areas:

- The status describes the user's current situation (e.g. “private”, “at work”, “meeting”). This information changes frequently and determines which part of the rules will be applied.
- The user specific configuration is defined in the Reachability Management System’s configuration dialogue. In this dialogue the subscriber uses individual evaluation rules to define how the reachability manager should react to incoming communication requests.
- The evaluation rules are complemented by common reachability rules which can't be changed by the subscribers (for example the definition that emergency calls should always be put through).

As a result of the evaluation, the interpreter updates the communication context and decides whether the communication request will be accepted or denied. The interpreter may also require further information (from the user or from the caller) to make the final decision. Subsequently, appropriate messages will be sent to the user of the reachability manager (or rather to the user interface) resp. to other components of the user's or the caller's reachability manager.

5 REACHABILITY MANAGEMENT IN FUTURE NETWORK INFRASTRUCTURES

To receive the full benefit from multilateral secure reachability managers in future network infrastructures, the networks have to support the concept of multilateral security.

The network's support is necessary for anonymous and pseudonymous, or even better, unobservable communication. Broadcast signalling and implicit addressing [KFJP96, Pfitz93, PW87, PPW91] is a part of this. Even if many of these features might seem to be unrealistic today because of the networks narrow bandwidth, they should be easier to implement with the help of future broadband networks. Then the reachability manager could be addressed via temporarily valid implicit addresses, which the subscriber hands out to a circle of well chosen persons.

The limited possibilities of the today's signalling channels indicate an additional problem. They only allow the transmission of absolutely necessary signalling information. In future it will possibly be better to deviate from the strict separation of (free of charge) signalling and (subject to charges) data communication. If universally available services like “Universal Personal Communication” (UPT) are to be established it will be obligatory to extend the signalling networks.

Features like “offering a surety” inevitably call for the integration of systems for electronic payments or the transfer of values. However, in these systems the subscriber's anonymity and unobservability have to be guaranteed.

6 REFERENCES

[Chaum85] Chaum, D. (1985) Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985), 1030-1044.

[Hetsc93] Hetschold, T. (1993) Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes. GMD-Studien Nr. 222, Oktober 1993.

[KFJP96] Kesdogan, D.; Federrath, H.; Jerichow, A. and Pfitzmann, A. (1996) Location Management Strategies increasing Privacy in Mobile Communication Systems; in Information Systems Security. Facing the information society of the 21st century. Proc. IFIP/SEC '96 - 12th International Information Security Conference 21-24 May 1996, Island of Samos, Greece, Chapman & Hall, 1996.

[KS95] Kumbruck, C. and Schneider, M.J. (1995) Simulation Studies, a new method of prospective Technology Assessment and Design; Working Paper, No. 190, provet, Darmstadt, September 1995.

[MS95] Müller, G. and Stoll, F. (1995) The Freiburg Communications Assistant Enabling Decentralization and Privacy in Mobile Communications Systems. Speaker's Papers, 7th World Telecommunication Forum, Technology Summit "Convergence of technologies, services and applications" Vol. 1, ITU Telecom 95 Technical Forum, Geneva, 3-11 October 1995, International Telecommunication Union, October 1995, 245-249.

[Pfitz93] Pfitzmann, A. (1993) Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

[PW87] Pfitzmann, A. and Waidner, M. (1987) Networks without user observability; Computers & Security 6/2 (1987), 158-166.

[PPW91] Pfitzmann, A.; Pfitzmann, B. and Waidner, M. (1991) ISDN-MIXes - Untraceable Communication with very small Bandwidth Overhead; Proc. IFIP/SEC '91 - 7th International Information Security Conference Brighton, UK, May 1991; North-Holland; 1991; 245-258.

[Ranne94] Rannenberg, K. (1994) Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security; in Richard Sizer, Louise Yngström, Henrik Kaspersen and Simone Fischer-Hübner: Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference August 12-17, 1993, onboard M/S Ilich and ashore at St. Petersburg, Russia; North-Holland; 1994, 113-128.

[USA_DOD85] DoD Standard (1985) Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711.