Daidalos Security Framework for Mobile Services

William FITZGERALD[1], Kevin DOOLIN[1], Fiona MAHON[1], Christian HAUSER[2],Antonio F. GOMEZ-SKARMETA[3] , Stephen BUTLER[4], Peter SCHLOSSER[5], Benjamin WEYL[6]

[1]*Waterford Institute of Technology, TSSG, Cork Road, Waterford, Ireland*
Tel:+353 51 302901, Fax:+353 51 302902, Email:{wfitzgerald,kdoolin,fmahon}@tssg.org
[2]*Universität Stuttgart, Pfaffenwaldring 47, 70174, Stuttgart, Germany*
Tel: +49 711 6857990, Fax:+49 711 685 7983, Email: hauser@ikr.uni-stuttgart.de
[3]*Universidad de Murcia, Apartado 4021, 30001 Murcia, Spain*
Tel: +34 968364607, Fax:+34 968364151, Email:skarmeta@dif.um.es
[4]*Lake Communications, Business Innovation Centre, IT Sligo, Ballinode, Sligo, Ireland*
Tel:+353 51 9156832, Fax:+353 71 9155069, Email: Stephen.butler@lakecommunications.com
[5]*BMW Softlab GmbH, Bollinhenstrasse 54, 3006 Bern, Germany*
Tel:+41 31 330 14 78, Email: peter.schlosser@softlab.ch
[6]*BMW Group Research and Technology, Hanauer Str. 46, 80992 München, Germany*
Tel:+49 89 382 48951, Fax: +49 89 382 41136, Email: Benjamin.Weyl@bmw.de

Abstract: Mobility is now the central focus of the lives of European citizens in business, education, and leisure. This will be enriched by pervasiveness in the future. The Daidalos vision is to seamlessly integrate heterogeneous network technologies that allow network operators and service providers to offer new and profitable services, giving users access to a wide range of pervasive, personalised voice, data, and multimedia services. This paper discusses the security issues that need to be addressed to make Daidalos a real viable solution for future pervasive mobility. Issues include among others privacy & identity management, secure protocols, distributed key management, security in ad hoc networks.

1. Introduction

The growth in the capabilities of telecommunication networks has spurned the development of new paradigms that are made possible by these new capabilities - one of which is pervasive networks. Pervasive networks allow technology to weave seamlessly into everyday life, continuously monitoring users and their usage patterns, learning and pre-empting requirements. In this environment the trend is towards a more open market, increasing the potential for more services and unlocking users from the single provider scenario.

Continuous "surveillance" of users in such a network, where there are many potential services using this detailed information, means security and privacy becomes a cornerstone issue. Technical support for security and privacy protection must be greatly improved as compared to today's systems in which a large portion of an operators security framework consists of organisational policies and contracts.

Daidalos [1] is a European research project comprising major European operators designing such a future telecommunication system. Using two key scenarios (1) University Scenario and (2) the Automotive Mobility Scenario, it has a user centric approach to design. Such an approach avoids a technology driven system and keeps focus on user and market requirements at all times and at all levels of development.

In the next section a high level description of the Daidalos model and the security issues that lie within it are introduced. The paper continues in section 2.2.1 by describing Daidalos' underlying approach to achieving privacy protection. Section 2.2.2 defines the security and privacy support of the Pervasive Service Platform (PSP). The paper continues to describe in section 2.2.3 protection provided by the Service Provisioning Platform (SPP). The paper finishes with a presentation of the security and privacy mechanisms of the access networks including sensor networks.

2. Daidalos Security Infrastructure

To understand the security solutions presented in this paper, it is necessary to know the underlying architecture. Therefore, a short overview on the architecture is given in section 2.1.

2.1 – Underlying Architecture

The Daidalos infrastructure revolves essentially around a 3-tier system (Figure 1 depicts this architecture with its security features):

1. Top Tier: Pervasive Service Platform (PSP)
2. Middle Tier: Service Provisioning Platform (SPP)
3. Bottom Tier: Access Networks (AN).

At the top of the 3-tier architectural model, Daidalos provides a platform (PSP) for the deployment and provision of pervasive services by providing enabling services neatly integrated with the traditional service-provisioning platform. These enabling services comprise, e.g., a pervasive service management allowing for composition of basic services to more sophisticated ones, a context management and a personalization subsystem for tailoring the services for each user's needs.

For the support of traditional services and the PSP, Daidalos integrates the core network in terms of control & data planes and integrates these with the basic enabling services necessary for the operation of a carrier-grade network, a third party network and application services.

For accessing the core infrastructure Daidalos integrates many types of access networks ranging from ad-hoc networks over Ethernet, WLAN, GPRS/UMTS, to broadcast networks like DVB-H by the coherent IP solution. A special kind of access networks are sensor networks. Sensors are important sources of context information necessary for providing context-aware services. Daidalos not only provides the infrastructure for traditional sensors like active badges, but also for wireless sensor networks consisting of small sensors with limited technical capabilities like computation, communication or battery power.

2.2 Daidalos Security Infrastructure

Maintaining a homogeneous level of security and guaranteeing a high level of seamless access to services in next generation network environments is complex and challenging. These issues include [2]: multiple authentication mechanisms, Single-Sign-On (SSO) for multiple services and administrative domains which will be needed, distributed authorisation mechanisms, multiple identities across different providers, multiple sessions of multiple users using multiple devices, contracts and so forth.

The Daidalos Security Infrastructure provides a flexible security solution with components and mechanisms covering these issues. The rest of the paper discusses in detail how this solution is achieved.

2.2.1 Identity and Privacy Model

Identity management is important to maintain sensitive data and confidential relationships with service providers and so forth. In distributed networks users may have multiple contracts with different providers, using various digital identities. The identity management and privacy framework must be able to facilitate private information to be flexible, providing different levels of security and privacy, allowing users to trade privacy against convenience when necessary [3].

In the Daidalos identity model a user can choose the identity he/she wants to use to authenticate and register for services. When the user first signs a contract with a Daidalos operator, an identity under which the contract and the respective profiles and rights are defined is issued. This identity, called Registration Identity (RegID), holds the information necessary for charging its owner, and can be seen as the system representation of the signer of the contract. For the purpose of having different levels of privacy, Virtual Identities (VIDs) are defined on-the-fly. By using different VID's, the user can reveal different personal information in the context of each VID. These identities are always related to a RegID and can share all or none of the RegID's attributes. As such, they are privacy-enabled and possibly anonymous representations of the RegID.

This yields a concept that small amounts of personal information are much less sensitive than a huge aggregation of personal information. So, it is possible to split the trace of personal information left by the user in the system. Although, the user can use different VID's towards foreign (service and network) providers, a means must be provided by which all actions of a user's VID's can be accounted to a real person for monetary as well as for legal accountability. The home operator is assumed to be trusted to know the link of all VID's to the RegID. Daidalos has taken a hybrid approach to allow user anonymity via pseudonyms and the utilisation of single sign-on processes (E.g.: Liberty Alliance [4]) to manipulate or tie those pseudonyms to a RegID [2].

The SPP can utilise the PSP VID's to provide a means for the operator to cope with this multiplication of user contexts. By this, a user can use different VID's towards different services or service providers and foreign network providers, but all actions can be accounted to his contract by the home provider.

While this approach is a huge step forward in privacy protection, it introduces some configuration burden on the user. First of all, the different VID's must be configured, i.e., it must be specified which information may be revealed in its context – including, e.g., setting the access rights for accessing context information about the user. Second, it must be decided when the aggregated revealed information is too privacy sensitive and the VID must not be used any longer. Third, the user must decide for each service to use, which VID to take. As this is acceptable in a traditional world of rarely changing services it needs extensions in a pervasive world in which a user is experiencing frequently changing services without even noticing it. This is where the security and privacy subsystem of the PSP acts and complements the respective functions of the service provisioning platform.

2.2.2 Pervasive Service Platform Security

The PSP is fundamentally based on information about the user's current situation, habits and so forth derived from context sensitive information. Thus, it is critical that a user's private information remains confidential and maintains constant integrity. The PSP layer provides an Identity & Privacy Management module to provide a secure service to manage a user's context sensitive information. The identity & privacy management provided by the PSP layer is funnelled down through the underlying layers to provide global system privacy.

The security and privacy subsystem provides an enabling service of the pervasive service platform that allows users to automate the above-mentioned VID related actions. Moreover, it comprises the respective counterparts being used by third party services. The overall functionality consists of three parts: (1) Privacy Policy Negotiation, (2) Identity Management and (3) Credential Management and Access Control

If a new service is discovered and to be used, the Privacy Policy Negotiation module is invoked, which negotiates anonymously with the respective Privacy Policy Negotiation counterpart at the service. The result of this policy is not only a statement about what the service guarantees to do with the personal information being revealed during the service use

(similar to what the Platform for Privacy Preferences (P3P) [5] does) but also a list of personal context information the service needs for the requested service provision, e.g., the user's location.

Based on this negotiation result, the Identity Management module selects or creates a VID in which context this information may be revealed. For this, it estimates the level of privacy invasiveness of all data being revealed in the context of the respective VID, so far. Finally, the Credential Management interfaces to the A4C subsystem of the service provisioning platform in order to create the respective authorizations for the service to access the negotiated context information according to the chosen VID. This module is complemented by the Access Control of the context management which checks the authorization in case of a context request again by interfacing with the A4C (Authentication, Authorization, Accounting, Auditing & Charging) subsystem of the service provisioning platform. Note, that there are also other entities in the Pervasive Service Platform implementation such as access control. Their description is omitted due to clarity reasons. A more detailed description of these modules, their inter-working and functionality can be found in [6].

2.2.3 Service Provisioning Platform Security

From Figure 1, one can see that the different components in the general architecture are: Pervasive Service Platforms, Service Provisioning Platforms (SPP), Access Networks (AN), Mobile Terminals (MTs), (Third Party) Service Providers and a Key Interconnection. The circles within Figure 1 indicate where the main entities that will support the security architecture in the SPP, are placed.

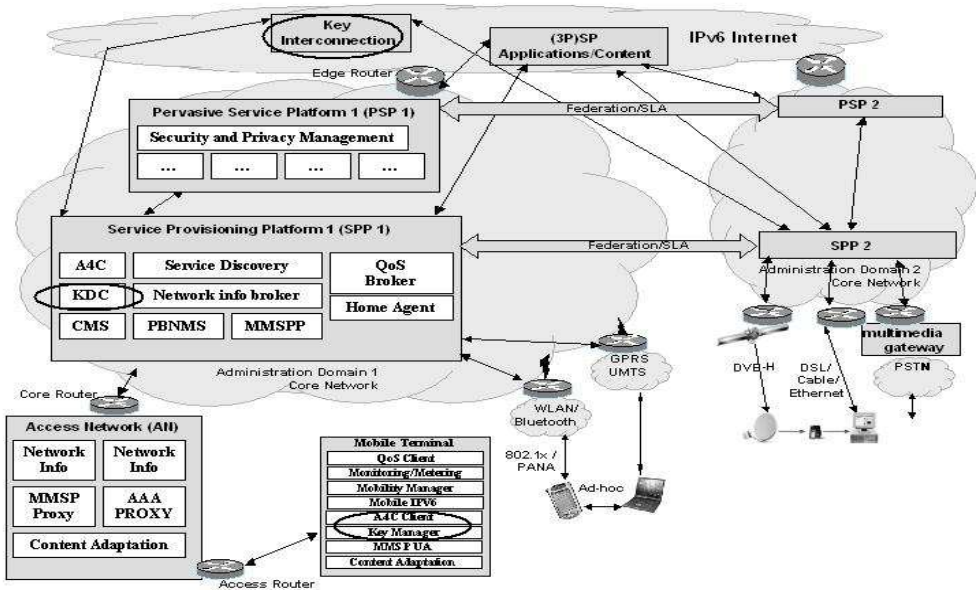

Figure 1: Security Components in Daidalos Architecture

As can be seen, in order to provide security both inter-domain and intra-domain key management is provided, fully integrated with the access control of mobile terminals (MT) in the AN, and with support for the security of the operator and service provider infrastructures.

2.2.3.1 Intra- and Inter-domain Key Management:

The 'Key Interconnection' is needed for enabling communication between various 'Key Management' systems within different administrative domains; that is, establishing a secure

context between an entity belonging to one domain and an entity belonging to another. For that purpose, the Key Interconnection entity provides secure inter-domain key transport.

The 'Key Distribution Center' (KDC), is the component in charge of managing credentials, certificates and, in general, digital identities. It provides support for the lifecycle of identities and keys within different scenarios and for various entities requesting them. Additionally, it is in charge of retrieving authorization assertions from the Authorization Authority (AA) and storing the received material into the appropriate repository.

The Key Manager will store/recover, and in general manage, the available authentication/authorization material in the key-store/authorization-repository. It will also sign/verify supplied material. These actions will be performed upon request of the A4C client or PSP components (e.g., A4C client may ask the key manager to sign a charging guarantee to protect against repudiation).

2.2.3.2 Security Related Protocols and Requirements:

The Mobile Terminal (MT) is responsible for acquiring network access, where the terminal and/or the user are authenticated and authorized. The A4C client is the component that performs these functions, using the Protocol for carrying Authentication for Network Access (PANA) [7] and 802.1x [8]. Figure 2 illustrates the authentication related components of the architecture, and shows communication patterns between them. The design provides not only authentication but also authorization support by means of (1) using EAP (Extensible Authentication Protocol) [9] as the basic transport protocol for credential management over PANA; and (2) integrating with SAML [2][3][10][11] for authorization. This requirement comes from the A4C infrastructure, where the AA will be part of the general Authentication, Authorization and Accounting (AAA) architecture. Authorization messages are transported by the same protocol and follow a similar path, as authentication messages. As illustrated in Figure 2, in order to support communication integrity and/or confidentiality between network elements like routers, servers, etc., IPsec [12] will be deployed as the basic security protocol; hence, a means to distribute and manage cryptographic material not only within a single domain but also across domains is required. If additionally the need to provide credentials and digital identities to MTs, users, providers and services, is identified then the conclusion is that the KDC system will be mainly based in a Public Key Infrastructure (PKI) [13] and its associated protocols.

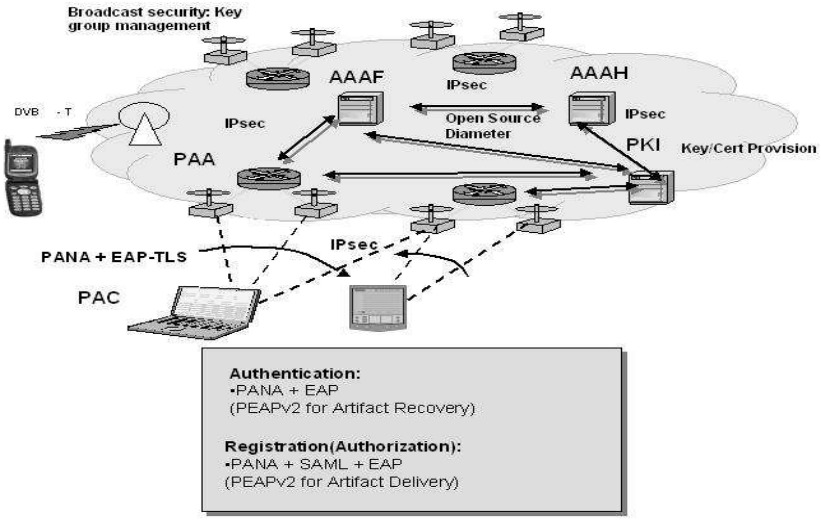

Figure 2: Protocols and Services for Security

The A4C and PKI models are only part of the framework for authorization. There is a special need for a flexible yet unambiguous means of communicating authorization information between the key elements of the system users, services, and the network. Due to the flexibility of the approach required in order to support attribute certificates, and credentials in general, the option of SAML has been considered and analysed extensively in order to provide the AA support for Daidalos.

2.2.3.3 Federated and Privacy-enabled Access Control:

Within DAIDALOS the Security Assertion Markup Language (SAML) has been chosen for integrating distributed authentication, authorization and SSO into federated, Beyond-3G operator concepts. SAML standardizes the exchange of information about a user's authentication status, authorization decisions and attributes. By applying SAML, the authentication infrastructure can be made independent of the specific mechanism used for the authentication of users. In addition, SAML supports SSO across administrative domains.

These advantages result in a decoupling of value-added service provider's infrastructure from access network infrastructure on one hand (distributing services independently from specific access technologies), and on the other hand enabling the usage of the same security functionalities for network security and building secure federations among all participating entities. The SAML Authority in conjunction with the Identity Manager, plays an important role in concealing identities and protecting users' privacy [2]. The RegID is never revealed and is concealed by using VID's, provided by the PSP identity management module.

The Asserting Authority has the following main functionalities for concealing the RegID:

- Asserting and providing information on a user's successful authentication via an authentication assertion. Authentication takes place based on a user's VID. The VID is mapped to the respective RegID (by accessing the Identity Manager) and an authentication assertion is generated and stored. Thus, the Asserting Authority can prove one's authentication to another entity within the federation.
- Issuing authorization decisions: For authorizing a specific user to a requested value-added service, the Policy Enforcement Point of the service can request authorization decisions from the Authority. The Asserting Authority issues the authorization decision based on the policies and profiles it holds connected to the binding of the VID and the Service Identifier.
- Collecting and issuing users' attributes and profiles: If a service has to be personalized for the user, it may require some attributes and profiles. The authority can collect the required attributes from the profile associated to the VID and issue them via an attribute assertion.

Every request for service authorization, broadcast services or individual services, uses a so-called Identity Token, being an enhanced SAML artifact, issued during the primal authentication process.

Authentication and authorization for broadcast services have to be seamlessly integrated into future security architecture. The basic idea of the SAML-based approach is that a user authenticates and receives authorizations for broadcast services as he does for all network services [11][14]. Prior to requesting broadcast services, a user is identified by "standard" network authentication mechanisms. After establishing the user's identity, authorization decisions for broadcast service access can be taken and granted. Key material allowing the access to subscribed broadcast services is distributed as an integral part of the standard network authentication within SAML assertions and allows access to broadcasted content on the user's mobile terminal.

2.2.4 Access Networks Security

Daidalos is implementing cryptographically generated addresses (CGA) and secure neighbour discovery within the IPv6 access network. This provides considerable protection against many of the routing attacks possible in an open access network. The Daidalos project has concentrated on how SEND [15] and CGA may be integrated into ad hoc networks and deliver fast hand over processes. Trust is bootstrapped from a low initial level by incrementally generating a candidate CGA, assuring this CGA is unique, establishing the certificate trust anchors necessary for SEND and finally once the PANA network authentication process has succeeded, a check can be made for certificate revocation. In the case of an ad hoc network Daidalos has evolved this process to provide a tunnel between a mobile terminal on the edge of the ad hoc cloud and its access router.

Ad hoc On Demand Distance Vector (AODV) routing was chosen in Daidalos as the most suitable candidate for a routing protocol in the ad hoc access networks. The protocol allows the mobile nodes to update and obtain routes quickly, as well as to destroy outdated routes. AODV deploys UDP messages and, since it is close to existing Internet routing protocols, it allows possible integration with the fixed network.

Secure Ad hoc On Demand Distance Vector (SAODV) [16] is an extension to the above-mentioned protocol that can be used to protect the route discovery process providing features such as Integrity, Authentication and Non-repudiation. The main goal is to prevent a malicious node forging AODV packets, listening to the others and replay attacks. SAODV does not describe which key management scheme should be used and, besides, it does not exclude the possibility to deploy a certification authority. This solution allows all the nodes joining the ad hoc network to download public keys plus the public key of the certification authority. If no certificates are used, it is assumed that SHA is the hash algorithm and RSA the encryption method.

As with any ad hoc network, there is a need to protect traffic between the Mobile Terminal (MT) and the router. This can be accomplished by creating an IPsec tunnel between the two elements. This both ensured that the MT was one virtual hop away from it's access router (a requirement for PANA [7]) and that data was protected from intermediate and rogue node interception and manipulation. However this did lead to problems in QoS routing decisions based on encapsulated QoS header fields. To overcome this problem Daidalos has ensured that these header fields were copied into the outer header of tunnelled packets.

The development of the solutions for secure charging of network traffic was another goal for Daidalos, particularly in ad hoc edge networks. To this end Daidalos implemented Secure Charging Protocol (SCP) [17]. This gave us non-refutable proofs of network usage that could be used in a later charging scheme. The proofs inserted in the packets use mechanisms considered to be secure like MD5 hashing. The control messages use Elliptic Curve Cryptography to minimise computational overhead. These routines are provided by a Common Cryptographic Library in Daidalos. The project also looked at the interoperation of SCP with core network A4C.

2.2.8 Sensor Network

The goal at this level is to aggregate data and deliver this as a data stream service into other services in a confidential and secure manner. The traditional way of doing this is by encrypting on a hop-by-hop basis within the sensor network. Encrypting data on a hop-by-hop methodology is too computationally intensive for the sensors used in Daidalos. Thus Daidalos is testing unique concealed data aggregation cryptographic techniques and privacy homomorphic algorithms, which allow us to aggregate encrypted data at certain points in the sensor network without decrypting this data. This means there is reasonably strong end-

to-end confidentiality that can be used in ad hoc networks of low-power, low cost sensor units.

3. Conclusions

Daidalos provides an important security and privacy infrastructure to allow operators to securely provide their communication infrastructures, to allow third party providers to securely provide their services as well as to allow users to use the system with preservation of their privacy. Due to the rapid prototyping approach followed in Daidalos, the security and privacy framework described in the paper is already integrated in many parts of the core system and will conquer the other parts in the future to deliver a fully integrated secure mobility system for operators, service providers and end-users.

4. Acknowledgements/Disclaimer

The societal research contributions described in this paper is based on results of IST FP6 Integrated Project Daidalos, funded under the European Community's Sixth Framework Programme, whose support is gratefully acknowledged. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. IST Daidalos Research: www.ist-daidalos.org.
2. B. Weyl, P. Brandão, A. F. Gómez Skarmeta, R. Marin Lopez, P. Mishra, C. Hauser, H. Ziemek, “Protecting Privacy of Identities in Federated Operator Environments“, in Proceedings of IST Mobile & Wireless Communications Summit 2005, Dresden.
3. A. Olivereau, A. F. Gómez Skarmeta, R. Marin Lopez, B. Weyl, Pedro Brandão, P. Mishra, C. Hauser, “An Advanced Authorization Framework for IP-Based B3G Systems”, in Proceedings of IST Mobile & Wireless Communications Summit 2005, Dresden.
4. Liberty Alliance Open Standards: http://www.projectliberty.org/.
5. W3C, Platform for Privacy Preferences, P3P 1.0, 2002.
6. J.Clarke, S. Butler, C.Hauser, M. Neubauer, P. Robertson, I.Orazem, A. Blazic, H. Williams, Y. Jang, “Security and Privacy in a Pervasive World”, Eurescom Summit 2005, April 2005.
7. A. Yegin, Y. Ohba, R. Penno, G. Tsirtsis, C. Wang, "Protocol for Carrying Authentication for Network Access (PANA) Requirements", IETF Internet Draft <draft-ietf-pana-requirements-08.txt>, work in progress, June 2004.
8. IEEE Standard for Local and Metropolitan Area Networks, “Port-Based Network Access Control”, June 2001.
9. L.Blunk , J.Vollbrecht, “Extensible Authentication Protocol (EAP)”, draft-ietf-eap-rfc2284bis-07.txt.
10. Ph. Hallam-Baker, E. Maler (eds.), “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1,” OASIS Standard, Version 1.1, September 2nd 2003, http://www.oasis-open.org.
11. B.Weyl, “SAML-based Access Control for Broadcast Services”, MMC 2005, Berlin.
12. Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC2401, November 1998.
13. IETF PKI WG, www.ietf.org/charters/pkix-charter.html.
14. “Deliverable D3.4.1: A4C Framework Design Specification”, Daidalos Consortium, Sept. 2004, www.ist-daidalos.org.
15. J. Arkko, J. Kempf, "Secure Neighbour Discovery (SEND)", IETF Internet-Draft: draft-ietf-send-ndopt-03, work in progress, Network Working Group, January 2004.
16. Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet-Draft: draft-guerrero-manet-saodv-00.txt, 12 August 2001.
17. B. Lamparter, K. Paul, and D. Westhoff, "Charging Support for Ad Hoc Stub Networks", Elsevier Journal of Computer Communication, "Internet Pricing and Charging: Algorithms, Technology and Applications", Elsevier Science, Volume 26, Issue 13, August 2003.