Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 1

Artikel: Access control in interdomain security management

Autor: Maier, Stefan / Bach, Rene / Rao, Sathya

DOI: https://doi.org/10.5169/seals-876416

DVP

Access Control in Interdomain Security Management

In the TRUMPET Project a security management architecture has been developed. The architecture was developed to support secure and high integrity interactions between administratively separate bodies concerned with the provisioning of broadband telecommunications services.

STEFAN MAIER, RENE BACH, SATHYA RAO, BERNE

The following article describes this project and discusses access control features of security management in detail. The chosen architecture was realised in implementing security management package using the various known, specifically Java, CMIP ind

CORBA. These technologies were deployed so as to provide a technology independent interface information model following the TMN recommendations. The field trials are conducted in Switzerland, Scotland and France to validate the architecture and the implemented security management package.

Security Policy

The project has studied the security policies. The approach taken adopts a comprehensive method of risk assessment which builds upon state of the art results of previous European research projects, together with standardisation activities in the field of TMN security. TRUMPET only considers management systems which conform to the TMN model. Furthermore, it is assumed that even customers will be in possession of at least a rudimentary TMN system. Thus, all interdomain interactions proceed over TMN X reference points, which TRUMPET assumes will always be realised as X interfaces, since it is very unlikely that different TMN systems will share equipment. Every management system will need its own security policy. In the TRUMPET context, each TMN system (of a provider or a customer) is viewed as a separate security domain, possibly comprising subdomains. Since the domain authorities are unrelated, the security domains must be viewed as independent domains. Elements of independent security domains can only communicate when they share a common interdomain security policy, agreed between the domains. This interdomain policy is implemented in each domain as part of the internal security policy of the domain. In a multiprovider situation, where the number of providers may grow large, it is clear that this interdomain policy, which is applied at the X interfaces between providers, must be standardised, and agreed between all providers involved. In effect, a limited set of security policies is needed, covering security requirements of various severity. The method applied to arrive at the policies is largely based on RACE II PRISM results [RACECFS H211] that have been contributed to, and to a large extent adopted by, the on-going ETSI work on TMN security [ETSI NA-0432081].

The TRUMPET secure interdomain service management systems have been developed and tested, in system trials distributed across Europe in Switzerland, Scotland and France.

Architecture

Management System Architecture

TRUMPET focuses on the secure operation of interdomain management systems within the Open Network Provisioning (ONP) framework. The TRUMPET scenario shown in figure 1 involves the following players: two (or more) Public Network Operators (PNOs), a Value Added Service Provider (VASP), and a number of customers at various sites – Customer Premises Networks (CPNs) [TRUMPET-D61].

Security Architecture

The security architecture consists of a set of security components, which can be used by TMN platforms with open or closed protocol stacks.
The architecture is shown in figure 2, with dashed lines indicating the components added by TRUMPET, and solid lines indicating existing components.

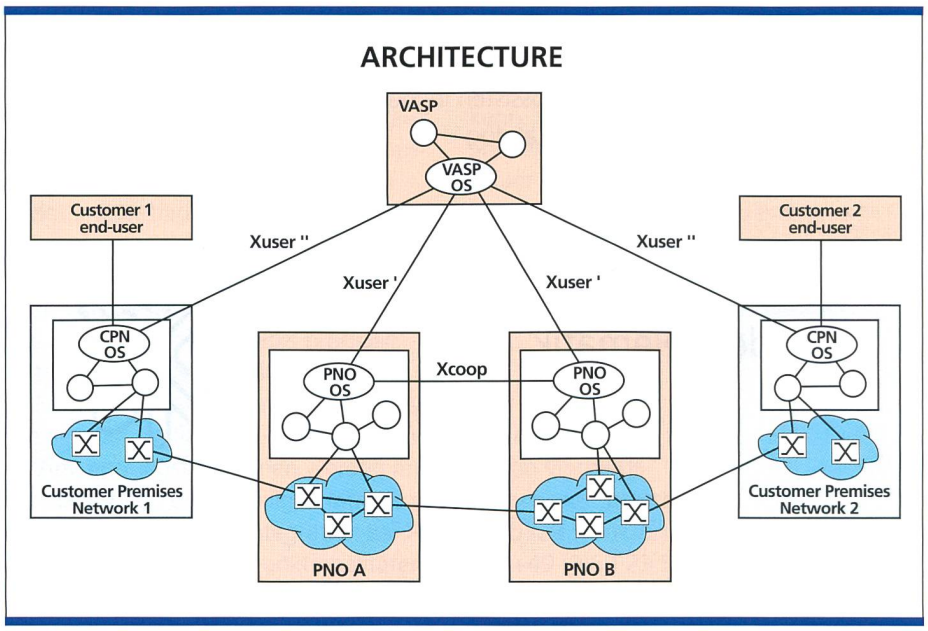

Fig. 1. The TRUMPET Reference Architecture.

The architecture is targeted towards a realisation of the security policies defined by TRUMPET, although it should be able to support a larger variety of policies. However some policy decisions inherently form the architecture, like the decision to use public key cryptography. The system architecture supports the following security services:

- security context negotiation, is somehow restricted due to the lack of protocol support for exchange of the negotiation information
- data origin authentication
- access control with respect to (establishment of) a management association between peer entities, and for operations on managed objects
- selected field and connection data integrity
- selected field and connection data confidentiality
- key management
- security audit and alarm
- to some extent non-repudiation of origin and non-repudiation of delivery, although these services are not fully specified

Management of security is for most parts internal to the individual management domains, with the exception of parts of the management of certificates for cryptographic keys. TRUMPET's security policies prescribe use of public key mechanisms for authentication, non-repudiation, and possibly also for key management (of secret keys). Use of TTPs in the role of Certification Authorities (CA) is described. Each provider participating in interdomain management must be in charge of a CA which issues certificates for the subjects within the provider's domain. The providers' CAs must in turn be certified by an interdomain management CA. This certification structure should be placed under the umbrella of existing initiatives for public key infrastructure, notably the ICE-TEL project [ICE-TEL].

System Components Level overall Architecture

Figure 3 shows main components of the security architecture, the internal architecture of the Security Support Component (SSC), and the contract interfaces of the SSC to other components. The security services of the SSC can be accessed through an Adapter Component. The purpose of the Adapter Component is to transform platform specific syntax (e. g. XOM objects [XOM]) to generic data structures (e. g. BER encoding). With this approach, platform specific code can be restricted to the Adapter Component, and the SSC can be reused without major modifications for other management platforms.
The implementation of security package is based on the SecuDE software package [SECUDE].

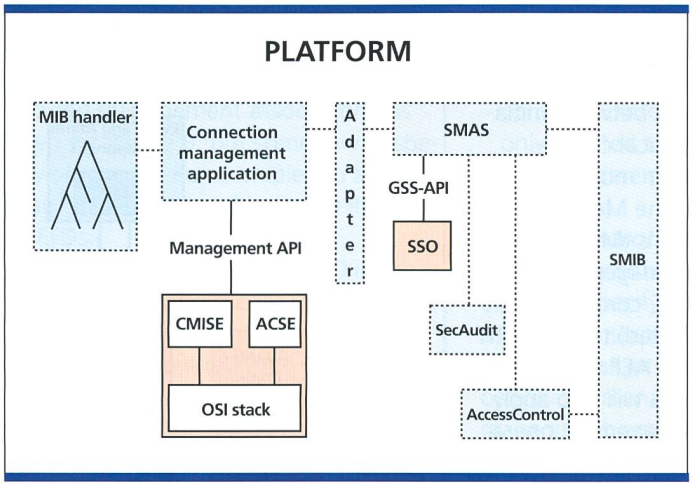

Fig. 2. Architecture for a Commercial Management Platform.

Access Control

The access control architecture is based on [ITU-T X.812] which specifies an access control framework, and [ITU-T X.741] which specifies a model for controlling access to management information and operations. The access control profile AOM24322 (ACL: Access Control List with Item Rules) [ISP 12060-9] are used.
The actual access control is carried out within each individual domain. However, the domains need to agree on the nature of the Access Control Information (ACI) and how this information is exchanged over the X interface. TRUMPET aims at use of X.741 for access control even in other environments than CMIS/P (for example RMI for Java). The choice of technology will not impact the architecture presented here.

Global Access Control Architecture

Figure 4 shows the global access control architecture. The black boxes refer to locations where the access control functionality/mechanisms are built into the system. In the initiator domain, access control is applied to outgoing management association requests and outgoing management notifications (event reports). In the target domain, access control is applied to incoming management association requests, incoming management operation requests and incoming management notifications. Each of these aspects of access control are further developed in the next sections. The security in TRUMPET is applied point-to-point, with no transitive security implemented at present.
For incoming access control in the target domain, the access control services may in the future require the support of TTPs. Use of Privilege Attribute Certificates (PAC), where a privilege attribute server in the initiator domain (or perhaps even an external TTP) signs a certificate for the access rights granted to the requesting entity, is for further study in TRUMPET.

Location of the Access Control Functions

The functions needed for the enforcement of access control are the Access control Decision Function (ADF) and the Access control Enforcement Function (AEF). The AEF will be integrated in the Security Support Component (SSC) and the ADF will be realised as a separate Access Control component, as shown in figure 3. The ADF uses information in a Security MIB (S-MIB) which contains information relevant to the ADF such as Initiator lists, target lists, ACL for operations, Access Control Rules and rules. Access control Operation causes potential event reports, which are forwarded through EFD (Security Audit component) to the logs. Event reports are generated by AEFs, according to X.812.
The static location of the access control functions in the OSFs within the TMN OSs on the initiator and target sides is shown in figure 5. (The Adapter component is neglected for simplicity when access control is discussed.) This access control architecture can be realised on

both commercial and research TMN platforms. As defined in X.812, the AEF shall enforce the access control and always be a part of the access path between initiator and target. The practical consequence is that the AEFs in most cases will be integrated with the Message Communication Functions (MCF) on both sides. Since the management entity (MAF) has to call the SSC component (in which the AEF is integrated) to establish a secure association, the AEF will be in line with the activity. This will also apply to access control to management operations if the target SSC automatically is called first when the request comes in.

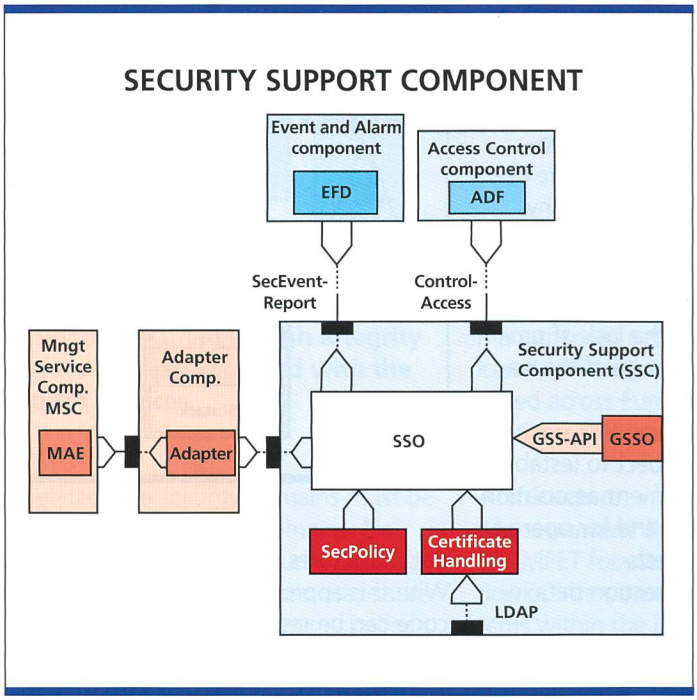

Fig. 3. Graphical representation of the security support component.

Access Control to Management Associations

The access control policy requires access control to be enforced in the initiator and the target domains to ensure that the initiator is authorised to establish a management association to the specific target. Access control to management associations is required by all security profiles, and is performed as an integral part of the establishment of a secure management association. As shown in figure 5 both domains will need an AEF, an ADF and a S-MIB.

Initiator side: It is assumed that the initiating person/entity/process (illustrated by the Human Machine Adaptation, HMA, in fig. 5) has a group or role identity assigned by the initiating system during the login. The MAE requests secure association establishment by calling the SSC, specifying the identity of the target MAE, its own identity, and possibly the identity of an entity it is acting on behalf of (for example a human operator). The initiator identity used for access control has to be the same identity as the one which is authenticated during association establishment, i. e. the legal initiator entity. The SSC invokes access control in the initiator domain, to decide whether the association establishment request shall be allowed to leave the domain. If access is granted, the MCF carries out the association request to the target domain under the identity of the initiator domain (or for the advanced profile a group or role). After processing of the association request in the target domain, the initiator domain receives a reply to the management request. The response may be a failure report if access control in the target domain yields a negative result. The activity concerning access control will be forwarded by the EFD and written in a log. Access control will not be applied to the association response.

Target side: Upon reception of the management request, the SSC will initiate access control using the initiator ACI (initiator domain or role identity) contained in the request. The initiator TMN is granted or denied to set up the requested management association by the ADF. The activity is taken note of and forwarded by the EFD to the log.

Access Control to Management Operations

This control is required for all security profiles only differed in the granularity of the access control. Originally TRUMPET specified access control to operations in both the initiator (outgoing) and the target (incoming) domains, where the initiator domain would validate the operation before it was even allowed to leave the domain. The intention was to use the access control profile AOM24326 (capability based) [ISP 12060-9] in the initiator domain. Access control to management operations in the initiator domain will be difficult to realise unless the initiator has a "shadow MIB", or otherwise has detailed knowledge of the contents of the MIB at the target side. Especially for the interdomain case, it is not expected that many targets will trust the initiators enough to give them a copy of the MIBs. Validation of (taking the example of a VASP) whether a particular customer/user is authorised to perform a specific operation (which will be carried out under the VASP's identity or a role assigned to the VASP towards the PNO) therefore has to be determined by other means. TRUMPET will base this decision on the role that the customer or user was assigned when logging onto the VASP i. e. a previous access control decision. Operations performed by a certain customer (identified by a role) will only be allowed to trigger certain outgoing operations towards the PNO. The lack of outgoing access control will certainly be a weakness of the solution since this outgoing access control would be highly appropriate as an extra screening.

Access control for management operations in the target domain is based on an identity scheme (identity of initiator domain or a role, as discussed above) using Access Control Lists (ACL).

Initiator side: Outgoing access to management operations will not be implemented but handled as described above.

Target side: The MAE receives the management operation request from the initiator domain. The SSC passes the decision request to the ADF containing the following information: initiator ACI, requested management operation, ACT related to the data, identification of the target object class and instance, action identifier, attribute identifier. The ADF bases its decision on the above information together with the retained ACI, the

target ACI, the access control rules and the contextual information.
The ADF uses an ACL to determine whether the initiator may access the particular target in the interdomain MIB. To do this, the <Initiator, Target> pair is mapped to the access rights (of the initiator) in the ACL. If access to the target is granted, the MAE may apply the management operation to the target. Note again that initiator identity is either that of the initiator domain, or one of a few roles attributed to that domain.
It is expected that an operation will trigger one access decision only, although this is at the discretion of the target domain. If the scope of the operation implies that the initiator has access to only some of the resources requested, the complete operation will be denied.

Access Control to Notifications

This kind of control will only be implemented for the advanced security profile. Notifications are forwarded to managers that have previously subscribed to receive these notifications. This is enforced in the agent by the event forwarding discriminators (EFD). Because subscribing to receive notifications from an agent from a remote domain is a management operation that is submitted to interdomain security measures, only legitimate managers will have registered to receive notifications and only those managers will receive notifications. Therefore, there is no need for extra outgoing access control mechanisms in the agent domain, notification even if such outgoing access control is specified by X.741.
The above guarantees that notifications will not be emitted to illegitimate managers, it does not stop misbehaving agents from emitting notifications to managers. In the manager domain, it is possible that unwanted notifications are received from properly authenticated (notifications are received only after a secured management association has been established), but somehow misbehaving agents. For example, an agent may not have properly secured its access to EFDs.
A notification is issued by a MO in the MIB and passed to the EFD by the MAE. If the notification passes the discriminator filter, an event report is generated and sent to the target manager. On the manager side, the ADF verifies whether the incoming notification should be processed by this manager/MAE.

Access Control Information (ACI)

Access Control Information needs to be exchanged between real systems as a part of the access control function. The ADF requires this information to be able to decide whether access shall be granted or denied. The types of ACI include initiator, target, access request, operation, operand and contextual information as described in X.812. ACI includes [ITU-T X.741] (table 1):
- access control rules (see next section)
- the identity of the initiator of the access request (part of the initiator ACI, which is ACI about an initiator)
- capabilities and security clearances associated with the initiator (initiator ACI)
- information pertaining to the authentication of the of the initiator (Retained ADI)
- the management information identities (targets) to which access has been requested (Target ACI)
- capabilities and security clearances associated with the target (Target ACI)
- the permitted operations that may be performed on the management information (initiator ACI, Target ACI)
- information retained by the access control decision function (ADF) for subsequent use (Retailed ADU)
- contextual information (e. g. access is only granted to special locations or within a time period)

Access Control Rules

The access control rules provide a flexible means of specifying management policy as a relationship between initiator domain and target domain in terms of the operations managers can perform on managed objects. Constraints (contextual information) will also be a part of the access control rules. Access control procedures (i. e. validation of initiator-bound ACI, identification of the target etc.) will be performed according to the chosen Security Policy, which is specified by access control rules.
The access control rules is the part of the Access Control Information (ACI) which represents the permitted operations and the conditions upon their execution in a security domain. There are five classifications of access control rules which are to be applied by the Access Decision Function (ADF) [ITU-T X.74 1]:
Globally deny rules;
access control rules that deny access to all targets. If a global rule denies access, then no other rule shall apply. If a global rule does not deny access, then the item deny rules are imposed.
Item deny rules;
access control rules that deny access to particular targets. If an item deny rule denies access, then no other rule shall apply. If an item deny rule does not deny access, then the global grant rules are applied.
Global grant rules;
access control rules that grant access to all targets. If a global rule grants access, then no other rule shall apply. If a global rule does not grant access, then the item grant rules are imposed.
Item grant rules;
access control rules that grant access to particular targets. If an item grant rule grants access, then no other rule shall apply. If an item grant rule does not grant access, then the default rules are applied.
Default rules;
the access control rules to be applied when no other rule has specifically granted or denied access. The default rules shall grant or deny access.
Regarding attributes or attributes values

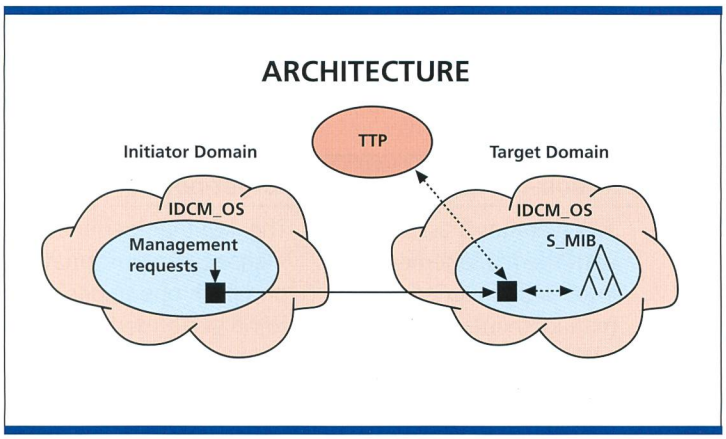

Fig. 4. Global architecture for access control.

(i. e. item grant rules) the following permission categories may be applied:
- Compare: This permits the attributes and its values to be used in a compare operation.
- Read: If granted, the respective attribute and its values may be returned as entry information in a read or search operation.
- Filter Match: If granted, this permits the evaluation of a filter within a search criterion.
- Add: If granted for an attribute, a complete attribute may be added where none was existing before. If granted for an attribute value, a new attribute value may be added to an already existing attribute.
- Remove: If granted, this permits the removal of an attribute and all of its values. If granted for an attribute value, it permits the removal of an individual attribute value.
- Disclose of Error: If granted for an attribute, it permits the disclosure of the existence of an attribute during an attribute or security error. If granted for an attribute value, it permits disclosure of the existence of an attribute value during an attribute security error.

Access Control Schemes

There are five access control schemes which are considered in X.812:
- identity based with no protocol
- identity based with security certificate (Token or Access Control Certificate, ACC)
- capability based with token
- capabillty based with ACC
- label based

Based on the evaluation the following schemes are chosen to fulfil the advanced security profile.

Initiator side:
- Management associations: as stated in [D2B], the number of initiators is not expected to he very high. When operating, in a distributed multidomain environment, a mandatory access control policy should be applied to allow domains to interconnect. Different levels of access – or different capabilities – to the target shall be given to the potential users in the initiator domain. This role based security policy will be enforced with a capability based scheme with token. The initiator will be assigned an initiator role or group which identifies the capabilities given to him.
- Management operations: the capability level assigned for access to management associations will also determine the accessible management operations. This means that the possible set of management operations will be given by the initiator role or group assigned after successful access control to management associations.
- Management notifications: no access control except for that implied by the filtering in the EFD.

Target side:
- Management associations: when considering the future laws and regulations, an identity based scheme with token is expected to be the natural choice for management associations. The capabilities can be groups of default management mechanisms which every TMN has to provide, by law, to every authorised (i. e. licensed) counterpart. The identity granularity will then be low for management associations (i. e. all initiators from the same domain will have equal identity).
- Management operations: the initiator will have the possibility to operate on the default capabilities assigned to his group or role when access for an association is granted. The target domain owner will most probably want to have the possibility to control the contractual access rights (as a part of the contractual security policy between initiator and target) in his domain. The identity based scheme with token can support this control, and the fine granularity which will be needed for controlling access to management operations at attribute level. The identity will be recovered from a mapping of the label of the initiator domain and the group or role assigned to the initiator in the initiator domain. In principle, it should only be possible to gain access in one way i. e. no alternative ways to gain access to the system should exist.
- Management notifications: the filter function specified in X.741 will be used on the target side for management notifications.

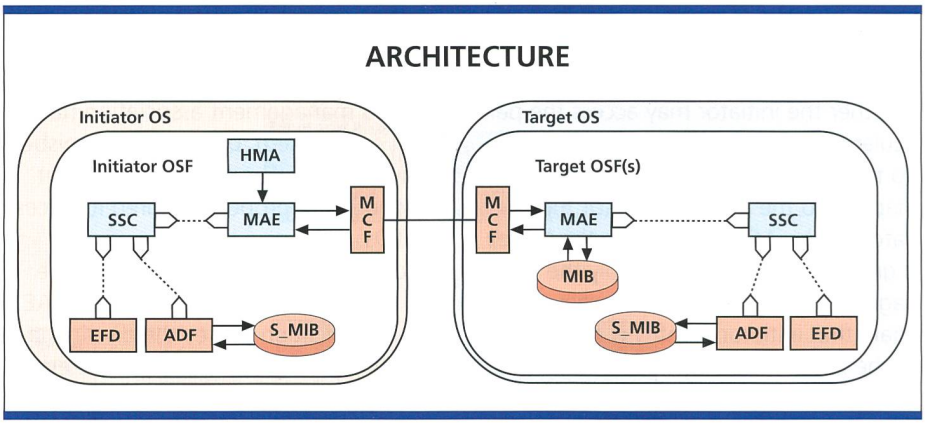

Fig. 5. The TRUMPET access control architecture.

Conclusion

This paper briefly introduced the security management architecture implemented by the TRUMPET project for securing TMN X interfaces, in terms of:
- security policies, which are definitions of the security services and mechanisms selected for use on X interfaces, for varying levels of security
- system architecture, which is identification of the components and interfaces used to implement the security policies within one TMN OS
- Details of Access Control functionality

The security package is intended to be fairly general. Although it is mainly targeted towards TMN compliant systems communicating by means of CMIS/P over

Initiator-bound ACI	Action-bound ACI	Target-bound ACI
The ACI provided by or otherwise associated with, the initiator of a management request.	The ACI that is associated with the management information carried in management operations and event reports.	The ACI that identifies management information on which operations are to be performed.

Table 1. Access control information categories.

an OSI-based protocol stack, adaptation to other environments should be fairly straightforward. The security architecture is independent from the actual management application to be used, and of the kind of X interface (Xcoop or Xuser).

9.4

Acknowledgement
The work conducted in the TRUMPET is partially financed by Bundesamt für Bildung und Wissenschaft (BBW), Swisscom and the European Union. The contents of the paper is the result of the work done by consortium members of the project.

***Stefan Maier**, Telscom AG, Sandrainstrasse 17, 3007 Bern*

***Rene Bach** received his PhD from the University of Geneva (Molecular Biology) in 1980. He then spent six years in the USA, first as a knowledge expert with the CSD at Stanford University, then as a knowledge engineer Witz Varian Associates in Palo Alto. After his return in Switzerland, he was a senior engineer with Ascom, then moved to the Engineering School of Berne, where he contributed to the inception of a postgraduate study in informatics and telecommunication. In 1996 he joined Telscom to work on ACTS projects. Since 1998, he is a member of the scientific staff at the Swiss Statistical Office in Neuchâtel.*

***Dr. Sathya Rao** has degrees in electrical communication engineering from Bangalore University and the Indian Institute of Science. He moved to Switzerland in 1980, where he gained his doctoral degree from Neuchâtel University. In 1986, he joined Ascom, where he led much of the work on ISDN systems and broadband communications. He was one of the core members of the team responsible for defining the European research framework on advanced communications, i. e. RACE and ACTS. In 1995, he founded Telscom, providing consultancy services and support to advanced communication research work. Telscom has grown ever since into a company which is involved in ATM system development and internet and ATM solutions for business needs. Sathya has published three books on broadband networking issues as an editor and is an editor-in-chief of the journal "Interoperable Communication Networks (ICON)". He has many patents and publications to his credit. Sathya Rao and his company have an established record in organising international and European conferences. Under the patronage of the European Commission, he has organised many international workshops, and distributed seminars using the ATM networks and applications across European centres.*

Zusammenfassung

Zugriffskontrolle beim Sicherheitsmanagement zwischen verschiedenen Bereichen

Dieser Beitrag beschreibt die Architektur des Sicherheitsmanagements, welche im Projekt TRUMPET entwickelt wurde und geht im Detail auf Zugriffskontrollfunktionen beim Sicherheitsmanagement ein. Die Architektur wurde zur Unterstützung des sicheren und hochintegren Austausches zwischen administrativ von einander unabhängigen, für die Verbreitung von Breitbandkommunikationsdiensten verantwortlichen Einheiten entwickelt. Die gewählte Architektur basiert auf der Implementation eines Sicherheitsmanagementpakets, bei dem die verschiedenen bekannten Technologien, insbesondere Java, CMIP und CORBA eingesetzt wurden. Das Ziel bestand darin, ein technologieunabhängiges Schnittstelleninformationsmodell gemäss TMN-Empfehlungen zu schaffen. Die Feldversuche zur Validierung der Architektur und des implementierten Sicherheitsmanagementpakets finden in der Schweiz, in Schottland und in Frankreich statt.

Ein Standard für Interface Notebook-LCD

Es hat lange gedauert, aber jetzt haben sich die führenden Hersteller geeinigt: Die wichtigsten Standards für die Austauschbarkeit von Flachbildschirmen in Notebooks wurden jetzt festgeschrieben. Bisher hat fast jeder LCD-Hersteller gemacht, was er wollte – mit dem Erfolg, dass ein Wechsel auf einen anderen Lieferanten unmöglich war. Die Dell Computer Corp. als die grösste Computerherstellerin hat seit einem Jahr massiven Druck ausgeübt und nun haben sich die wichtigsten LCD-Hersteller und OEMs geeinigt (und den anderen bleibt nichts anderes übrig als sich anzuschliessen): Von der Lage der I/O-Steckverbinder über die elektrischen Interfaces bis hin zur Länge der konfektionierten Verbindungskabel wurden wichtige Standards gesetzt.

Kommen die Keramikgehäuse wieder?

Nachdem sie vor einigen Jahren als «zu teuer» verbannt wurden, scheinen sie jetzt vor einem Come-back zu stehen: die Keramikgehäuse. Jedenfalls nimmt die Nachfrage wieder zu: Auf der einen Seite durch den Boom für nahezu alles, was mit Hochfrequenzanwendungen (vor allem in der Mobiltelekommunikation) zu tun hat. Zum anderen fragt die Automobilindustrie Mikroelektronik im Keramikgehäuse nach. Das wurde auf der Jahrestagung der International Microelectronics and Packaging Society bestätigt. Um den Anwendern eine Perspektive über die zu erwartenden Leistungsdaten zu geben, wurde eine Roadmap für die nächsten zehn Jahre erstellt.

Kommunikationsterminal am Handgelenk

Philips-Forscher arbeiten daran, in wenigen Jahren den alten Science-Fiction-Traum vom universellen «Communicator» in der Armbanduhr zu realisieren: E-Mail, Telefon, Bildübertragung, GPS-System – all das soll aus einem Gerät am Handgelenk kommen. Dazu werden gegenwärtig die nötigen Systemarchitekturen entwickelt. Die Uhrzeit wird man auch noch ablesen können. Dieses Kommunikationsterminal wird selbst eine mikrosekundengenaue Funkuhr in den Schatten stellen.