Development of Security Policies for Inter-domain Management

Jon Ølnes[1], Dominique Maillot[2]

Introduction

ACTS project AC112, TRUMPET (Inter-domain Management with Integrity), studies interactions between management domains with particular emphasis on the security of such operations. One of the first tasks of the project is to define a set of security policies, suitable for securing inter-domain management interactions with various security requirements. Inter-domain management has two facets:

- co-operation between the management systems of different service providers and network operators[3], where, in the context of TRUMPET, each system is viewed as one (top-level) management domain, possibly containing a domain hierarchy;

- customer / end user access to management functionality, especially service management, where a customer is expected to possess at least a minimal management system, constituting a separate management domain.

The first facet corresponds to both the Xcoop and Xuser TMN interfaces [M3010], while the definition of X-interfaces[4] for customer/user access has not been treated in the standards. In our view, there is no conceptual difference between an X-interface between a service provider and a network operator, and an X-interface between two network operators. Thus, in this document we use the term "Xuser" for an X-interface between a real customer/user and a provider of any type, and "Xcoop" for an X-interface between two providers of any type.

Every provider will regard the management system as a critical resource to its operation. A breach in the security of the management system may lead to:

- malfunctioning or breakdown of the management system itself;

---

[1] Norwegian Computing Centre (NR), P.O.Box 114 Blindern, N-0314 Oslo, Norway. E-mail: Jon.Olnes@nr.no

[2] Télis, 3-5 Rue Hélene Boucher, F-78285 Guyancourt Cedex, France. E-mail: maillot@pmail.sqy.tel.telis.fr

[3] Both called "provider" in the following, since the distinction between network and value-added services is not important to this discussion.

[4] Customer/user access could be through TMN F-interfaces. However, external access to a TMN via F-interfaces does not fit well with the TMN functional architecture. A realistic assumption is to assume that customers will be in possession of at least some minimal TMN OS functionality, capable of communicating over an X-interface. Such a customer module will be implemented by TRUMPET for the project's trials.

- compromise of information or functions in the management system;

- degradation in the QoS of the networks or services which rely on the management system, in the worst case causing denial of service to all customers;

- compromise of customer communication, for example through an attack on the security management system.

Thus, continuous and secure operation of the management systems is essential for successful introduction and use of IBC services. The management systems will contain customer related information and network / service related information, structured as distributed databases. Much of this information will be highly sensitive, especially with respect to integrity. The privacy of the users and customers must also be ensured, and business considerations will require confidentiality of some information. Especially in a multi-provider environment, accountability measures are needed, in order to determine responsibilities for the effects of the management actions performed. For each management system, a security policy must be defined in order to guarantee adequate security.

It is crucial to providers, and to some extent also to the customers, that the management services are available when needed, with a sufficient QoS (Quality of Service). Lack of availability may lead to reduced QoS of the services, which in turn may lead to loss of market shares. The security policies for the management systems should address the availabilty problem.

A security policy specification is not an implementation specification, but rather a selection of security countermeasures. The realm of a policy is the security domain(s) to which it is applied. For each domain, there is a security authority responsible for the policy. Implementation of countermeasures may be:

- physical, which is (at least almost) entirely outside the scope of TRUMPET;

- logical, especially hardware and software implementing security services and mechanisms, possibly also recommendations for network or system configuration;

- administrative, like assignment of responsibilities, procedures and work routines - this is at least to a large extent outside the scope of TRUMPET.

Security countermeasures may be:

- preventive, to avoid incidents;

- detecting, to discover and possibly limit the effect of incidents;

- correcting, to repair damage, and restore the system to a secure state.

Usually, preventing countermeasures are the most important category, but the other two need to be considered as well.

The security work in TRUMPET is based on, and will input to, standardisation efforts for TMN security, notably the ETSI/NA4 working group on TMN security [ETSI-NA043208]. However, ITU/SG11/Q29 and EWOS activities on standards profiling are also possible targets.

Inter-domain Security Policies and Scope of TRUMPET's Work

As stated, each 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 sub-domains. Since the domain authorities are unrelated, the security domains must be viewed as independent domains [ISO10181-1].

Efficient provisioning of telecommunication services in a multi-provider environment, that is when the services are based on underlying (network and other) services obtained from a multitude of providers, is only possible if the management operations are at least to a large extent automated. Thus, the deregulation of the European telecommunications market implicitly calls for definition of Xcoop interfaces between the providers' TMN systems, where the appropriate X-interface should be accessible to any service provider[5] that buys services from the owner of the TMN system. This access requirement calls for standardisation of the X-interfaces, including security.

Elements of independent security domains can only communicate when they share a common inter-domain security policy [ISO10181-1], agreed between the domains. This inter-domain policy is implemented in each domain as parts of the internal security policy of the domain. In a multi-provider situation, where the number of providers may grow large, it is clear that this inter-domain policy, which is applied at the X-interfaces between domains, must be standardised, and agreed between all providers involved. In effect, a set of security policies is needed, covering security requirements of various severities.

Security of inter-domain management interactions has three other aspects, which are outside the scope of the policy work in TRUMPET, but which may be studied by the project at a later stage:

- ensure an approximately uniform level of security end to end, that is within all TMNs involved in a management interaction, and on the interfaces between them - note that protection measures may be widely different in different TMNs;

- devise countermeasures to maintain the security of one particular management domain when connecting to other domains, given that new threats or increased vulnerabilities may result from the interconnection, that is specify changes to intra-domain policies given the inter-domain environment - use of firewalls may be one example here;

- specify mapping between security functions and attributes valid inside one domain, and functions and attributes applicable under the inter-domain policies, that is the mapping between the internal and external security policies - this may be complex if the policies are widely different.

The requirements for standardisation of the Xuser interfaces towards customers are less clear, especially with one-stop shopping agreements between the customers and specific providers. It is clear that Xuser interfaces are useful, to let the customers access information or perform management operations that would otherwise require intervention by the provider's personell. Such access will of course be strictly limited and well secured. The main requirement for standardisation is openness with respect to selection of providers and purchasing of (management) software from the customers' point of view.

---

[5] Existing telecommunications organisations (like PNOs) will probably only open up their management system for external access if "someone points a gun at their head". This "gun" may either be a regulatory demand, or an environment where competition makes it impossible to avoid providing such services.

It is intended that the security policies developed by TRUMPET shall be applicable to both Xuser and Xcoop interfaces. Several policies are necessary because of requirements of varying severity, but only a small number of policies, for example three, should be developed. The policies should be sufficiently general to be used for both Xuser and Xcoop interfaces. The policies must be agreed between the authorities of all TMNs involved, and should be applied to all management interactions on X-interfaces.

Policy Development Method

A methodical approach is necessary for development of security policies. The method followed by TRUMPET is shown in the figure on the next page. The work in TRUMPET extends the results of the RACE/PRISM project [CFS-H211]. TRUMPET's work on the policy establishment phase will be concluded by the issuing of the project's Deliverable 2 [DEL-2] by the end of June 1996. The project will then enter the implementation phase. It is not expected that the implementations done by TRUMPET will actually be formally tested against evaluation criteria.

This paper gives a short description of the steps performed during the policy establishment phase. The policy implementation phase is not described.

Laws and Regulations

The Open Network Provision (ONP) directive [ONP] sets the framework for the liberalised market. Although this applies only to networks at present, it may be assumed that similar directives will be applied to value-added services in the near future. ONP demands interconnection of networks (and presumably services later on) through well-defined interfaces, open in principle to all other licensed providers. A service will frequently be based on network capacity from several networks, and may even be based on several other services, offered by a range of providers.

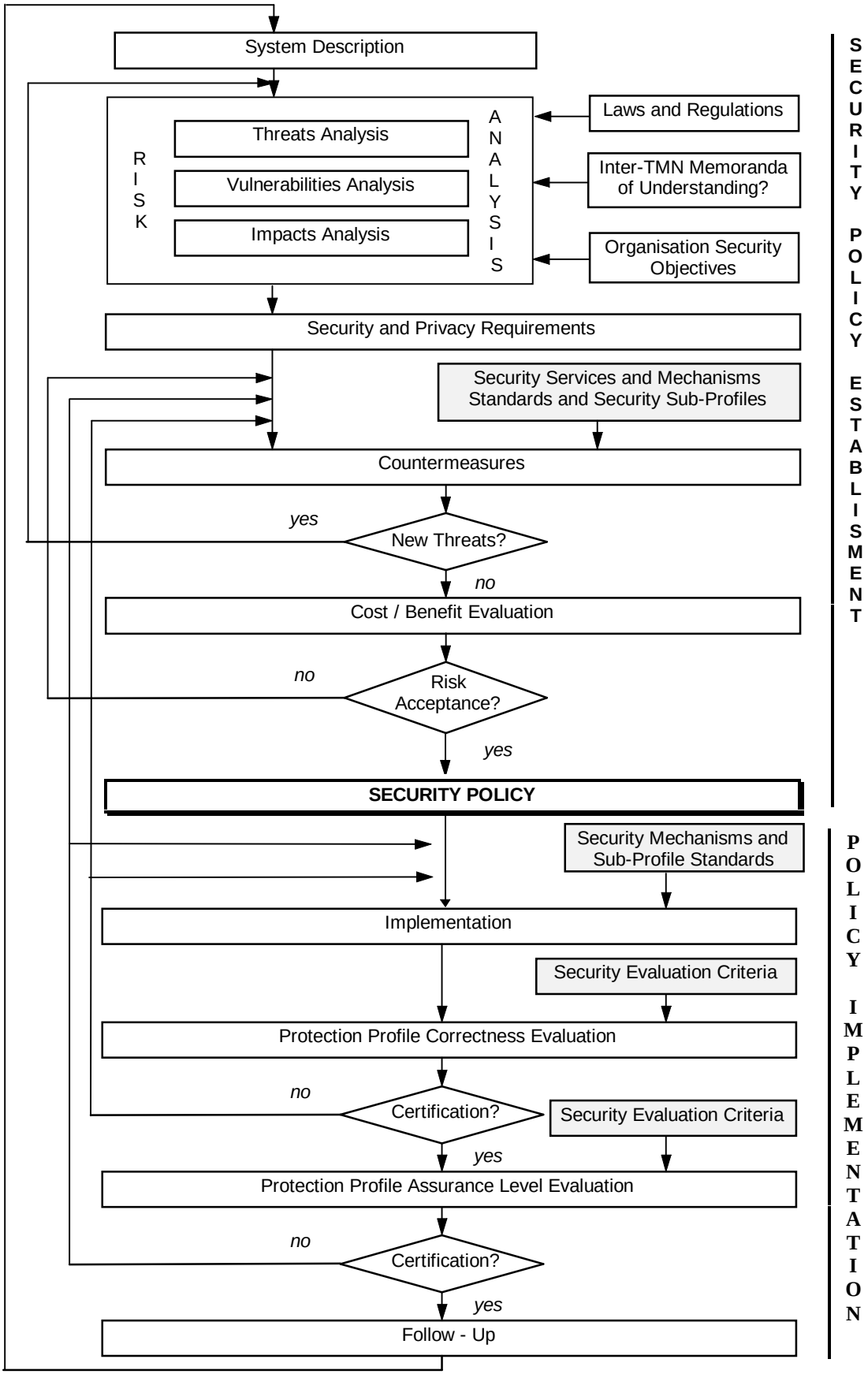
Implicitly the ONP directive demands interconnection of the management systems of the providers, since this is the only way that services which span several networks may be managed in an efficient way. Management services will also be offered to customers, presumably in most cases viewed by them as integrated parts of ordinary services. ONP-like directives for service provisioning may even take effect for management services, which in this respect may be considered as value-added services by themselves. The requirement for open, well-defined interfaces is valid for management systems. One important task of TRUMPET is to contribute to making these interfaces well-secured as well.

The regulatory area was examined in detail by the RACE/PRISM project [CFS-H211, MAILLOT-95-1].

Inter-TMN MoUs

For some new telecommunications services, for example GSM mobile telephony, Memorandums of Understanding (MoU) - normally several per service - have been developed as standardised agreements. Providers signing the MoUs thereby agree to follow their contents with respect to provision of the service, and especially with respect to co-operation with other providers of the same service.

Such agreements can be a useful tool to formally establish the rules for co-operation in service and network management as well. It must be determined if specific MoUs are needed for management of each network / service class, or if "generic" management MoUs are possible. Correspondingly, it must be determined if specific security MoUs are needed for security of each network / service class (and its management), or if "generic" security MoUs can be envisaged.


System Description
RISK
Threats Analysis
Vulnerabilities Analysis
Impacts Analysis
ANALYSIS
Laws and Regulations
Inter-TMN Memoranda of Understanding?
Organisation Security Objectives
Security and Privacy Requirements
Security Services and Mechanisms Standards and Security Sub-Profiles
Countermeasures
yes
New Threats?
no
Cost / Benefit Evaluation
no
Risk Acceptance?
yes
SECURITY POLICY
Security Mechanisms and Sub-Profile Standards
Implementation
Security Evaluation Criteria
Protection Profile Correctness Evaluation
no
Certification?
Security Evaluation Criteria
yes
Protection Profile Assurance Level Evaluation
no
Certification?
yes
Follow - Up
SECURITY POLICY ESTABLISHMENT
POLICY IMPLEMENTATION

The assumption of TRUMPET is that a limited number of protection profiles can be developed, which can be referred to in future MoUs for security of management.

Signing of the MoUs should be mandatory in order to get a license to operate, and a provider signing a security MoU must at the same time agree to provide at least the same level of security internally in its TMN. This will ensure that information is protected in an approximately uniform way in the source and destination TMN as well as in transit between them.

MoUs should also cover issues like selection of TTPs, and procedures to settle disputes. Other agreements may concern handling of alarms and incidents.

Organisation Security Objectives

According to ETSI/STAG (Security Technical Advisory Group), description of basic security objectives is one of several steps in a requirements capture. STAG states [ETSI-NA002501]:

> *"Depending on the internal structure and the intended tasks of the system a list of basic Security Objectives of a very general and generic nature should be defined before any detailed security investigation takes place. Knowing that an absolute secure system is illusory and prohibitively expensive the Security Objectives definition should give a clear orientation for the succeeding investigations."*

The security objectives are high-level goals for the security of an organisation. Together with a risk analysis, to a large part they determine the security requirements for the management system, including relationships to customers and other service providers, The security policy shall meet the requirements of the organisation.

In the Introduction section to this paper, we gave examples of incidents that may happen if the security of a TMN is too lax. This suggests that the objectives for security of a TMN should indicate a fairly high level of security. However, different providers may put different weight on such arguments, which means that initially the level of security of different TMN systems may vary. In order to reach a uniform protection level across the co-operating TMNs, MoUs, as discussed in the previous section, can be a useful tool.

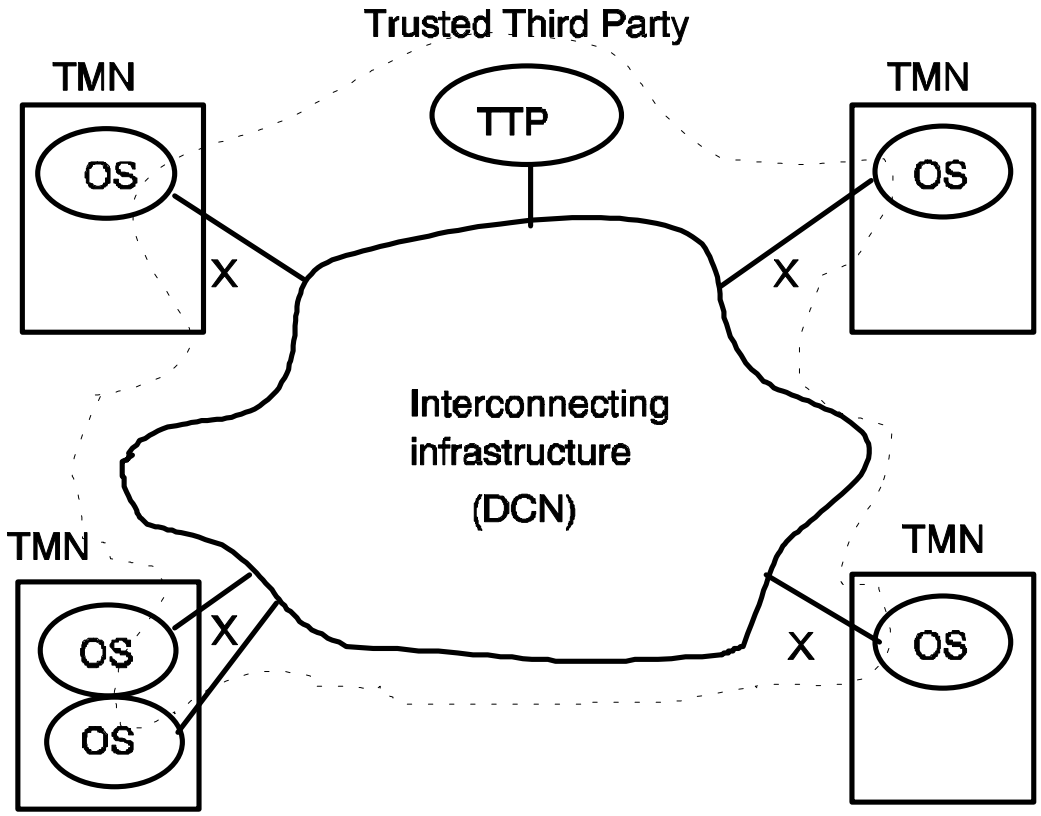
System Description

In the context of TRUMPET, the “system” consists of the following:

- a collection of providers’ TMNs, operating as independent management and security domains, and interconnected by Xcoop interfaces;

- TMNs of customers (each actor is assumed to have at least some rudimentary TMN functionality available), usually connected to the TMN of one provider per customer by Xuser interfaces, since the customers will normally use one-stop-shopping services.

The number of different providers may be substantial, and in principle every provider should be able to access the TMNs of all other providers, following the ONP principles. Thus, full connectivity between the TMNs is necessary. This can be accomplished by any kind of network capable of delivering communication services with the desired QoS. Logically speaking these network connections will constitute a DCN (Data Communications Network) in TMN terminology. This structure is shown in the figure below.



The figure shows only the Xcoop interfaces, depicted as open service offerings on the DCN network, accessible to in principle any other provider. Access to all but very limited information will of course be restricted by authorisation by the TMNs' owners. Authorisation to relevant and necessary management information will be granted to providers which are accepted as customers with respect to services. Authorisation will be to certain managed object classes and instances, and certain management operations, that is to a particular SMK (Shared Management Knowledge) between the providers.

With a large number of providers, possibly with a limited direct trust between them, TTPs (Trusted Third Party) may be needed in order to set up secure relationships between TMNs, and for various other services. Further details on the use of TTPs in this context may be found in [CFS-H211, MAILLOT-95-2].

In addition to this description of the relationships between providers, the architecture (including TMN functional, information and physical architectures) and functions of the system need to be described, including the following properties:

- functional description of each system component and its interface(s);
- identify the information's storage characteristics: the kind of information, where it is stored, whether it is permanent or temporary, and its importance/sensitivity to the correct functioning (integrity) of the system, to the privacy requirements of the system's subscribers and users, and to business sensitivity (competitive information);
- the sequence and meaning of the information flows between the system components;
- identify the borders of responsibilities with respect to system management and service provision (the domain boundaries);

- identify all assets/resources inside a domain in need of protection;

- identify all actors and their roles, and their access rights to functions and information in the system (the access policy);

- provide some insight into how the system will be realised physically;

- any evolutionary aspects of the system that may affect the choice of security solutions.

Risk Analysis

There are a lot of threats to the security of a management system. Each threat has a probability (with high uncertainty in most cases) of occurance, and the damage a threat will cause if it occurs may be estimated (also usually with a high uncertainty). Based on a risk analysis - threats, vulnerabilities and impacts - a decision must be taken to counteract threats to the effect of guaranteeing adequate security. A discussion on threats to TMN security may be found in [CFS-H210], while Deliverable 2 from TRUMPET [DEL-2] has risk analysis as one of its main topics.

The risk may be viewed as the sum of the intra-domain risks, within the domains of each provider, and an inter-domain risk, which results from the interconnection of the management systems. In principle, ONP allows a provider to deny interconnection from a particular counterpart, if the risk implied by the connection is unacceptable (ONP essential requirements). However, the intention is that this paragraph of ONP shall be used as rarely as possible.

Note that the introduction of security countermeasures introduces new risks, which have to be encountered. As one example, secure use of cryptographic countermeasures depends on proper key management and protection of the keys used.

Security and Privacy Requirements

The security policy of a TMN system shall, to the degree determined by the organisation's security objectives, fulfil the following purposes:

- **accountability -** legitimate users (human users or entities acting on their behalf or on behalf of external systems) shall be accountable for the utilisation of any management services;

- **integrity -** the system shall behave in the expected way; i.e. each system component must function properly and the information stored within or exchanged between the system components must be correct;

- **confidentiality -** information exchanged between TMN entities shall be kept confidential when needed and access to stored information shall be controlled and limited to those with legitimate rights to that information;

- **availability -** TMN functions and information shall be available to authorised users when needed;

- **security violations** of the system shall be detected and reported;

- **limitation of damaging effects** of security violations;

- **recovery of the security state** conforming with the security policy.

The inter-TMN security policies shall be applied to the interfaces between TMN systems, which means that a lot of these purposes are outside of the scope. Specifically, an X-interface provides communication, while stoage and processing is internal to the individual TMNs.

[CFS-H211] contains a rather detailed study of requirements for inter-TMN security, determined by an analysis of the management operations performed, and the management information transferred, over X-interfaces. Operations and information may be classified according to management functional areas (accounting, security, performance, ...). For a particular management operation, security requirements are expressed in terms of the operation's need for high/low/medium/none security in the areas:

- availability - to authorised initiators when needed;
- integrity - the correctness of the information transferred;
- confidentiality - against inspection by outside parties;
- accountability - the ability to produce proof of the identity of the party responsible for certain events.

There are strong availability requirements, but these are not treated by TRUMPET at present. Most availability mechanisms are not security mechanisms per se, but protection against denial of service attacks etc. should be considered.

The study clearly indicates that data integrity is the most important security service. This must necessarily include proper access control to stored data, which places requirements on the nature of the access control information conveyed over the X-interface. Since all security relies on proper authentication of the entities involved, peer-entity authentication is necessary, and strong authentication mechanisms are preferred. Note that customers and end-users shall not be identified or authenticated over X-interfaces. [CFS-H211] cites several reasons for this decision, one of them is the privacy of these actors. Cryptographic integrity protection of information transferred over the X-interfaces is usually a requirement. Confidentiality is seldom a strong requirement, but is sometimes necessary for business or privacy reasons. Accountability can in most cases be accomplished by simple audit trails[6], although stronger mechanisms are needed in some cases.

Different kinds of information and management operations may to a large extent be grouped into a few classes requiring approximately the same level of protection. This points at the definition of security functionality classes, as suggested in the next section.

Security Functionality Classes

Security functionality classes are consistent sets or groupings of security services, suitable to meet requirements of varying severity. The goals of such security functionality classes are:

[6] This cannot really be called a non-repudiation service in security terms, but under most jurisdictions even a cleartext log will be regarded as a (possibly weak) evidence.

- facilitate agreements between interacting management domains by identifying consistent sets of measures, that may be referred to for example in MoUs and in inter-domain security policies;

- to give manufacturers and vendors indications for designing the security features of their management products, in order to meet the requirements of the sector, and to ease their evaluation and certification by the providers.

A security functionality class may be implemented in variuos ways, dependent on the selection of security mechanisms for the services specified. Such selections will be specified for the security policies devised by TRUMPET.

According to the security requirements for the X interface of a service management system, three levels of security functionality classes are proposed:

- minimal functionality class, stressing the correctness of stored data and a minimal accountability for all management activities;

- basic functionality class, stressing the protection of transferred data against disclosure, modification, insertion or deletion, and requiring strong authentication of the initiator (managing) entity;

- advanced functionality class, for areas such as accounting and security management, where authentication and accountability have to be stressed, confidentiality of transfers is needed, as well as high availability;

Minimal FC	**Basic FC**	**Advanced FC**
Emphasis on the integrity of stored managed resources	Plus integrity and confidentiality of transferred data	Plus strong availability, and strong accountability of management operations
Managing entity simple authentication Management association access control Managed resources access control Data origin authentication Security alarm, audit and recovery	Managing entity strong authentication Management association access control Managed resources access control Data origin authentication Security alarm, audit and recovery Data integrity Connection integrity Data confidentiality Connection confidentiality . Security alarm, audit and recovery	Management entities strong mutual authentication Management association access control Management notification access control Managed resources access control Data origin authentication Security alarm, audit and recovery Data integrity Connection integrity Data confidentiality Connection confidentiality Detection of denial of service Origin non repudiation Destination non repudiation Security alarm, audit and recovery

Security Countermeasures and Security Sub-Profiles

By security countermeasures one generally understands both the security services and the specific security mechanisms able to realise those security services. In general, neither the services nor the mechanisms have to be standard, provided they ensure the desired security.

However, in the context of standardised open management systems, security functionality classes should be realised as far as possible by a selection of standardised security services and mechanisms, and through security parts of international standards. Such a selection amounts to a standards profile. Since this security profile will be part of a profile for the X-interfaces, the term “sub-profile” is used here [ITAEGV-92].

Measures for high security may be costly. However, selection between alternatives (even a few ones) may also be complicated, and thus costly. This suggests the following approach:

- cheap security measures are applied by default in all cases, for example bulk encryption of all data on a link when hardware is available;
- whenever alternatives are needed, their number must be small;
- alternatives must be clearly identifiable, to allow negotiation.

A small number of alternatives also increases the chances that the security sub-profiles will be implemented by vendors, and the chances that service management systems will share common profiles that can be agreed upon.

A common profile can be negotiated at association establishment time, and be valid for the entire duration of the association. A sub-profile corresponding to the highest level of security needed must be chosen. For re-negotiation, one must normally release and establish a new association.

Real security sub-profiles will be comprehensive and consistent sets of standard security mechanisms providing given security services, together with all their parameters, such as the identification of algorithms and their modes of operation. Because few standards exist for security mechanisms and their use by base standards such as CMIP, sub-profiles based only on standards cannot be specified in detail at this stage. The following constraints should be noted:

- lack of appropriate standards, which may lead to selection of de-facto or even non-standard alternatives;
- implementation constraints, for example caused by availability of products, or their effectiveness for real-time applications like management;
- constraints imposed by existing management systems and their security policies, for example:
    - interfacing to non-TMN systems, possibly through QAF-functions, and especially SNMP-based management systems;
    - complexity of mapping between internal and external policies.

Cost/Benefit Evaluation and Risk Acceptance

Security countermeasures should be introduced following a cost / benefit analysis, where the costs implied by the countermeasures must be justified by the estimated costs of the incidents they protect against. Estimating the costs is relatively straightforward. Suggested cost factors are [CFS-H211]:

- hardware and software costs - purchasing or development of the countermeasure itself;
- installation and maintenance costs of hardware and software;
- overhead - in terms of reduced performance of equipment, possibly cumbersome (but more secure) work procedures etc.;
- management costs.

Maintenance and management include costs for the staff managing the services, training of the staff, and costs for the resources (file systems, databases, licenses, extra equipment etc.) required to support the security countermeasure. This will frequently outweigh the other cost factors.

In most cases, the benefit of a security countermeasure is the expenses avoided[7] due to the extra protection against incidents. In this respect, security countermeasures can be likened to an insurance, which costs money, but saves more money if something happens. The costs of the countermeasures must be justified by the benefits, just like the insurance rates.

In addition to these overall cost/benefit considerations, [CFS-H211] suggests benefit factors per countermeasure as follows:

- applicability - to the security problem at hand, for example “strong mutual authentication”;
- reliability - with respect to strength, completeness, ease of use etc.;
- availability - of products and technology;
- standardisation - of the security countermeasure;
- usefulness for other services - general purpose or specialised countermeasures.

After application of the security countermeasures, there will still be a remaining risk, which must be deemed acceptable. This risk is composed of:

- the risk of someone or something penetrating the security countermeasures;
- the risk of omissions and mistakes in the definition of the security policies;

---

[7] A purely economic analysis is not sufficient. For example, it is not possible to assign a monetary value to personal data. In addition, laws and regulations must be obeyed, even if they imply countermeasures that are not justified by a cost/benefit analysis.

- the risk of underestimating the importance of certain threats with respect to vulnerability and/or impact.

If the remaining risk is unacceptable, or the costs are too high, the objectives and requirements may have to be re-examined in order to come up with an acceptable solution.

Inter-TMN Security Policies

An inter-TMN security policy is a specification for a realisation of one of the selected security functionality classes, by means of a selection of security services and mechanisms, plus additional specifications for administrative and physical security if appropriate.

It is also necessary to specify how the security services and mechanisms are to be integrated with management services and protocols like CMIS/CMIP. Several alternative policies may support one security functionality class, but the intention is to make a selection, and define one policy per functionality class.

The security services, and example mechanisms, are:

- peer-entity authentication, preferably by cryptographic mechanisms - note that human user authentication is outside of the scope of the policies, since this is done inside the individual domains;

- access control, where mechanisms may be based on identity, capabilities, labels or context, and access control atttributes may be transferred in the form of PACs (Privilege Attribute Certificate);

- integrity, which should be realised by cryptographic means for transfer of data on X-interfaces (plus access control to stored data);

- confidentiality, likewise relised by cryptographic means, plus acces control;

- non-repudiation, in the simplest case by ordinary logs and audit trails, by use of digital signatures, and/or TTPs (Trusted Third Party);

- audit, realised by logging and alarms to detect and prove breaches in security.

With respect to management services and protocols, services and mechanisms may be realised at different layers:

- lower layers of the ISO model, notably the Network or Transport layers, and notably to implement transparent integrity and confidentiality protection[8] between front-end computers (like a router, or a firewall);

- general functionality in the Application and Presentation layers of the ISO model, following the GULS (Generic Upper Layer Security) standards [ISO11586];

[8] EURESCOM project P408 uses this approach to integrity and confidentiality.

- in the management ASEs (Application Service Element), for example access control according to ISO 10164-9 [ISO10164-9] and logging and alarms according to ISO 10164-7 [ISO10164-7] and ISO 10164-8 [ISO10164-8];

- in the management applications, outside the OSI environment, for example deposit of evidence at a notary TTP for non-repudiation purposes.

Not all services may be realised at all layers, and a combination of security services at different layers is likely.

In addition to services and mechanisms, algorithms have to be specified, in particular for cryptographic countermeasures. It is anticipated that an asymmetric algorithm (like RSA) will be used for authentication, key management, digital signatures etc., while a symmetric algorithm will be used for bulk protection for data integrity and confidentiality. ETSI is developing a symmetric algorithm specifically for use in pan-European management [ETSI-STAG-5].

The exact solutions recommended by TRUMPET are not yet determined, but a first version of the security policies will be presented in [DEL-2] by end of June 1996.

Conclusion

Interactions between management domains will proceed over well-defined TMN X-interfaces (Xuser and Xcoop). The aim of the security policy activity in TRUMPET is to contribute to making these X-interfaces well-secured as well. Security should be realised by standardised security policies, defined as security sub-profiles of management standards profiles, and agreed by the authorities of the TMNs engaged in the inter-TMN activities. TRUMPET will define a set of such policies, applicable to security requirements of varying severity. Later in the project, the policies (or at least some of them) will be implemented and tested in real-life trials.

References

[CFS-H210] RACE CFS H210: “TMN Security Architecture”, CFS Issue F, August 1995.

[CFS-H211] RACE CFS H211: “Security of Service Management”, CFS Issue F, August 1995.

[DEL-2] D.Maillot (editor): “Security Policies for Inter-TMN Management”, Deliverable 2 of ACTS project AC112 TRUMPET, June 1996 (forthcoming).

[ETSI-NA002501] ETSI/STAG: “Security Requirements Capture”, ETSI TCRTR/NA-002501, 1995.

[ETSI-NA043208] ETSI STC NA4 Rapp. Gr.: “Introduction to Standardising Security for TMN”, ETSI DTR/NA-043208, 1996.

[ETSI-STAG-5] ETSI/STAG: “Requirements Specification for an Encryption Algorithm for Operators of European Public Telecommunications Networks”, ETSI TC-TR NA/STAG 5 (93) 123 rev. 4, November 1993.

[ISO10164-7] ISO 10164-7: “Systems Management - Part 7: Security Alarm Reporting Function”, 1993.

[ISO10164-8] ISO 10164-8: “Systems Management - Part 8: Security Audit Trail Function”, 1993.

[ISO10164-8] ISO 10164-9: “Systems Management - Part 9: Objects and Attributes for Access Control”, 1995.

[ISO10181-1] ISO DIS 10181-1: “Security Frameworks Overview”, 1995.

[ISO11586] ISO 11586: “Generic Upper Layers Security - Parts 1-4”, 1994.

[ITAEGV-92] CEN/CENELEC/ ITAEGV: “Security Sub-Profiles, Functionality Classes and Security Targets”, draft version 4.0, June 1992.

[M3010] ITU-T SG IV: “ Principles for a Telecommunications Management Network”, ITU Recommendation M.3010, <time of latest issue>.

[MAILLOT-95-1] D.Maillot, J.Ølnes, P.Spilling: “The New Eoropean Regulatory Environment for Telecommunications - Implications for Service Management and Its Security”, Proceedings of the IEEE Conference of Communications, Seattle, June 1995.

[MAILLOT-95-2] D.Maillot, J.Ølnes, P.Spilling: “A TTP-based Architecture for TMN Security and Privacy”, Proceedings of the IS&N’95 Conference (Springer Verlag, Lecture Notes in Computer Science no. 998), Heraklion, Greece, October 1995.

[ONP] CEC: “On the Establishment of the Internal Market for Telecommunications Services through the Implementation of Open Network Provision (ONP Directive)”, Council Directive DIR(90) 388 ECC, 1990.