INTERNATIONAL STANDARD

ISO/IEC 18028-2

First edition
2006-02-01

Information technology — Security techniques — IT network security —

Part 2: Network security architecture

Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI —

Partie 2: Architecture de sécurité de réseau

Reference number
ISO/IEC 18028-2:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*, in collaboration with ITU-T. This part of ISO/IEC 18028 is technically aligned with ITU Rec. X.805 but is not published as identical text.

ISO/IEC 18028 consists of the following parts, under the general title *Information technology — Security techniques – IT network security*:

— *Part 1: Network security management*

— *Part 2: Network security architecture*

— *Part 3: Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

— *Part 5: Securing communications across networks using Virtual Private Networks*

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. Thus, the purpose of ISO/IEC 18028 is to provide detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in ISO/IEC 18028 to meet their specific requirements. Its main objectives are as follows:

- in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyse the communications related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);
- in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;
- in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;
- in ISO/IEC 18028-4, to define techniques for securing remote access;
- in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPN).

ISO/IEC 18028-1 is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for Information Security (IS) and/or network security, network operation, or who are responsible for an organization's overall security programme and security policy development.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example IT network managers, administrators, engineers and IT network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).

Information technology — Security techniques — IT network security —

Part 2:
Network security architecture

1 Scope

This part of ISO/IEC 18028 defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where end-to-end security is a concern and independently of the network's underlying technology. The objective of this part of ISO/IEC 18028 is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

CCITT Recommendation X.800 (1991), *Security architecture for Open Systems — Interconnection for CCITT applications*

3 Terms and definitions

For the purposes of this document, the following terms defined in ISO 7498-2:1989 | CCIT Rec. X.800 apply.

3.1
access control
prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

3.2
data origin authentication
corroboration that the source of data received is as claimed

3.3
peer-entity authentication
corroboration that a peer entity in an association is the one claimed

3.4
availability
property of being accessible and useable upon demand by an authorized entity

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.7
non-repudiation with proof of origin
security service in which the recipient of data is provided with proof of the origin of data

NOTE 1 This will protect against any attempt by the sender to falsely deny sending the data or its contents.

NOTE 2 Adapted from ISO 7498-2 | CCIT Rec. X.800.

3.8
non-repudiation with proof of delivery
security service in which the sender of data is provided with proof of delivery of data

NOTE 1 This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

NOTE 2 Adapted from ISO 7498-2 | CCIT Rec. X.800.

3.9
privacy
right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

4 Abbreviations

ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DS-3	Digital Signal level 3
IPsec	IP Security protocol
MD5	Message Digest Version 5
OAM&P	Operations Administration Maintenance and Provisioning
OSI	Open Systems Interconnection
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
SHA-1	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network

SS7 Signalling System #7

SSL Secure Socket Layer (encryption and authentication protocol)

TLS Transport Layer Security (encryption and authentication protocol)

VLAN Virtual Local Area Network

5 Reference Architecture for network security

The Reference Architecture was created to address the global security challenges of Service Providers, enterprises, and consumers and is applicable to wireless, optical and wire-line voice, data and converged networks. In context of this document the word “reference” in conjuncture with the word “architecture” is used to convey that the specification presents an example of high-level security architecture that could serve as a base for designing more detailed security solutions for various networks. This Reference Architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. The Reference Architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to predict, detect, and correct security vulnerabilities.

The Reference Architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The Reference Architecture addresses the network security needs covering following essential questions:

1. What kind of information needs to be protected?
2. What are the security risks, and what kind of protection is needed to manage these risks?
3. What are the distinct types of network activities that need to be protected?
4. What are the distinct types of network equipment and facility groupings that need to be protected?

A risk assessment should be conducted to prioritize the protection requirements and help to determine the appropriate security measures for security architecture.

These questions are addressed by three architectural components – Security Dimensions, Security Planes and Security Layers.

The principles described by the multifaceted Reference Architecture can be applied to a wide variety of networks independent of the network's technology or location in the protocol stack.

The following sections describe in detail the architectural elements and their functions with respect to the major security threats.

6 Security Dimensions

Typically within a risk management process, appropriate security measures are identified to manage or mitigate assessed risks. The security dimensions introduce a grouping of security measures that are used to implement particular aspects of network security. The concept of security dimensions is not limited to networks, but is also usable in the context of application or end-user information. In addition, the Security Dimensions apply to Service Providers or enterprises offering security services to their customers. The Security Dimensions are: (1) Access Control, (2) Authentication, (3) Non-repudiation, (4) Data Confidentiality, (5) Communication Flow Security, (6) Data Integrity, (7) Availability, and (8) Privacy.

Properly designed and implemented Security Dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management.

6.1 Access Control Security Dimension

The Access Control Security Dimension provides authorization for the use of the network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows for which they are authorized.

6.2 Authentication Security Dimension

The Authentication Security Dimension serves to confirm the identities or other authorizing attributes of communicating entities. Authentication ensures the validity of the claimed identities when used by authorization or Access Control of the entities participating in communication (e.g. person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. Authentication methods that employ techniques based on user identification and password pair, two-factor authentication (e.g. token), biometrics are among widely used methods.

6.3 Non-repudiation Security Dimension

The Non-repudiation Security Dimension provides technical means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It helps to ensure the availability of evidence that can be presented to a third party as technical proof that some kind of event or action has taken place. Note, however, that non-repudiation provided by technical means does not lead to a necessary conclusion of law. Cryptographic methods are often used for providing non-repudiation.

6.4 Data Confidentiality Security Dimension

The Data Confidentiality Security Dimension protects data from unauthorized disclosure. Encryption is a method often used to ensure data confidentiality. Access control lists, and file permissions are methods that help to keep data confidential.

6.5 Communication Flow Security Dimension

The Communication Flow Security Dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). Security mechanisms of Communication Flow Security Dimension do not protect against modification/corruption; this is a function of Data Integrity. MPLS tunnels, VLANs, and VPNs are examples of technologies that can provide communication flow security.

6.6 Data Integrity Security Dimension

The Data Integrity Security Dimension ensures the correctness or accuracy (i.e., data are only processed by authorized processes or actions of authorized people or devices) of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. Hashed Message Authentication Code methods (e.g. MD5, SHA-1) often used for ensuring data integrity.

6.7 Availability Security Dimension

The Availability Security Dimension ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

6.8 Privacy Security Dimension

The Privacy Security Dimension provides for the protection of any information (identity of a party to communications or any data – including packet headers – pertaining to any activity carried by this party) that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a Service Provider network. Network Address Translation (NAT) and application proxies are examples of the techniques that can be used for privacy protection. Depending on the respective national privacy and data protection legislations and regulations, this Privacy Security Dimension should also provide the appropriate protection structure and controls for collection, processing and dissemination of personal information.

7 Security Layers

In order to provide an end-to-end security solution, the Security Dimensions described in the previous section must be applied to a hierarchy of network equipment and facility groupings, which are referred to as Security Layers. This Reference Architecture defines three Security Layers – the Infrastructure Security Layer, the Services Security Layer, and the Applications Security Layer, which build on one another to provide network-based solutions.

The Security Layers are a series of enablers for secure network solutions: the Infrastructure Security Layer enables the Services Security Layer and the Services Security Layer enables the Applications Security Layer. The Reference Architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular security layer. The decision of whether the higher levels must assume that lower level security has functioned as intended or whether they should contain processes to detect failures is left to implementations.

It should be noted that Security Layers (as defined above) have different than the OSI layers meaning.

The Security Layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the Infrastructure Security Layer, then – for the Services Security Layer, and finally security vulnerabilities are addressed for the Applications Security Layer. Security Dimensions identify areas that need to be addressed in each Security Layer. Figure 1 depicts how the mechanisms within each Security Dimension are applied to Security Layers in order to diminish vulnerabilities that exist at each layer and thus mitigate security attacks.

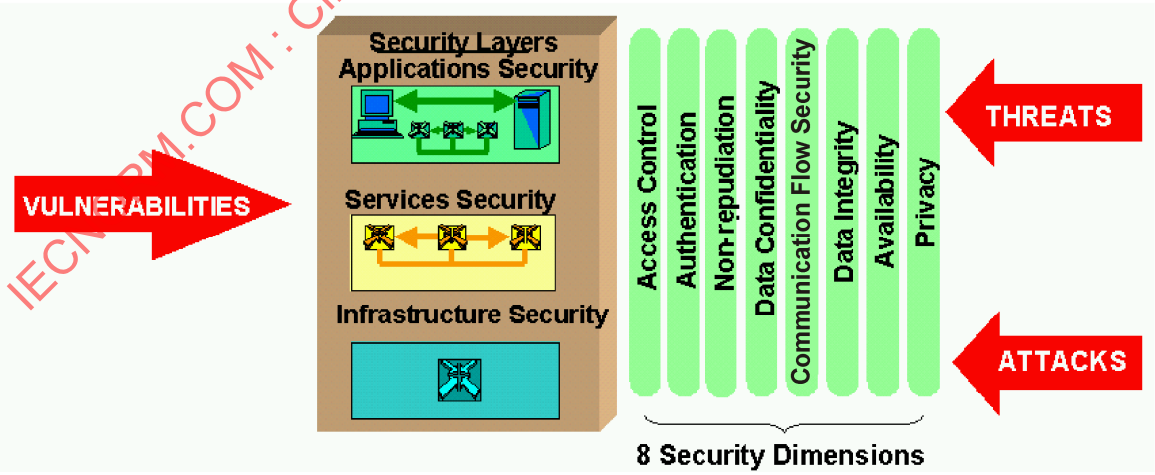

Figure 1 — Applying Security Dimensions to Security Layers

7.1 The Infrastructure Security Layer

The Infrastructure Security Layer consists of the network transmission facilities as well as individual network elements protected by the mechanisms that are implemented for the Security Dimensions. The Infrastructure Security Layer represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to the Infrastructure Security Layer are individual routers, switches and servers as well as the communication links between individual routers, switches and servers.

7.2 The Services Security Layer

The Services Security Layer addresses security of services that Service Providers provide to their customers. These services range from basic transport and connectivity to service enablers like those that are necessary for providing Internet access (e.g. authentication, authorization, and accounting services, dynamic host configuration services, domain name services, etc.) to value-added services such as freephone service, QoS, VPN, Location Services, Instant Messaging, etc. The Services Security Layer is used to protect the Service Providers and their customers, both of which are potential targets of security threats. For example, the attackers may attempt to deny the Service Provider's ability to offer the services, or they may attempt to disrupt service for an individual customer of the Service Provider (e.g., a corporation).

7.3 The Applications Security Layer

The Applications Security Layer focuses on security of the network-based applications accessed by Service Provider customers. These applications are enabled by network services and include basic file transport (e.g., FTP) and web browsing applications, fundamental applications such as directory assistance, network-based voice messaging, and email, as well as high-end applications such as customer relationship management, electronic/mobile-commerce, network-based training, video collaboration, etc. Network-based applications may be provided by third-party Application Service Providers (ASPs), Service Providers acting also as ASPs, or by enterprises hosting them in their own (or leased) data centers. At this layer there are four potential targets for security attacks: the application user, the application provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the Service Provider.

8 Security Planes

A Security Plane is a certain type of network activity protected by the mechanisms that are implemented for the Security Dimensions. This Reference Architecture defines three Security Planes to represent the three types of protected activities that take place on a network. The Security Planes are: (1) the Management Security Plane, (2) the Control Security Plane, and (3) the End-User Security Plane. These Security Planes address specific security needs associated with network management activities, network control or signalling activities, and end-user activities correspondingly.

Networks should be designed in such a way that events on one Security Plane are kept as much as possible and as appropriate isolated from the other Security Planes. For example, a flood of DNS lookups on the End-User Security Plane, initiated by end-user requests, should not lock out the OAM&P interface in the Management Security Plane that would allow an administrator to correct the problem.

Figure 2 illustrates the Reference Architecture with the Security Planes included. Each type of the described network activities has its own specific security needs. The concept of Security Planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently. Consider, for example, a VoIP Service, which is addressed by the Services Security layer. Securing the management of the VoIP service (e.g., provisioning users) has to be independent of securing the control of the service (e.g., protocols such as SIP) and also has to be independent of securing the end-user data being transported by the service (e.g., the user's voice).

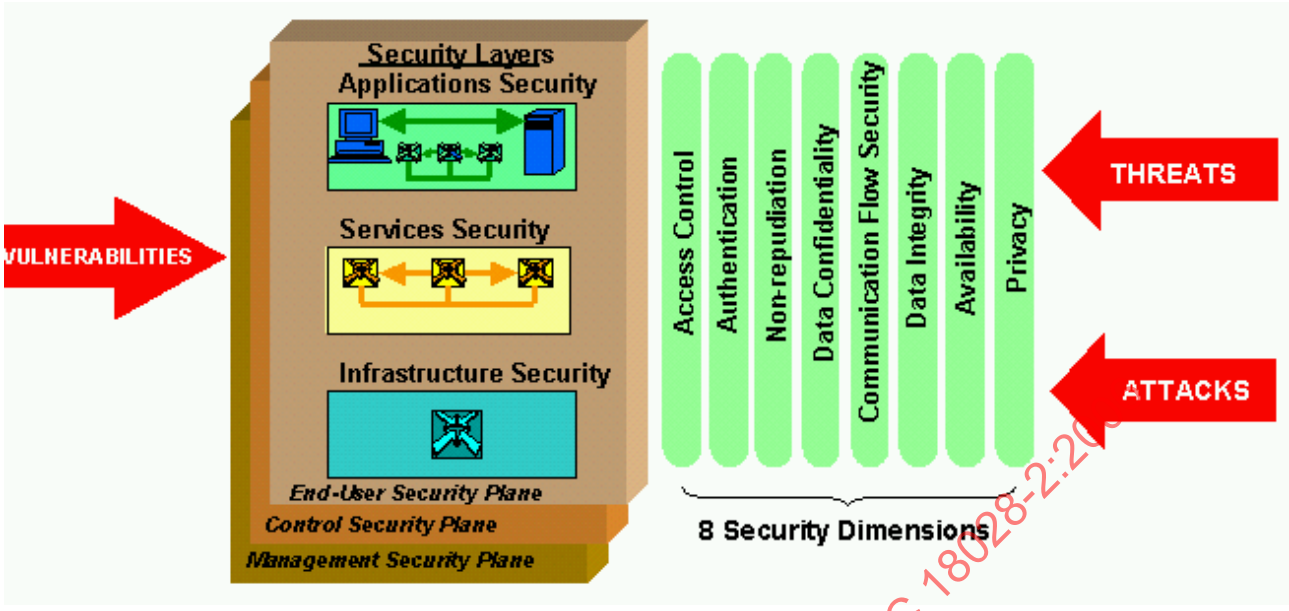

Figure 2 — Security Planes Reflect the Different Types of Network Activities

8.1 The Management Security Plane

The Management Security Plane is concerned with the protection of OAM&P functions of the network elements, transmission facilities, back-office systems (Operations Support Systems, Business Support Systems, Customer Care Systems, etc.), and Data Centers. The Management Security Plane supports the Fault, Capacity, Administration, Provisioning, and Security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the Service Provider's user traffic.

8.2 The Control Security Plane

The Control Security Plane is concerned with protection of the activities that enable the efficient delivery of information, services and applications across the network. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine- how to best route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control or signaling information. The network carrying these types of messages may be in-band or out-of-band with respect to the Service Provider's user traffic. For example, IP networks carry their control information in-band; whereas, the PSTN carries its control information in a separate out-of-band signaling network (the SS7 network). Example traffic of this type includes routing protocols, DNS, SIP, SS7, Megaco/H.248, etc.

8.3 The End-User Security Plane

The End-User Security Plane addresses security of access and use of the Service Provider's network by customers. This plane is also concerned with the protection of the actual end-user data flows. End-users may use a network that only provides connectivity, they may use it for value-added services such as VPNs, or they may use it to access network-based applications.

9 Security threats

The Reference Architecture defines a plan and set of principles that describe a security structure for the end-to-end security solution. The architecture identifies security issues that need to be addressed in order to prevent both intentional threats as well as accidental threats. The following threats are described in ISO 7498-2:1989 | CCIT Rec. X.800 (1991):

- destruction of information and/or other resources,
- corruption or modification of information,
- theft, removal or loss of information and/or other resources,
- disclosure of information,
- interruption of services.

The intersection of each Security Layer with each Security Plane represents a security perspective where Security Dimensions are applied to counteract the threats. Table 1 provides a mapping of Security Dimensions to the security threats. The mapping is the same for each security perspective.

The letter "Y" in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding Security Dimension.

Table 1 — Mapping Security Dimensions to security threats

Security Dimension	Security Threat				
	Destruction of Information or Other Resources	Corruption or Modification of Information	Theft, Removal or Loss of Information and Other Resources	Disclosure of Information	Interruption of Services
Access Control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data Confidentiality			Y	Y	
Communication Flow Security			Y	Y	
Data Integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Figure 3 illustrates the Reference Architecture with the architectural elements shown and indicates the security threats described above. The figure depicts the concept of protecting a network by Security Dimensions at each Security Plane of each Security Layer in order to provide a comprehensive security solution. It should be noted that, depending on a given network's security requirements, it might not be necessary to have all architectural elements implemented (that is to have a complete set of the Security Dimensions, Security Layers and Security Planes).

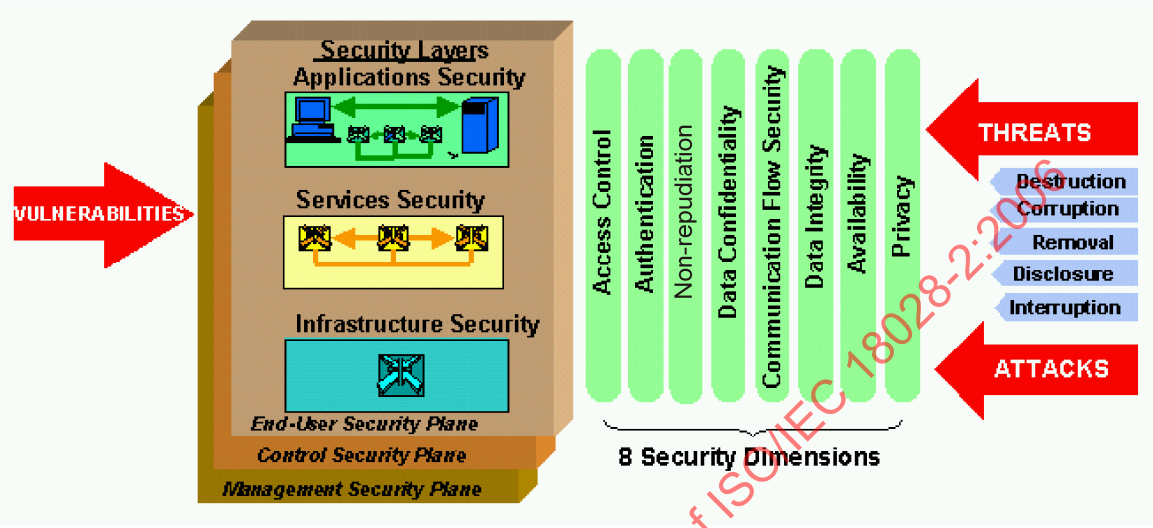

Figure 3 — Reference Architecture for End-to-End Network Security

10 Description of the objectives achieved by application of Security Dimensions to Security Layers

The Reference Architecture can be applied to all aspects and phases of a Security Program as depicted in Figure 4. As can be seen from Figure 4, a Security Program consists of policies and procedures in addition to technology, and progresses through three phases over the course of its lifetime: (1) the Definition and Planning phase, (2) the Implementation phase, and (3) the Maintenance phase. The Reference Architecture along with the guidelines of ISO/IEC 13335 can be applied to security policies and procedures, as well as technology, across all three phases of a Security Program.

Based on business requirements, the network architecture, policy definitions, incident response and recovery plans are determined. In this process the Reference Architecture can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each Security Dimension at each Security Layer and Plane during the definition and planning phase. The Reference Architecture can also be used as the basis of a security assessment that would examine how the implementation of the Security Program addresses the Security Dimensions, Layers and Planes as policies and procedures are rolled out and technology is deployed. Once a Security Program has been deployed it must be maintained in order to keep current in the ever-changing security environment. The Reference Architecture can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the Security Program address each Security Dimension at each Security Layer and Plane.

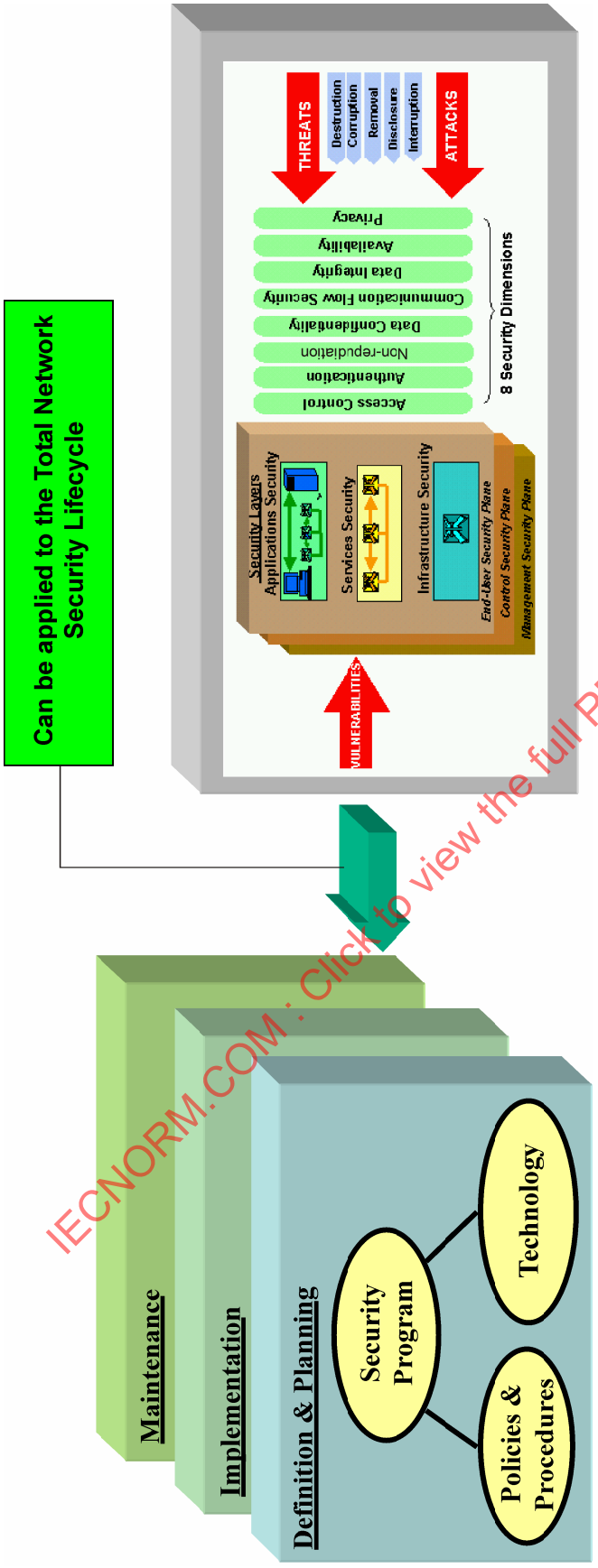

Figure 4 — Applying the Reference Security Architecture to Security Programs

In addition, the Reference Architecture can be applied to any type of network at any level of the protocol stack. For example, in an IP network, which resides at layer three of the protocol stack, the Infrastructure Security Layer refers to the individual routers, the point-to-point communications links between the routers (e.g., SONET, ATM PVCs, etc.), and server platforms used to provide the support services required by an IP network. The Services Security Layer refers to the basic IP service itself (e.g., Internet connectivity), the IP support services (e.g., AAA, DNS, DHCP, etc.), and advanced value-added services offered by the Service Provider (e.g., VoIP, QoS, VPN, etc.). Finally the Applications Security Layer refers to the security of user applications that are to be accessed via the IP network (such as email, etc.).

Likewise, for an ATM network, which resides at layer two of the protocol stack, the Infrastructure Security Layer refers to the individual switches, and the point-to-point communications links between the switches (carrier facilities, for example DS-3). The Services Security Layer refers to the different classes of transport provided by an ATM service offering (Constant Bit Rate, Variable Bit Rate – Real Time, Variable Bit Rate – non-Real Time, Available Bit Rate, and Unspecified Bit Rate). Finally, the Applications Security Layer refers to the applications the end-user is using the ATM network to access, such as a video conferencing application.

Figure 5 presents the Reference Architecture in a tabular form and illustrates a methodical approach to securing a network. As can be seen from the figure, the intersection of a Security Layer with a Security Plane represents a unique perspective for consideration of the eight Security Dimensions. Each of the nine modules combines the eight Security Dimensions that are applied to a particular Security Layer at a particular Security Plane. It should be noted that the Security Dimensions of different modules may have different objectives and, consequently, may comprise different sets of security measures. The tabular form gives a convenient way of describing the objectives of the Security Dimensions for each module.

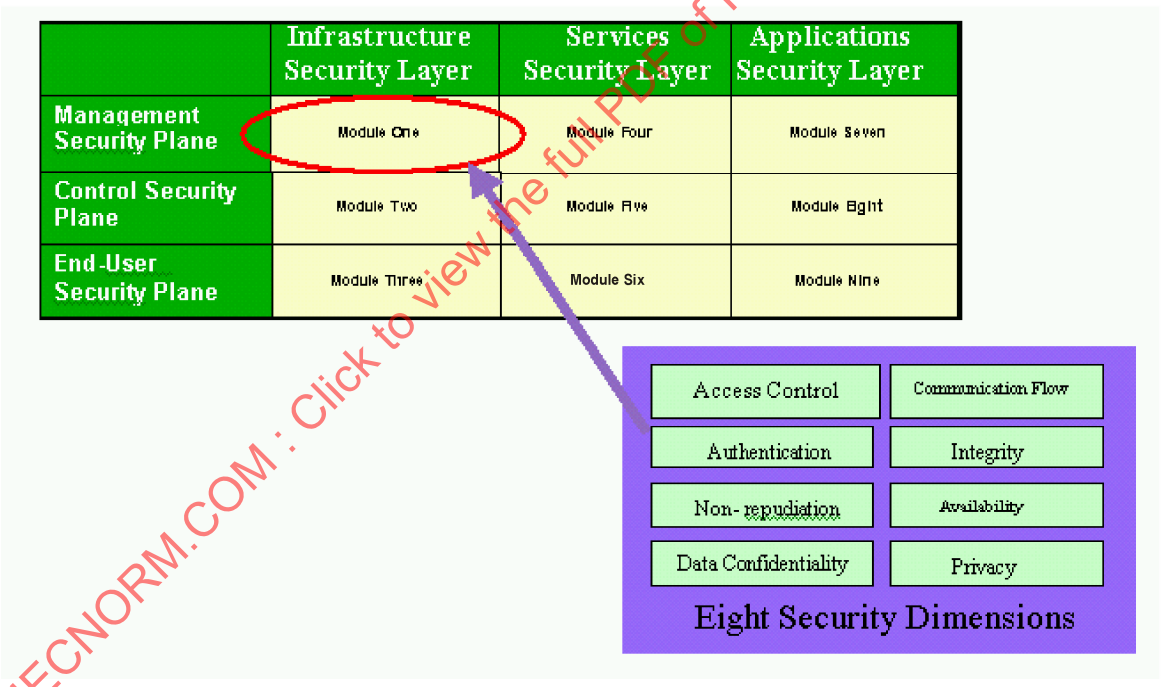

Figure 5 — Reference Architecture in a tabular form

It should be noted that the concept of protection used in the tables below encompasses creating the mechanisms to detect where control mechanisms fail and to ensure that either the event is reported for action and/or the devices/processes in place rectify any consequences of such failure.

10.1 Infrastructure Security Layer

Securing the Management Security Plane of the Infrastructure Security Layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) as well as configuration of the individual network elements, communication links, and server platforms that comprise the network. An example of infrastructure management that needs to be secured is the configuration of an individual router or switch by

network operations personnel. Table 2 describes the objectives of applying the Security Dimensions to the Infrastructure Security Layer, Management Security Plane.

Table 2 — Applying Security Dimensions to the Infrastructure Security Layer, Management Security Plane

Module 1: Infrastructure Security Layer, Management Security Plane	
Security Dimension	**Security Objectives**
Access Control	Ensure that only authorized personnel or devices (e.g., in the case of SNMP managed devices) are allowed to perform or attempt to perform administrative or management activities on the network device or communications link. This applies to both direct management of the device via a craft port and remote management of the device.
Authentication	Verify the identity of the person or device performing the administrative or management activity on the network device or communications link. Authentication techniques may be required as part of Access Control.
Non-repudiation	Provide a record identifying the individual or device that performed each administrative or management activity on the network device or communications link and the action that was performed. This record can be used as proof of the originator of the administrative or management activity.
Data Confidentiality	Protect the network device or communications link configuration information from unauthorized access or viewing. This applies to configuration information resident in the network device or communications link, configuration information being transmitted to the network device or communications link as well as backup configuration information stored offline. Protect the administrative authentication information (e.g., administrator identifications and passwords) from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality.
Communication Flow Security	In the case of remote management of a network device or communications link, ensure that the management information only flows between the remote management stations and the devices or communication links that are being managed. The management information is not diverted or intercepted as it flows between these endpoints. The same type of consideration is applied to administrative authentication information (e.g., administrator identifications and passwords).
Data Integrity	Protect the configuration information of network devices and communications links against unauthorized modification. This protection applies to configuration information resident in the network device or communications link, as well as configuration information that is in transit or stored in offline systems. The same type of consideration is applied to administrative authentication information (e.g., administrator identifications and passwords).
Availability	Ensure that the ability to manage the network device or communications link by authorized personnel or devices cannot be denied. This includes protection against active attacks such as Denial of Service (DoS) attacks as well as protection against passive attacks such as the modification or deletion of the administrative authentication information (e.g., administrator identifications and passwords).
Privacy	Ensure that information that can be used to identify the network device or communications link is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network device provides targeting information to attackers. Ensure that personal information is collected, processed and disseminated through the network in accordance with local data protection legislation and regulation.

Securing the Control Security Plane of the Infrastructure Security Layer consists of securing the control or signaling information that resides in the network elements and server platforms that comprise the network as well as securing the receipt and transmission of control or signaling information by the network elements and server platforms. For example, the switching tables residing in network switches need to be protected from tampering or unauthorized disclosure. In another example, routers need to be protected from receiving and propagating bogus routing updates or responding to bogus routing requests originating from spoofed routers. Table 3 describes the objectives of applying the Security Dimensions to the Infrastructure Security Layer, Control Security Plane.

Table 3 — Applying Security Dimensions to the Infrastructure Security Layer, Control Security Plane

Module 2: Infrastructure Security Layer, Control Security Plane	
Security Dimension	**Security Objectives**
Access Control	Ensure that only authorized personnel and devices are allowed to access, or to attempt to access, control information resident in the network device (e.g., a routing table) or in offline storage. Ensure that the network device will only accept control information messages from authorized network devices (e.g., routing updates).
Authentication	Verify the identity of the person or device observing or modifying control information resident in the network device. Verify the identity of the device sending control information to the network device. Authentication techniques may be required as part of Access Control.
Non-repudiation	Provide a record identifying each individual or device that observed or modified control information in the network device and the action that was performed. This record can be used as proof of access to or modification of the control information. Provide a record identifying the device originating control messages sent to the network device and the action that was performed. This record can be used as proof that the device originated the control message.
Data Confidentiality	Protect control information resident in a network device or in offline storage from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for control information resident in the network device. Protect control information destined for a network device from unauthorized access or viewing as it is being transported across the network.
Communication Flow Security	Ensure that control information being transported across the network (e.g., routing updates) only flows between the source of the control information and its desired destination. The control information is not diverted or intercepted as it flows between these endpoints.
Data Integrity	Protect control information resident in network devices, in-transit across the network, or stored offline against unauthorized modification.
Availability	Ensure that network devices are always available to receive control information from authorized sources. This includes protection against deliberate attacks such as Denial of Service (DoS) attacks and accidental occurrences (e.g., route flapping).
Privacy	Ensure that information that can be used to identify the network device or communications link is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers. Ensure that personal information is collected, processed and disseminated through the network in accordance with local data protection legislation and regulation.

Securing the End-User Security Plane of the Infrastructure Security Layer consists of securing user data and voice as it resides in or is transported through network elements as well as while it is being transported across communications links. Protecting user data resident on server platforms is of concern here as well as protecting user data against unlawful interception as it is transported through network elements or across communication links. Table 4 describes the objectives of applying the Security Dimensions to the Infrastructure Security Layer, End-User Security Plane.

Table 4 — Applying Security Dimensions to the Infrastructure Security Layer, End-User Security Plane

Module 3: Infrastructure Security Layer, End-User Security Plane	
Security Dimension	**Security Objectives**
Access Control	Ensure that only authorized personnel or devices are allowed to access, or to attempt to access, end-user data that is transiting a network element or communications link or is resident on offline storage devices.
Authentication	Verify the identity of the person or device attempting to access end-user data that is transiting a network element or communications link or is resident on offline storage devices. Authentication techniques may be required as part of Access Control.
Non-repudiation	Provide a record identifying each individual or device that accessed end-user data that is transiting a network element or communications link or is resident on offline devices and the action that was performed. This record is to be used as proof of access to the end-user data.
Data Confidentiality	Protect end-user data that is transiting a network element or communications link or is resident on offline devices against unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for end-user data.
Communication Flow Security	Ensure end-user data that is transiting a network element or communications link is not diverted or intercepted as it flows between these endpoints without authorized access (e.g., legal wiretaps).
Data Integrity	Protect end-user data that is transiting a network element or communications link or is resident in offline devices against unauthorized modification.
Availability	Ensure that access to end-user data resident in devices by authorized personnel (including end-users) and devices cannot be denied. This includes protection against active attacks such as Denial of Service (DoS) attacks as well as protection against passive attacks such as the modification or deletion of authentication information (e.g., user identifications and passwords, administrator identifications and passwords).
Privacy	Ensure that network elements do not provide information pertaining to the end-user's network activities (e.g. user's geographic location, web sites visited, etc.) to unauthorized personnel or devices. Ensure that personal information is collected, processed and disseminated through the network in accordance with local data protection legislation and regulation.

10.2 Services Security Layer

Securing the Services Security Layer is complicated by the fact that services may build upon one another in order to satisfy customer requirements. For example, in order to provide a VoIP Service, a Service Provider must first provide basic IP Service, with its requisite enabling services such as AAA, DHCP, DNS, etc. The Service Provider may also need to deploy a VPN service in order to meet customer QoS and security requirements for the VoIP service. Therefore, the service offering under consideration must be decomposed into its composite services to address its overall security.

Securing the Management Security Plane of the Services Security Layer is concerned with securing the OAM&P functions and configuration of network services. An example of services management that needs to be secured is the provisioning of authorized users of a specific end-user service by network operations personnel. Table 5 describes the objectives of applying the Security Dimensions to the Services Security Layer, Management Security Plane.

Table 5 — Applying Security Dimensions to the Services Security Layer, Management Security Plane

Module 4: Services Security Layer, Management Security Plane	
Security Dimension	**Security Objectives**
Access Control	Ensure that only authorized personnel and devices are allowed to perform, or attempt to perform administrative or management activities of the network service (e.g., provision users of the service).
Authentication	Verify the identity of the person or device attempting to perform administrative or management activities of the network service. Authentication techniques may be required as part of Access Control.
Non-repudiation	Provide a record identifying the individual or device that performed each administrative or management activity of the network service and the action that was performed. This record is to be used as proof that the indicated individual or device performed the administrative or management activity.
Data Confidentiality	Protect the network service's configuration and management information (e.g., downloadable IPsec client settings for a VPN service) from unauthorized access or viewing. This applies to management and configuration information resident in network devices, being transmitted across the network, or stored offline. Protect the network service's administrative or management information (e.g., user identifications and passwords, administrator identifications and passwords) from unauthorized access or viewing.
Communication Flow Security	In the case of remote management of a network service, ensure that the administrative and management information only flows between the remote management station and the devices being managed as part of the network service. The administrative and management information is not diverted or intercepted as it flows between these endpoints. The same type of consideration is applied to the network service authentication information (e.g., user identifications and passwords, administrator identifications and passwords).
Data Integrity	Protect the administrative and management information of network services against unauthorized modification. This protection applies to administrative and management information resident in network devices, being transmitted across the network, or stored in offline systems. The same type of consideration is applied to network service authentication information (e.g., user identifications and passwords, administrator identifications and passwords).
Availability	Ensure that the ability to manage the network service by authorized personnel and devices cannot be denied. This includes protection against active attacks such as Denial of Service (DoS) attacks as well as protection against passive attacks such as the modification or deletion of the network service administrative authentication information (e.g., administrator identifications and passwords).
Privacy	Ensure that information that can be used to identify the network service administrative or management systems is not available to unauthorized personnel or devices. Examples of this type of information include a system's IP address or DNS domain name. For example, being able to identify the network service administrative systems provides targeting information to attackers. Ensure that personal information is collected, processed and disseminated through the network in accordance with local data protection legislation and regulation.

Securing the Control Security Plane of the Services Security Layer consists of securing the control or signaling information used by the network service. For example, issues of securing the SIP protocol that is used to initiate and maintain the VoIP sessions are addressed here. Table 6 describes the objectives of applying the Security Dimensions to the Services Security Layer, Control Security Plane.

Table 6 — Applying Security Dimensions to the Services Security Layer, Control Security Plane

Module 5: Services Security Layer, Control Security Plane	
Security Dimension	**Security Objectives**
Access Control	Ensure that control information received by a network device for a network service originates from an authorized source (e.g., a VoIP session initiation message has originated from an authorized user or device) before accepting it. For example, protect against the spoofing of a VoIP session initiation message by an unauthorized device.
Authentication	Verify the identity of the origination of network service control information sent to network devices participating in the network service. Authentication techniques may be used as part of Access Control.
Non-repudiation	Provide a record identifying the person or device originating the network service control messages received by a network device participating in the network service and the action that was performed. This record can be used as proof that the person or device originated the network service control message.
Data Confidentiality	Protect network service control information resident in a network device (e.g., IPsec session databases), being transported across the network, or stored offline from unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data Confidentiality for network service control information residing in the network device.
Communication Flow Security	Ensure that network service control information being transported across the network (e.g., IPsec key negotiation messages) only flows between the source of the control information and its desired destination. The network service's control information is not diverted or intercepted as it flows between these endpoints.
Data Integrity	Protect network service control information resident in network devices, in transit across the network, or stored offline against unauthorized modification.
Availability	Ensure that network devices participating in a network service are always available to receive control information from authorized sources. This includes protection against active attacks such as Denial of Service (DoS) attacks.
Privacy	Ensure that information that can be used to identify the network devices or communications links participating in a network service is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers. Ensure that personal information is collected, processed and disseminated through the network in accordance with local data protection legislation and regulation.