# Draft ITU-T Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications


## Summary

This Recommendation defines the general security-related architectural elements that when appropriately applied can provide end-to-end network security.


## 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 have high availability, appropriate response time, reliability, integrity, scalability, and provide accurate billing information. Security capabilities in products are crucial to the 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. To achieve such a solution in multi-vendor environment, network security should be designed around a standard security architecture.

**CONTENTS**

## 1 Scope

This Recommendation defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where the end-to-end security is a concern and independently of the network's underlying technology. This Recommendation defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.

## 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

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

## 3 Terms and definitions

This Recommendation uses the following terms from Recommendation X.800:

– access control
– availability
– authentication
– confidentiality
– data integrity
– non-repudiation
– privacy

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| ASP | Application Service Provider |
| ATM | Asynchronous Transfer Mode |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Service |
| DoS | Denial of Service |
| DS-3 | Digital Signal level 3 |
| FTP | File Transfer Protocol |
| IP | Internet Protocol |
| IPSec | IP Security protocol |

| | |
|---|---|
| OAM&P | Operations Administration Maintenance & Provisioning |
| OSI | Open Systems Interconnection |
| PSTN | Public Switched Telephone Network |
| PVC | Permanent Virtual Circuit |
| QoS | Quality of Service |
| SIP | Session Initiation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SONET | Synchronous Optical Network |
| SS7 | Signaling System #7 |
| SSL | Secure Socket Layer (Encryption and authentication protocol) |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |

## 5 Security Architecture

The Security 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. This Security Architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. The Security 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 detect, predict, and correct security vulnerabilities.

The Security 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 Security Architecture addresses three essential questions with regard to the end-to-end security:

1. What kinds of protection are needed and against what threats?
2. What are the distinct types of network equipment and facility groupings that need to be protected?
3. What are the distinct types of network activities that need to be protected?

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

The principles described by the Security Architecture can be applied to a wide variety of networks independently 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

A Security Dimension is a set of security measures designed to address a particular aspect of the network security. This Recommendation identifies eight such sets that protect against all major security threats. These dimensions are not limited to the network, but extend to applications and end user information as well. 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 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 protects against unauthorized use of network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, 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 that they are authorized for.

### 6.2 Authentication Security Dimension

The Authentication Security Dimension serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities 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.

### 6.3 Non-repudiation Security Dimension

The Non-repudiation Security Dimension provides 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 ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

### 6.4 Data Confidentiality Security Dimension

The Data Confidentiality Security Dimension protects data from unauthorized disclosure. Data Confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

### 6.5 Communication Security Dimension

The Communication 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).

### 6.6 Data Integrity Security Dimension

The Data Integrity Security Dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

### 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 information 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.

## 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 Recommendation 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 Layer enables the Services Layer and the Services Layer enables the Applications Layer. The Security 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.

It should be noted that Security Layers (as defined above) represent a separate category and all three Security Layers can be applied to each layer of the OSI Reference Model.

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 Layer, then - for the Services Layer, and finally security vulnerabilities are addressed for the Applications Layer. Figure 1 depicts how the Security Dimensions are applied to Security Layers in order to diminish vulnerabilities that exist at each layer and thus mitigate security attacks.

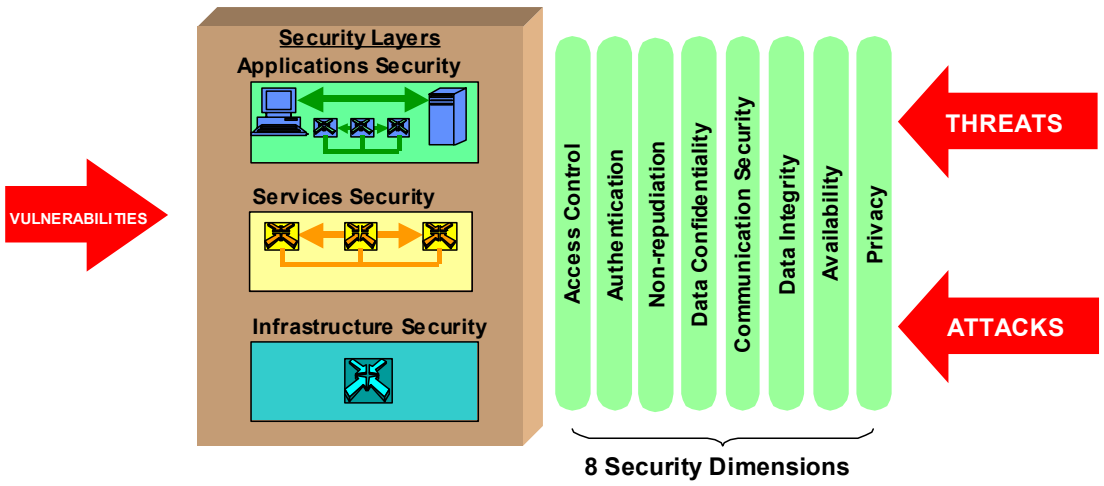


**Figure 1 – Applying Security Dimensions to Security Layers**

### 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 Security Dimensions. The Infrastructure Layer represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to the Infrastructure 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. AAA 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 Security Dimensions. This Recommendation 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 Plane, (2) the Control Plane, and (3) the End-User Plane. These Security Planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly.

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

Figure 2 illustrates the Security 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).

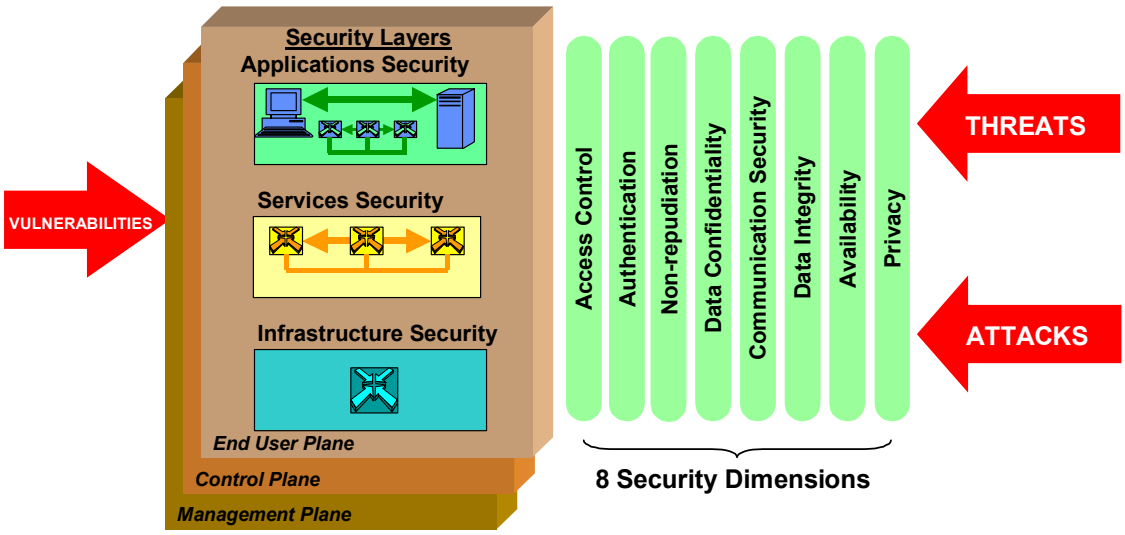


**Figure 2 – Security Planes Reflect the Different Types of Network Activities**

### 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 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 also represents 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 Security 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 CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications:

- 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 Plain 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 Security | | | Y | Y | |
| Data Integrity | Y | Y | | | |
| Availability | Y | | | | Y |
| Privacy | | | | Y | |

Figure 3 illustrates the Security 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).

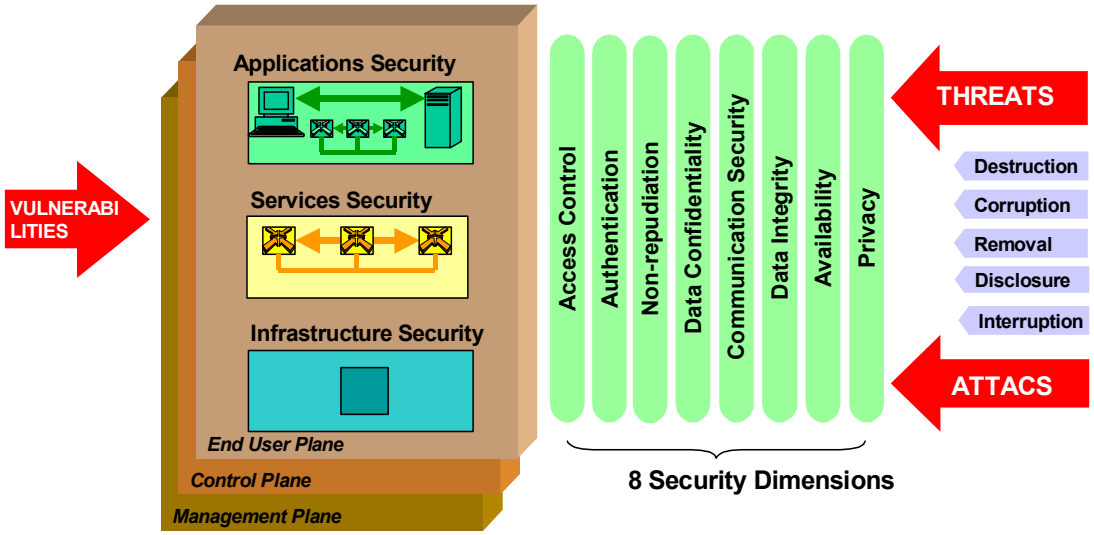


**Figure 3 – Security Architecture for End-to-End Network Security**

## 10 Description of the Objectives Achieved by Application of Security Dimensions to Security Layers

The Security 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 Security Architecture can be applied to security policies and procedures, as well as technology, across all three phases of a Security Program.

The Security 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 Security 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 Security 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.

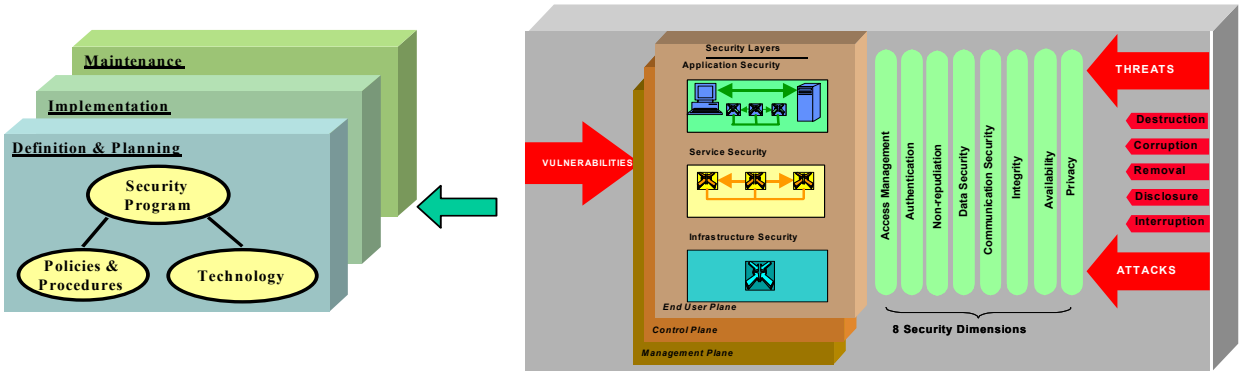


**Figure 4 – Applying the Security Architecture to Security Programs**

In addition, the Security 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 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 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 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 Layer refers to the individual switches, and the point-to-point communications links between the switches (carrier facilities, for example DS-3). The Services 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 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 Security 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 have different objectives and consequently comprise different sets of security measures. The tabular form gives a convenient way of describing the objectives of the Security Dimensions for each module.

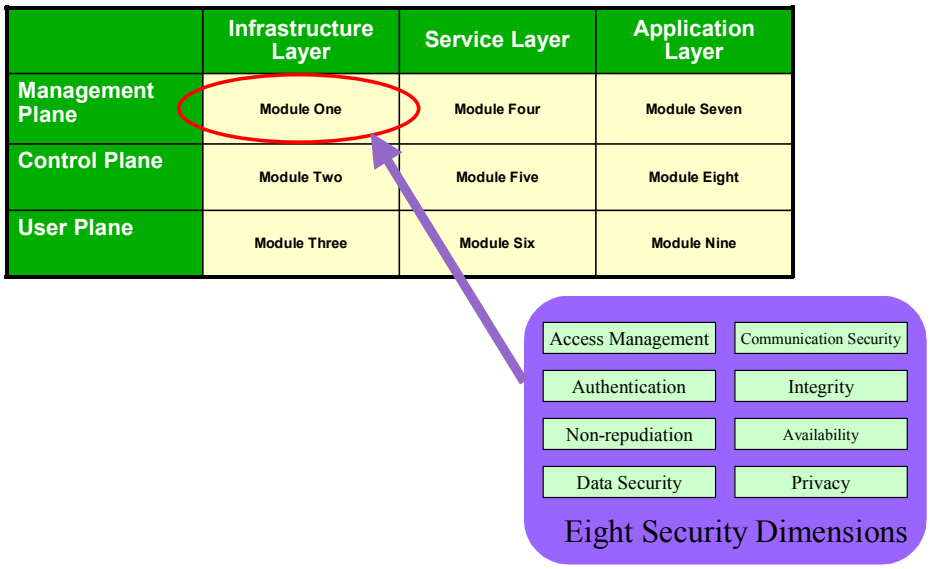


**Figure 5 – Security Architecture in a tabular form**

## 10.1 Securing the Infrastructure Layer

**10.1.1** Securing the Management Plane of the Infrastructure Layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the individual network elements, communication links, and server platforms that comprise the network. We consider the configuration of network devices and communications links to be a management activity as well. 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 Layer, Management Plane.

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

| Module 1: Infrastructure Layer, Management 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 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.<br>Protect the administrative authentication information (e.g., administrator identifications and passwords) from unauthorized access or viewing.<br>Techniques used to address Access Control may contribute to providing Data confidentiality. |
| **Communication 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.<br>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, deletion, creation, and replication. 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.<br>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. |

**10.1.2** Securing the Control Plane of the Infrastructure 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 Layer, Control Plane.

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

| **Module 2: Infrastructure Layer, Control Plane** | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized personnel and devices are allowed to access control information resident in the network device (e.g., a routing table) or in offline storage.<br>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.<br>Verify the identity of the device sending control information to the network device.<br>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.<br>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.<br>Protect control information destined for a network device from unauthorized access or viewing as it is being transported across the network. |
| **Communication 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, deletion, creation, and replication. |
| **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. |

**10.1.3** Securing the End-User Plane of the Infrastructure 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 Layer, End-User Plane.

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

| Module 3: Infrastructure Layer, End-User Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized personnel or devices are allowed 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.<br>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 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, deletion, creation, and replication. |
| **Availability** | Ensure that access to end-user data resident in offline 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. |

## 10.2 Securing the Services Layer

Securing the Services 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.

**10.2.1** Securing the Management Plane of the Services Layer is concerned with securing the OAM&P functions of network services. We consider the configuration of network services to be a management activity as well. An example of services management that needs to be secured is the provisioning of authorized users of an I service by network operations personnel. Table 5 describes the objectives of applying the Security Dimensions to the Services Layer, Management Plane.

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

| Module 4: Services Layer, Management Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized personnel and devices are allowed 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.<br>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 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.<br>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, deletion, creation, and replication. This protection applies to administrative and management information resident in network devices, being transmitted across the network, or stored in offline systems.<br>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. |

**10.2.2** Securing the Control Plane of the Services 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 Layer, Control Plane.

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

| Module 5: Services Layer, Control 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 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, deletion, creation, and replication. |
| **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. |

**10.2.3** Securing the End-User Plane of the Services Layer consists of securing user data and voice as it uses the network service. For example the confidentiality of a user's conversation must be protected in a VoIP service. Likewise, a DNS service must ensure the confidentiality of users of the service. Table 7 describes the objectives of applying the Security Dimensions to Services Layer, End-User Plane.

**Table 7 – Applying Security Dimensions to the Services Layer, End-User Plane**

| Module 6: Services Layer, End-User Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized users and devices are allowed to access and use the network service. |
| **Authentication** | Verify the identity of the user or device attempting to access and use the network service. Authentication techniques may be required as part of Access Control. |
| **Non-repudiation** | Provide a record identifying each user and device that accessed and used the network service and the action that was performed. This record is to be used as proof of access to and use of the network service by the end-user or device. |
| **Data confidentiality** | Protect end-user data that is being transported by, processed by, or stored by a network service against unauthorized access or viewing. Techniques used to address Access Control may contribute to providing Data confidentiality for end-user data. |
| **Communication Security** | Ensure end-user data that is being transported by, processed by, or stored by a network service 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 being transported by, processed by, or stored by a network service against unauthorized modification, deletion, creation, and replication. |
| **Availability** | Ensure that access to the network service by authorized end-users 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 end-user authentication information (e.g., user identifications and passwords). |
| **Privacy** | Ensure that the network service does not provide information pertaining to the end-user's use of the service (e.g., for a VoIP service, called parties) to unauthorized personnel or devices. |

## 10.3 Securing the Applications Layer

Securing the Management Plane of the Applications Layer is concerned with securing the OAM&P functions of the network-based application. We consider the configuration of network-based applications to be a management activity as well. For an email application, an example of the management activity that would need to be secured is the provisioning and administration of user mailboxes. Table 8 describes the objectives of applying the Security Dimensions to the Applications Layer, Management Plane.

**Table 8 – Applying Security Dimensions to the Applications Layer, Management Plane**

| Module 7: Applications Layer, Management Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized personnel and devices are allowed to perform administrative or management activities of the network-based application (e.g., administer user mailboxes for an email application). |
| **Authentication** | Verify the identity of the person or device attempting to perform administrative or management activities of the network-based application. 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-based application and the action that was performed. This record is to be used as proof that the administrative or management activity was performed with an indication of the individual or device that performed it. |
| **Data confidentiality** | Protect all files used in the creation and execution of the network-based application (e.g., source files, object files, executable files, temporary files, etc.) as well as the application configuration files from unauthorized access or viewing. This applies to application files resident in network devices, being transmitted across the network, or stored offline.<br>Protect the network-based application's administrative or management information (e.g., user identifications and passwords, administrator identifications and passwords) from unauthorized access or viewing. |
| **Communication Security** | In the case of remote administration or management of a network-based application, ensure that the administrative and management information only flows between the remote management station and the devices comprising the network-based application. The administration and management information is not diverted or intercepted as it flows between these endpoints.<br>The same type of consideration is applied to the network–based application's administrative or management information (e.g., user identifications and passwords, administrator identifications and passwords). |
| **Data Integrity** | Protect all files used in the creation and execution of the network-based application (e.g., source files, object files, executable files, temporary files, etc.) as well as the application configuration files against unauthorized modification, deletion, creation, and replication. This protection also applies to application files resident in network devices, being transmitted across the network, or stored in offline systems.<br>The same type of consideration is applied to network-based application administrative or management information (e.g., user identifications and passwords, administrator identifications and passwords). |
| **Availability** | Ensure that the ability to administer or manage the network-based application 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-based application's administrative authentication information (e.g., administrator identifications and passwords). |
| **Privacy** | Ensure that information that can be used to identify the network-based application's administrative or management systems are 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-based application's administrative systems provides targeting information to attackers. |

**10.3.2** Securing the Control Plane of the Applications Layer consists of securing the control or signaling information used by the network-based applications. This type of information typically causes the application to perform an action in response to receiving the information. For example, issues of securing the SMTP and POP protocols used to control the delivery of email would be

addressed here. Table 9 describes the objectives of applying the Security Dimensions to the Applications Layer, Control Plane.

**Table 9 – Applying Security Dimensions to the Applications Layer, Control Plane**

| Module 8: Applications Layer, Control Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that application control information received by a network device participating in a network-based application originates from an authorized source (e.g., an SMTP message requesting the transfer of email) before accepting it. For example, protect against the spoofing of a SMTP client by an unauthorized device. |
| **Authentication** | Verify the identity of the origination of application control information sent to network devices participating in the network-based application. Authentication techniques may be used as part of Access Control. |
| **Non-repudiation** | Provide a record identifying the person or device originating the application control messages received by a network device participating in the network-based application and the action that was performed. This record can be used as proof that the person or device originated the application control message. |
| **Data confidentiality** | Protect application control information resident in a network device (e.g., SSL 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-based application control information resident in the network device. |
| **Communication Security** | Ensure that application control information being transported across the network (e.g., SSL negotiation messages) only flows between the source of the control information and its desired destination. The network-based application's control information is not diverted or intercepted as it flows between these endpoints. |
| **Data Integrity** | Protect network-based application control information resident in network devices, in transit across the network, or stored offline against unauthorized modification, deletion, creation, and replication. |
| **Availability** | Ensure that network devices participating in network-based applications 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-based application 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. |

**10.3.3** Securing the End-User Plane of the Applications Layer consists of securing user data provided to the network-based application. For example the confidentiality of a user's credit card number must be protected by an e-commerce application. Table 10 describes the objectives of applying the Security Dimensions to the Applications Layer, End-User Plane.

## Table 10 – Applying Security Dimensions to the Applications Layer, End-User Plane

| Module 9: Applications Layer, End-User Plane | |
|---|---|
| **Security Dimension** | **Security Objectives** |
| **Access Control** | Ensure that only authorized users and devices are allowed to access and use the network-based application. |
| **Authentication** | Verify the identity of the user or device attempting to access and use the network-based application. Authentication techniques may be required as part of Access Control. |
| **Non-repudiation** | Provide a record identifying each user or device that accessed and used the network-based application and the action that was performed. This record is to be used as proof of access to and use of the application by the end-user or device. |
| **Data confidentiality** | Protect end-user data (e.g., a user's credit card number) that is being transported by, processed by, or stored by a network-based application against unauthorized access or viewing.<br>The same types of considerations are applied to user data as it flows from the user to the network-based application.<br>Techniques used to address Access Control may contribute to providing Data confidentiality for end-user data. |
| **Communication Security** | Ensure end-user data that is being transported by, processed by, or stored by a network-based application is not diverted or intercepted as it flows between these endpoints without authorized access (e.g., wiretaps).<br>The same types of considerations are applied to user data as it flows from the user to the network-based application. |
| **Data Integrity** | Protect end-user data that is being transported by, processed by, or stored by a network-based application against unauthorized modification, deletion, creation, and replication.<br>The same types of considerations are applied to user data as it flows from the user to the network-based application. |
| **Availability** | Ensure that access to the network-based application by authorized end-users 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 end-user authentication information (e.g., user identifications and passwords). |
| **Privacy** | Ensure that the network-based application does not provide information pertaining to the end-user's use of the application (e.g., web sites visited) to unauthorized personnel or devices. For example, only disclose this type of information to law enforcement personnel with a search warrant. |