DATA SECURITY MANAGEMENT

NETWORK LAYER SECURITY

Steve Blanding

INSIDE
Network Layer Structure, Service, and Protocol; Security Service Architectural Placement;
End-System Level Security; Subnetwork Level Security; Network Layer Security Protocol;
Secure Data Transfer; Connection Establishment and Release

INTRODUCTION
Modern computer networks are characterized by layered protocol architectures, allowing network designs to accommodate unlimited applications and interconnection techniques. This layered approach allows protocols to become modularized; that is, developed independently and put together with other protocols in such a way as to create one complete protocol. The recognized basis of protocol layering is the open systems interconnection (OSI) architecture. The OSI standards establish the architectural model and define specific protocols to fit into this model, which defines seven layers. Protocols from each of the layers are grouped together into an OSI layer stack, which is designed to fulfill the communications requirements of an application process.

Standards are also needed to adequately support security in the OSI layered communications architecture. A broad, coordinated set of standards is required to ensure necessary security functionality and still provide a cost-effective implementation. Because of the complexity and flexibility of the OSI model, security must be carefully defined to avoid an increased potential for functions being duplicated throughout the architecture and incompatible security features being used in different parts of the architecture. There is also a possibility that different and potentially contradictory security techniques can be used in different applications or layers, where fewer techniques would provide the required results with less complexity and more economy.

Security standards were added to the OSI architecture to provide a
broad, coherent, and coordinated approach to applying security functionality. The security standards can be grouped into categories as follows: (1) security architecture and framework standards, (2) security techniques standards, (3) layer security protocol standards, (4) application-specific security standards, and (5) security management standards. This article focuses primarily on network layer security, which is part of the family of layer security protocol standards. However, because the standards are closely interrelated, a brief overview of the security architecture and framework standards is required. These standards serve as a reference base for building standards in the other categories, including network layer security.

NETWORK LAYER STRUCTURE, SERVICE, AND PROTOCOL
The network layer of the OSI model accommodates a variety of subnet-network technologies and interconnection strategies, making it one of the most complex of the seven layers in the model. The network layer must present a common service interface to the transport layer and coordinate between subnetworks of different technologies. There are also two styles of operation — connection oriented and connectionless — that significantly contribute to this complexity.

There are three ISO standards that describe the Network Layer services: ISO/IEC 8648, ISO/IEC 8880, and ISO/IEC 8348. The internal organization of the network layer is explained by the ISO/IEC 8648 standard. The general principles and the provision and support of the connection-mode and connectionless-mode network services are explained by the ISO/IEC 8880 standard. The network service definition, which includes the connection-mode, connectionless-mode addendum, and addressing addendum, is explained by the ISO/IEC 8348 standard; this standard also describes the concepts of end-system and intermediate system. An end-system models hardware across a complete seven-layer OSI communications model, whereas an intermediate system, which is located in the network layer, only functions across the lowest three OSI layers. Communications by an end-system can occur directly with another end-system or through several intermediate systems.

Intermediate systems can also include or refer to a real subnetwork, an internetworking unit connecting two or more real subnetworks, or a mix of both a real subnetwork and an internetworking unit. A collection of hardware and physical links that connect real systems is called a real subnetwork. Examples of real systems include local-area networks or public packet-switching networks. With this foundation, many different network layer protocols can be established. Because the protocol can exist at the subnetwork level within the network layer, they do not need to be designed to specifically support the OSI standard. As a result, support for all the functions required by the network layer service do not need to
be provided by the basic protocol of a subnetwork. To achieve OSI standard functionality, further sublayers of protocol can be provided above the subnetwork protocol.

Regardless of the type of interconnection designed, one of three roles is performed by a network layer protocol. These roles are Subnetwork-Independent Convergence Protocol (SNICP), Subnetwork-Dependent Convergence Protocol (SNDCP), and Subnetwork Access Protocol (SNAcP). The SNICP role provides functions to support the OSI network service over a well-defined set of underlying capabilities that are not specifically based on any particular subnetwork. The role is to convey addressing and routing information over multiple interconnected networks and commonly applies to the interconnecting protocol used. The SNDCP role is a role that operates over a protocol to provide the SNAcP role in order to add capabilities required by the SNICP or needed to provide the full OSI network service. The SNAcP role provides a subnetwork service at its endpoints, which may or may not be equivalent to the OSI network service. This protocol is inherently part of a particular type of subnetwork.

ISO/IEC 8473 identifies another protocol that is very important to the network layer: the Connectionless Network Protocol (CLNP). This protocol provides connectionless-mode network service within an SNICP role. The definition for how this protocol operates over X.25 packet-switched subnetworks or LAN subnetworks is contained within the ISO/IEC 8473 standard.

SECURITY SERVICE ARCHITECTURAL PLACEMENT
When designing security, significant decisions need to be made as to the layer(s) where data item or connection-based protection should be applied. Implementing security services in a layered communications architecture can be a complicated endeavor and can raise significant issues. The concept of protocol layering implies that data items can be embedded within data items and connections can be embedded within connections, with potentially multiple layers of nesting.

Guidance for where security services should be applied within the OSI model is provided in standard ISO/IEC 7498-2. As the first formal standard addressing layer assignment of security services, this standard, while providing guidance as to which OSI layers are appropriate for providing security services, does allow for many options. The security required is application dependent. Some services may need to be provided in different layers in different application scenarios, while some may even need to be provided in multiple layers in the same scenario. The complexity of these security services can be illustrated by a pair of end-systems communicating with each other through a series of subnetworks.

An end-system is typically defined as one piece of equipment, either a PC workstation, minicomputer, or mainframe computer. An end-system
is described as having only one policy authority for security purposes. A collection of communications facilities employing the same communications technology is a subnetwork. An example of a subnetwork is a local-area network (LAN) or wide-area network (WAN). A subnetwork is described as having only one policy authority for security purposes. Each subnetwork, however, typically has a different security environment and, as a result, will probably have a different policy authority. Also, an end-system and the subnetwork to which it is connected may or may not have the same policy authority.

Another complication typically found in end-systems is that, typically, they simultaneously support multiple applications such as e-mail, file access, and directory access for simultaneously for multiple users. These applications often need considerably different security requirements. Not only may security requirements differ among end-systems and for subnetworks, but they may also vary within a subnetwork. Subnetworks generally comprise multiple links connecting multiple subnetwork components, and different links can pass through different security environments. As a result, individual links may need to be protected through a security mechanism.

To reduce the complexity, security services can be described more simply and effectively within a four-level model. The four levels at which specific and distinct requirements for security protocol elements arise include the application, end-system, subnetwork, and the direct-link levels. In the application level, security protocol elements are application dependent. In the end-system level, security protocol elements provide protection on an end-system to end-system basis. In the subnetwork level, security protocol elements provide protection internal to a subnetwork, which is considered less trusted than other parts of the network environment. In the direct-link level, security protocol elements provide protection internal to a subnetwork, over a link that is considered less trusted than other parts of the subnetwork environment.

When determining where to locate security services within these four basic architectural layers, some general properties must first be examined that vary between higher and lower levels. These general properties include traffic mixing, route knowledge, number of protection points, protocol header protection, and source/sink binding.

Traffic mixing is a term used to describe the mix of data traffic between higher and lower levels of the OSI layer architecture. With the introduction of multiplexing, lower levels tend to have more data items from different source and destination applications and users mixed in the data stream than at higher levels. The type of security policy can significantly alter this factor. In instances where the security policy tends to leave individual applications or users to specify the data protection required, then placing security services at a higher level tends to be better. Individual applications or users will have inadequate protection where
security is specified at lower levels. In addition, some data would also be unnecessarily protected because of the security requirements of other data sharing the data stream.

Route knowledge is also an important factor in security placement. There tends to be more knowledge of the security characteristics of different routes and links at lower levels than at higher levels. Placing security at lower levels can have effectiveness and efficiency benefits in an environment where such characteristics vary significantly. Where protection is unnecessary on subnetworks or links, security costs can be eliminated while targeted security services are specifically employed as appropriate.

The number of protection points can vary significantly, depending on where security protection is placed. If security is placed at a very high level, such as the application layer, then security also needs to be placed in every sensitive application in every end-system. If security is placed at a very low level, such as the direct-link level, then security also needs to be placed at the ends of every network link. If security is placed closer to the middle of the architecture, then security features tend to need to be placed at significantly fewer points.

To have adequate protocol header protection, security services need to be placed at a low level. If security services is placed at higher levels, lower-level protocol headers will not receive protection, which in some environments may be sensitive.

Source/sink binding is the association of data with its source or sink. Implementation of data origin authentication and nonrepudiation security services depends on this binding. These security services are most effectively achieved at higher levels, especially at the application level. However, subject to special constraints, it can sometimes be achieved at lower levels.

END-SYSTEM LEVEL SECURITY

End-system level security relates to either the transport layer or subnetwork-independent network layer protocols. Standards have been developed supporting both options — ISO/IEC 10736 for the transport layer and ISO/IEC 11577 for the network layer. The types of security requirements suitable for an end-system level security solution fall into three broad categories. The first includes requirements relating to network connections that are not linked to any particular application. The second includes requirements dictated by the end-system authority that are to be enforced upon all communications, regardless of the application. Finally, the third includes requirements based on the assumption that the end-systems are trusted, but that all underlying communications network(s) are untrusted.

In choosing between the transport layer and network layer for placement of end-level security protection, factors favoring the network layer
approach include the (1) ease of transparently inserting security devices at standardized physical interface points, (2) ability to support any upper-layer architecture, including OSI, Internet, and proprietary architectures, and (3) ability to use the same solution at the end-system and subnetwork levels.

**SUBNETWORK LEVEL SECURITY**

Subnetwork level security provides protection across one or more specific subnetworks. Subnetwork level security needs to be distinguished from end-system level security for two important reasons. First, equipment and operational costs for subnetwork level security solutions may be much lower than those for end-system level solutions because the number of end-systems usually far exceeds the number of subnetwork gateways. Second, subnetworks close to end-systems are trusted to the same extent as the end-systems themselves because they are on the same premises and administered under the same conditions. As a result, subnetwork level security should always be considered as a possible alternative to end-system level security. In the OSI architecture, subnetwork level security maps to the network layer.

**Network Layer Security Protocol**

The network layer is among the complex of layers within the OSI model. As a result, several OSI standards are required to specify transmission, routing, and internetworking functions for this layer. The ISO/IEC 8880 standard describes an overview of the network layer. Two other standards, ISO/IEC 8348 and 8648, define the network service and describe the internal organization of the network layer, respectively. The most recent standard published is ISO/IEC 11577, which describes the Network Layer Security Protocol (NLSP).

Different sublayers make up the network layer, each performing different roles, such as Subnetwork Access Protocol (SNAcP) and Subnetwork-Dependent Convergence Protocol (SNDCP). The architectural placement of the NLSP can be in any of several different locations within the network layer, functioning as a sublayer. Above the highest layer is the transport layer, or possibly a router where a relay or routing function is in place.

Two service interfaces — the NLSP service interface and the underlying network (UN) service interface — are contained within the Network Layer Security Protocol. The NLSP service is the interface presented to an entity or sublayer above, and the UN service is the interface to a sublayer below. These service interfaces are specified in such a way as to appear like the network service, as defined in ISO/IEC 8348. The Network Layer Security Protocol can also be defined in two different forms or variations: connection oriented and connectionless. In the connection-oriented
NLSP, the NLSP service and the UN service are connection oriented; whereas in the connectionless NLSP, these services are connectionless. The flexibility of the architecture results from the ability of the NLSP to support both end-system level or subnetwork level security services.

For example, in a connection-oriented NLSP, X.25 is defined as the underlying subnetwork technology. In this configuration, the NLSP is placed at the top of the network layer (just below the transport layer and just above the X.25 subnetwork), allowing the NLSP service to equate to a secure version of the OSI network service. In this example, the X.25 protocol is not aware that security is provided from above.

The NLSP can also provide subnetwork level security. In instances where the subnetwork is untrusted, the NLSP adds the necessary security, which can equate to either the OSI network service in the end-system or to the network internal layer service (NILS) in a relay system. In connectionless cases, several configurations with practical applications are possible, such as the transfer of fully unencrypted ConnectionLess Network Protocol (CLNP) headers, encrypted CLNP addresses with parts of the header not encrypted, or fully encrypted CLNP headers.

SECURE DATA TRANSFER

Encapsulation is a security function used to protect user data and sensitive parameters. In both connection-oriented and connectionless NLSP, the primary function is to provide this protection originating on request or response primitives issued at the NLSP service. The encapsulation function applies this security by generating data values for corresponding request or response primitives issued at the UN service, which is then reversed at the receiving end. This is very similar to the process used in the TLSP, where the generation and processing of the Security Encapsulation PDU occurs.

Different encapsulation functions are available for different environments within the NLSP. This provision includes the basic encapsulation function, which is very similar to the encapsulation function defined in the TLSP. The NLSP does have some additional features included in the basic function. Each octet string to be protected contains a string of fields, including (1) address parameters requiring protection, (2) quality-of-service parameters requiring protection, (3) an indicator of the type of primitive (e.g., connect request, connect response, disconnect, etc.), (4) user data requiring protection, (5) test data for use in testing cryptographic system operation, and (6) security label.

When compared to the TLSP, the protection process is the same, with the exception of two additional fields included within the generated PDU. These are an integrity sequence number (ISN) and a traffic padding field. The ISN is used to support sequence integrity. Because transport protocol sequence numbers could serve this purpose in the TLSP, this
The traffic padding field is used to support the traffic flow confidentiality service, which is a requirement of the NLSP but not the TLSP.

The encapsulation function can include either a clear header process or, as an alternative to the basic encapsulation function, a no-header process. In the clear header feature, a clear header is prefixed to the resulting protected octet string to give an NLSP secure data transfer PDU, which contains the security association identifier. The no-header encapsulation feature is also available for optional use only with connection-oriented NLSP. The no-header option can be used when the only security mechanism applied is encryption and when the encryption/decryption processes do not change the data lengths. In the no-header alternative, the secure data transfer PDU is replaced by an encrypted version of the data requiring protection. This allows the NLSP to be inserted transparently within the network layer. The data characteristics of the underlying services, such as data rates, packet sizes, and bandwidth, are not affected. As a result, security functions can easily be added to an existing service without changing the network architecture. However, the range of services that can be supported is greatly reduced because ICV, ISN, padding, and security labels cannot be used. Integrity services can still be maintained where the data has sufficient natural redundancy and if cryptographic chaining is used. Basic confidentiality is also not compromised and can still be supported.

The mapping of the same type of NLSP service primitives to UN service primitives, with the exception of connection establishment and release, is how the NLSP operates. If fields do not require protection, they are copied directly from one service primitive to the other. Those NLSP fields that do require protection are processed by the encapsulation function. The encapsulated result, or secure data transfer PDU, is mapped to a user data parameter of the UN service primitive. The application of the encapsulation function may result in data expansion, which could require the use of segmentation.

**CONNECTION ESTABLISHMENT AND RELEASE**

As mentioned previously, special procedures are required to handle connection establishment with connection-oriented NLSP. The NLSP is similar to the TLSP in that not only does the NLSP support internal security protocol, but also security associations managed by other means. The use of special procedures depends on whether or not security association establishment needs to occur in conjunction with connection establishment.

Even where a suitable security association already exists — in other words, a situation not involving security association establishment — there is a requirement for a special NLSP protocol exchange at connection establishment time. This is needed to perform peer entity authenti-
cation, establish particular encryption and integrity keys for use on the connection, and to establish starting ISNs. In this case, a connection security control PDU is defined in the NLSP to convey this information. At connection establishment, a two-way exchange of these PDUs occurs. The type of connection authentication mechanism specified for the particular security association determines the variation in the precise contents of the PDU. The PDU fields would include a security label, key reference or key derivation information, and encrypted versions of two ISNs, one for each direction in traffic. Successful decryption of the ISN field can simultaneously provide protection against replay attacks on authentication, demonstrate key knowledge for authentication purposes, and confirm starting ISNs.

The data exchanges can be much more complex where security association establishment is to occur in conjunction with connection establishment. This additional complexity is typically addressed through the definition of a separate security association PDU. This separate PDU is used to handle the need for more than a two-way exchange for authentication and key derivation purposes, as well as substantial attribute negotiation. Again, like the TLSP, the NLSP does not require a particular security association establishment technique. Instead, one suitable technique based on the Authenticated Diffie-Hellman exchange is described.

The last area of discussion in this section is a description of how the protocol exchanges for NLSP connection establishment map onto the UN service. Mapping directly onto the UN connection establishment primitives would be the ideal situation; however, in reality, the required NLSP protocol exchanges add substantial overhead and thus prevents this possibility. There may not be space in the UN connection establishment PDUs for all the data that needs to be transferred because user data fields of network protocols are commonly limited in length. In addition to this, a multi-way protocol exchange may be needed to establish a security association.

These conditions require that two basic mapping alternatives be defined. An NLSP connection establishment can map directly to UN connection establishment where only a two-way exchange is necessary and all required data can fit in the user data fields of the UN connect primitives. If these conditions do not exist, the required data transfers map to UN data exchanges following UN connection establishment. Additional complications may occur where data transfers map to UN data exchanges. There is a possibility that the throughput, window size, quality-of-service, and other service parameters eventually negotiated do not match the characteristics of the UN connection. When this occurs, a new UN connection is established with the required, now-known, characteristics and the original UN connection is released.

Mapping problems can also occur where, upon release of an NLSP connection, user data on the disconnect needs to be protected by the encapsulating function and the resultant PDU cannot fit in the user data
parameter of UN disconnect. The NLSP PDU must map to a UN data exchange prior to UN disconnect in this scenario. The NLSP is a powerful and complex protocol because of the large number of possible mapping scenarios.

SUMMARY
In general, lower-layer security protocols support end-system level, direct-link level, and subnetwork level security services. Security services at the subnetwork and end-system levels support confidentiality, integrity, access control, and authentication services. Security services at the direct-link level support confidentiality only. These services differ according to whether the environment is connection oriented or connectionless.

Throughout the lower layers, the concepts of protection quality-of-service and security associations are used. To signal protection requirements across layer boundaries and to negotiate requirements between two ends, protection quality-of-service is used. To provide a consistent type of protection to a sequence of data transfers between two systems, a security association is used to model the collection of related attribute information maintained between those systems. A security association can be established through application layer protocol exchanges, lower-layer protocol exchanges in the same layer that uses the security exchange, or through non-standard methods.

The NLSP is very flexible, functioning at either the end-system or the subnetwork level. The NLSP can be positioned at any of several different places in the network layer, functioning as a sublayer. The NLSP is able to conceal trusted subnetwork protocol information while this information travels through an untrusted subnetwork, depending on its positioning within the network layer. Variations of NLSP include connection oriented and connectionless. The connection-oriented variant works in conjunction with such protocols as X.25, and the connectionless variant works in conjunction with the Connectionless Network Protocol (CLNP). An encapsulation process very similar to that of TLSP is used by NLSP. To provide for the establishment of security associations, optional protocol support is used.

Steven F. Blanding works in the Houston, TX office of Arthur Andersen LLP.