International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1161

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Framework for secure peer-to-peer communications

Recommendation ITU-T X.1161

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1161

Framework for secure peer-to-peer communications

Summary

Recommendation ITU-T X.1161 describes security threats and security requirements to the peer-to-peer (P2P) communications based on the service scenarios and characteristics of P2P communications. In addition, this Recommendation describes security functions that satisfy the security requirements.

Source

Recommendation ITU-T X.1161 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1161

Framework for secure peer-to-peer communications

1 Scope

Peer-to-peer (P2P) is an instantiation of network architectures where all peers have equivalent authority and responsibility, differing completely from that of server and client system. In the case of P2P communications, a peer can be both the server and the client. When data or messages are exchanged in a P2P network, a peer communicates with other peers directly. Because traffic and processing are distributed to each peer, the P2P network does not require high performance computing power and high bandwidth network compared with the server and client system.

Because the P2P communication architecture differs from that of the server and client system, further security threats emerge, which are not applicable to server and client architecture. With this in mind, P2P applications should be carefully built while taking into consideration the security threats to P2P communications.

This Recommendation describes the framework for secure P2P communications, which includes security threats and security requirements for P2P communications. In addition, this Recommendation describes the security functions for satisfying the security requirements of P2P communications. Security architectures and operations of P2P communications are defined in [ITU-T X.1162].

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; 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ITU-T X.800]: See data origin authentication defined in clause 3.1.10, and peer-entity authentication defined in clause 3.1.20.

NOTE – In this Recommendation, the term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead.

3.1.3 authentication information [b-ITU-T X.800]: Information used to establish the validity of a claimed identity.

3.1.4 authentication exchange [b-ITU-T X.800]: A mechanism intended to ensure the identity of an entity by means of information exchange.

3.1.5 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.6 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.7 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.8 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.1.9 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.10 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.11 decipherment [b-ITU-T X.800]: The reversal of a corresponding reversible encipherment.

3.1.12 denial of service [b-ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.13 digital signature [b-ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.

3.1.14 encipherment [b-ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce ciphertext.

NOTE – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.1.15 integrity [b-ITU-T X.800]: See data integrity.

3.1.16 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.17 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.18 notarization [b-ITU-T X.800]: The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.

3.1.19 password [b-ITU-T X.800]: Confidential authentication information, usually composed of a string of characters.

3.1.20 peer-entity authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.21 privacy [b-ITU-T X.800]: The 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.

NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

3.1.22 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.23 routing control [b-ITU-T X.800]: The application of rules during the process of routing so as to choose or avoid specific networks, links or relays.

3.1.24 threat [b-ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anonymity: Ability to allow anonymous access to services, which avoid the tracking of user's personal information and user behaviour such as user location, frequency of a service usage, etc.

3.2.2 content: Information created by individuals, institutions and technology to benefit audiences in contexts that they value. The contents are exchanged over the P2P networks.

3.2.3 P2P communications: Communications on P2P network, whereby each peer communicates with another peer directly for sharing information, resource, etc.

3.2.4 peer: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

3.2.5 traceability: A process to ensure that the communication of past activities can be checked.

3.2.6 traffic control: Adjustment of traffic amount for communications.

3.2.7 user authentication: The corroboration that a user of peer entity in an association is the one claimed.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

DoS Denial of Service

ID Identifier

P2P Peer-to-Peer

5 Conventions

None.

6 Concepts of P2P communications

Before describing the security threats and requirements for P2P communications, the concepts of P2P communications are explained in this clause.

6.1 Basic P2P service concept

Figure 1 shows a basic P2P service architecture. In the case of P2P communications, information data processed by each peer are exchanged directly among users. Because there is no central sever to store the information data, each peer needs to find which peers have target information data before retrieving the same. Moreover, each peer must also permit accesses from other peers to exchange the information data.

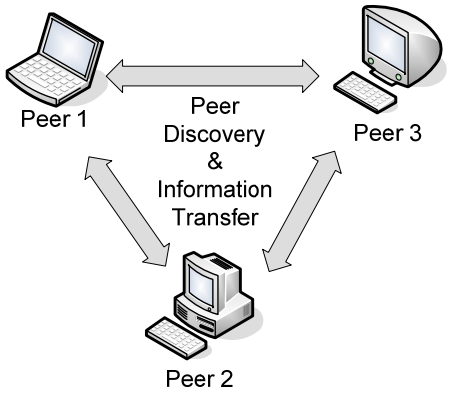

Figure 1 – P2P service architecture

6.2 Unstructured and structured P2P communications

There are two major kinds of P2P service concepts. One is unstructured P2P, and the other is structured P2P. In case of the unstructured P2P model, a P2P network is formed when the overlay links are established arbitrarily. Such networks can be easily constructed as a new peer that wants to join the network and which can copy existing links of another node and subsequently form its own links over time.

The structured P2P model has a specific topology to find target data quickly and efficiently. For example, a huge hash table that locates information data is managed by all peers in a distributed manner. By using this method, each peer can find the target node with a smaller number of hops as compared to the unstructured P2P type.

7 Service scenarios of P2P communications

7.1 Information sharing and contents distribution

A P2P network can be used as a large database. In this case, each peer stores several kinds of data in local storage, and other peers search the data and retrieve them. When the peers retrieve data, those data are stored in its local storage facility, normally with open access to other peers on the P2P network. This means the popular data will be stored in the storage of many peers, and renders the data distribution efficient.

7.2 Communication platform

A P2P network can be used as a communication platform. If a user would like to contact a specific user, the user starts to search for the location of the latter. When the user finds this information, the user makes contact with the specific user directly. In some cases, the other peer may mediate its communication when the users cannot communicate directly due to firewall problems, etc. The P2P communication platform is used for instant messaging, internet telephony, video conferencing, etc.

7.3 Groupware (Collaboration)

A P2P network can be used for collaborative work with group members. Basic technologies of this service scenario are based on the information sharing and communication platform. In this service scenario, group users can share files or data, and can contact other users easily when they are doing collaborative work.

7.4 Distributed computing

A P2P network can be used for distributed computing. In this service scenario, each peer joins the P2P network in order to provide its computational power. The P2P network becomes virtual high speed computer by collectively gathering such computing power.

8 Characteristics of P2P communications

P2P communications have various characteristics compared to general server-and-client data communication in an open network. This clause describes the characteristics of P2P communications regarding security.

Characteristic 1

Each peer needs to have capability as server. This means that the peer permits access from other peers.

Characteristic 2

In case of server and client communication, the server can know its communication situations, such as traffic, accessing client, accessed files, etc. Moreover, the server can control its traffic by changing the access control policy. However, it is not easy to know the communication situations in case of P2P communications.

Characteristic 3

If the P2P is used as a network platform, many users join this platform as peers. It may be easy for malicious users to join this P2P network.

Characteristic 4

In case of P2P communications, many data are exchanged between peers. In case of P2P communications, such data may be sent from unreliable peers.

9 Security threats to P2P communications

This clause describes security threats to P2P communications.

9.1 Eavesdropping

Because P2P communications use open networks, anonymous attackers may eavesdrop its communications by capturing traffic. Moreover, peers may be able to gather various kinds of data which are exchanged on P2P networks, if malicious users join the P2P network as peers.

9.2 Communication jamming

In case of P2P communications, all peers act as individual communication nodes for the P2P network. Therefore, malicious users, which join the P2P network as peers, may be able to disturb the P2P network. The following attacks are examples of this threat:

– A peer stores and retrieves data repeatedly.
– A peer joins and leaves the P2P network rapidly.
– A peer sends unsolicited messages to other peers repeatedly.
– A peer disturbs the routing information of the P2P network.

These kinds of attacks can result in DoS (Denial of Services) attacks.

9.3 Injection and modification of data

Because the peers of the P2P network relay data from one peer to another, they can easily inject and modify the data. Therefore, if the data are relayed by malicious or compromised peers, the relayed data may be altered by such peers. Moreover, it may be easy to distribute malicious software, such as viruses, worms, bots, etc., and malicious information, such as false file indexes, false IP addresses, or false routing tables.

9.4 Unauthorized access

Access control is the ability to limit and control the access to data and peers. This threat occurs when a malicious peer gains access to other peers by masquerading as a normal peer. Peers trying to gain unauthorized access must be identified, or authenticated.

9.5 Repudiation

This attack occurs when a peer denies the fact of having transmitted or received data, respectively.

9.6 Man-in-the-middle attack

A man-in-the-middle attack is a situation whereby an attacker can read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

9.7 Sybil attack

A Sybil attack is a situation whereby an attacker controls a P2P network by generating a large number of pseudonymous entities. The Eclipse attack is a typical example of the Sybil attack. Each node in the P2P network needs to maintain links to a set of neighbouring nodes, with which it communicates by forwarding messages. In case of the Eclipse attack, an attacker controls a large fraction of the neighbouring sets of victim nodes by dropping or rerouting messages. By performing such an attack, the attacker can eclipse the correct nodes from the P2P network.

10 Security requirements for P2P communications

10.1 User authentication

User authentication is used for one user of peer to prove its identity to a corresponding user of peer.

10.2 Anonymity

In some kinds of P2P applications, users would like to retain their anonymity during P2P communications. By ensuring the anonymity on the P2P applications, users can easily join communities on the P2P network. This enables the transmission of data so that other users cannot identify the sending user.

However, perfect anonymity may be used to attack the P2P network. The following are examples of attacks to the P2P network:

– One user may use another user's nickname to spread forged information, or to entrap someone.

– One user may handle multiple nicknames to confuse information.

– One user may distribute a lot of meaningless information or advertisement to the P2P network.

Therefore, protection mechanisms for such attacks should be considered when the anonymity is provided.

10.3 Privacy

Privacy provides for the protection of information that might be derived from the observation of network activities or communication. Examples of this information include communicating peers, the contents of transferred data or messages, a user's geographic location and user's ID.

10.4 Data integrity

In case of the P2P communications, data and messages are stored at peers, and transferred to other peers. When malicious users receive the data or messages, they may alter them in order to distribute malicious programs or messages. Data integrity ensures the correctness or accuracy of data or messages. Data or messages are then protected against unauthorized modification, deletion, creation and replication, and an indication of these unauthorized activities can be provided.

10.5 Data confidentiality

Various kinds of data and messages can be exchanged and transferred on a P2P network. In the case of certain applications, users might want to disclose sensitive data or messages to specified users only. Data confidentiality protects data from unauthorized disclosure, and ensures that the data content cannot be read by unauthorized peers.

10.6 Access control

Access control protects against unauthorized access to several kinds of resources, and ensures that only authorized peers are allowed access to data or messages, P2P networks and other peer resources. It is used in the following situations:

Access control on data or messages

When data or messages are exchanged and transferred on a P2P network, access control to those data or messages may be required to restrict access for specific users.

Access control on a P2P network

In order to restrict access to a P2P network, the P2P network might want to permit access based on the user's identity or other properties.

Access control on each peer

In case of P2P communications, each peer communicates with other peers directly. In some cases or applications, a peer might want to restrict access to itself from other peers, based on the user's identity or other properties.

10.7 Non-repudiation

Non-repudiation with proof of origin

This is used to prove that the origin of received data or messages is a particular peer. This mechanism is used in order to protect against any attempts by the peer to falsely deny sending the data or messages.

Non-repudiation with proof of delivery

This is used to provide proof of delivery of data or a message to a peer. This mechanism is used in order to protect against any subsequent attempts by the peer to falsely deny receiving the data or messages.

10.8 Usability

P2P networks consist of many peers, each of which communicates with other peers directly. Because each peer is a part of the P2P network, incorrect settings may adversely affect the P2P network. On the other hand, because each peer permits acceptance of the communication from other peers, wrong settings may result in vulnerability, leaving them open to attacks from malicious peers. For example, when a peer provides a storage resource for the P2P network, that should not contain valuable and important files. If the peer opens its storage space that contains important data, the data are then leaked onto the P2P network. In order to avoid such mistakes, P2P applications should provide a good user interface and security mechanisms that do not permit users to have incorrect settings.

10.9 Availability

Availability ensures that there is no denial of authorized access to several kinds of resources due to events impacting the network. Availability also allows users to receive an application service from anywhere and at anytime on P2P with the ability of such service.

10.10 Traceability

Traceability ensures that the communication of past activities can be checked. When a problem occurs, an administrator of a P2P network or a peer may need to trace the activity of the same. Traceability provides information concerning past activities, such as the accessed peers, transferred data or messages, etc.

10.11 Traffic control

P2P communications may result in a heavily congested situation. In such cases, traffic control mitigates the congested communication by controlling data or message transfer timing, and adjusting communication speed, etc.

10.12 Relationship between security requirements and security threats

Each security requirement is a countermeasure against certain security threats. The relationship between security requirements and security threats is shown in Table 1. The letter 'X' in a cell formed by the intersection of this table's columns and rows designates that a particular security requirement should be provided in order to remove or mitigate a specific threat.

Table 1 – Relationship between security requirements and security threats

Threats / Requirements	Eavesdropping	Communication jamming	Injection and modification of data	Unauthorized access	Repudiation	Man-in-the-middle attack	Sybil attack
User Authentication				X	X	X	X
Anonymity				X			
Privacy	X						
Data integrity		X	X			X	
Data confidentiality	X					X	
Access control			X	X			
Non-repudiation					X		
Usability				X			
Availability		X					
Traceability		X	X	X			X
Traffic control		X					

11 Security functions for satisfying security requirements of P2P communications

To achieve the security requirements for P2P communications, there are several security functions that may be used as follows:

– encipherment;
– key exchange;
– digital signature;
– trust management;
– access control;
– data integrity mechanism;
– authentication exchange;
– notarization;
– secure routing;
– traffic control mechanism;
– ID assignment.

11.1 Encipherment

The encipherment function can ensure the confidentiality of either communication data or stored data.

Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithms:

a) Symmetric (i.e., secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and

b) Asymmetric (e.g., public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret.

11.2 Key exchange

The key exchange function allows for key sharing in encipherment implementations, especially that of the symmetric encipherment algorithm.

11.3 Digital signature

The digital signature function defines two processes:

a) signing data; and

b) verifying the signed data.

The first process uses information that is private (i.e., unique and confidential) to the signatory. The second process uses procedures and information which are publicly available but from which the signatory's private information cannot be deduced.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signatory's private information as a private key.

The verification process involves the use of public procedures and information to determine whether the signature was produced correctly with the signatory's private information.

The essential characteristic of the signature function is the fact that the signature can only be produced using the signatory's private information. Thus, when the signature is verified, it can subsequently be proven to a third party (e.g. a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

11.4 Trust management

11.4.1 Local recommendation

The trust value of one user is acquired by inquiring of a finite number of other users. In such cases, the simple method of local broadcasting is widely employed. Usually this is suitable for a small scale P2P network, such as a small local area network. For a larger network, such trust values often become significantly biased.

11.4.2 Public key infrastructure

There are a few central nodes supervising the whole network and regularly notifying the errant nodes. The validity and effectiveness of these central nodes is guaranteed by CA issued certificates. This kind of system has central dependency and faces certain problems, such as the ability of extension and the single node invalidation aspect.

11.4.3 Reputation

The peer trust value of a peer node is calculated through the feedback of transactions between each other. The trust value of a user is calculated after evaluation and statistical analysis of such feedback.

11.4.4 Role base

In the role-based P2P trust model, the trust value of a specific peer node determines its user status in the network, and the status of a user can be mapped to its relation with other users. Normally, such a model provides a function to calculate the trust value of each node. It also provides a simple, low-cost algorithm to enable the users to verify the asymmetric trust relationship between two users.

11.5 Access control

The access control function may use the authenticated identity of a user or information about the user (such as membership within a known set of users) or the capabilities of the user, in order to determine and enforce the access rights of the same. If the user attempts to use an unauthorized resource or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail.

The access control function may be based on the use of the following items:

a) access control information bases, where the access rights of peer entities are maintained in a database;

b) authentication information, such as passwords, the possession and subsequent presentation of which is evidence of the accessing user's authorization;

c) capabilities, the possession and subsequent presentation of which is evidence of the right to access the user or resource defined by the capability;

d) security labels, which, when associated with a user, may be used to grant or deny access, usually according to a security policy;

e) time of attempted access;

f) route of attempted access;

g) duration of access; and

h) physical location of attempted access.

The access control function may be applied to either or both users of a communication association.

11.6 Data integrity mechanism

Two aspects of data integrity are considered: the integrity of a single data unit or field, and the integrity of a stream of data units or fields respectively. In general, different technologies are used to provide these two types of integrity function, although the provision of the second without the first is impractical.

Determining the integrity of a single data unit involves two processes: one at the sending entity and one at the receiving entity, respectively. The sending entity appends a quantity to data that is a function of the data itself. This quantity may be supplementary information such as a block check code or cryptographic check value, and may also be enciphered. The receiving entity generates a corresponding quantity and compares its result with the received quantity to determine whether the data have been modified in transit. This process alone will not protect against the replay of a single data unit.

Protecting the integrity of a sequence of data units (i.e., protecting against disorder, loss, replaying and inserting or modifying data) requires the addition of some form of explicit ordering, such as sequential numbering, time stamping, or cryptographic chaining.

11.7 Authentication exchange

Some security technologies that may be applied to authentication exchanges are:

a) the use of authentication information, such as passwords supplied by a sending user and checked by the receiving user;

b) cryptographic technologies; and

c) the use of characteristics and/or possessions of the user.

The authentication exchange function may be incorporated in order to provide communicating user authentication. If the function does not succeed in authenticating the user, this will result in rejection or termination of the connection, and may cause a user to show up on the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e., to ensure liveness).

The choices of security technologies, which are used to realize authentication exchange, will depend upon the circumstances in which they need to be used, alongside:

a) time stamping and synchronized clocks;

b) two- and three-way handshakes (for unilateral and mutual authentication respectively); and

c) non-repudiation functions achieved by digital signature and/or notarization mechanisms.

11.8 Notarization

The property of the data communicated between two or more users, such as its integrity, origin, time and destination, can be assured by the provision of a notarization function. The assurance is provided by a third-party notary, which is the trusted communicating entities trust, and which holds the necessary information to provide the required assurance in a verifiable manner. Each instance of communication may use digital signature, encipherment, and integrity functions, as appropriate, to the service being provided by the notary. When such a notarization function is invoked, the data are communicated between the communicating users via the protected instances of communication and the notary.

11.9 Secure routing

In case of P2P communications, the routing function is provided by each peer. In other words, when a peer receives messages or data, the peer forwards the messages or data to other peers according to the routing information. If a malicious peer abuses this routing function, the P2P network may be stopped. Otherwise, the malicious peer can obtain various messages or data by controlling the routing information.

In order to prevent this situation, a secure routing function can be applied. This function protects against incorrect routing information that may be generated by the malicious peers.

11.10 Traffic control mechanism

The traffic control function is used to prevent the congestion of messages or data transfer. It is also used to prevent access concentration to one peer.

11.11 ID assignment

In order to distinguish each peer and information, all peers and information are assigned a unique ID. Because there are no centralized servers in the case of pure P2P service models, such IDs are assigned by agreement of peers. If an ID assignment mechanism is not secure, malicious peers may attack the P2P communications using fake IDs. A secure ID assignment function is therefore used to protect against the misuse of assigned IDs and abuse of illegal IDs.

11.12 Relationship between security requirements and functions

These security functions are used to satisfy some of the security requirements. The details as to which functions satisfy which security requirements are shown in Table 2. The letter 'X' in a cell formed by the intersection of this table's columns and rows designates that a particular security function should be provided in order to satisfy a specific requirement.

Table 2 – Relationship between security requirements and functions

Functions / Requirements	Encipherment	Key exchange	Digital signature	Trust management	Access control	Data integrity mechanism	Authentication exchange	Notarization	Secure routing	Traffic control mechanism	ID assignment
User Authentication	X	X	X	X	X		X				X
Anonymity	X			X							X
Privacy	X				X		X				
Data integrity	X	X	X		X	X	X				
Data confidentiality	X	X			X		X				
Access control					X		X				X
Non-repudiation			X				X	X			X
Usability					X						
Availability					X		X		X	X	
Traceability			X						X		X
Traffic control		X								X	

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009