

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1036

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

**Framework for creation, storage, distribution
and enforcement of policies for network
security**

ITU-T Recommendation X.1036

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.

ITU-T Recommendation X.1036

Framework for creation, storage, distribution and enforcement of policies for network security

Summary

ITU-T Recommendation X.1036 establishes a set of network security policies that will drive the security controls of a system or a service. It also specifies the framework for the creation, storage, distribution and enforcement of policies for network security that can be applied to various network conditions and devices.

Source

ITU-T Recommendation X.1036 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation 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/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Terms and definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Network security policy.....	3
6.1	Attack detection policy.....	4
6.2	Access control policy	4
6.3	Alert control policy.....	4
6.4	Traffic control policy.....	4
6.5	Routing control policy	4
7	Network security policy information model.....	4
7.1	Class definitions of NSPIM.....	4
7.2	The class hierarchy of NSPIM	28
7.3	Association and aggregation of NSPIM	30
7.4	Relation of Classes	32
8	Network security policy framework	33
8.1	Creation of policies.....	34
8.2	Storage of policies	35
8.3	Distribution of policies	36
8.4	Enforcement of policies.....	37
8.5	An example of policy conversion and distribution.....	38
	Bibliography.....	41

.....

ITU-T Recommendation X.1036

Framework for creation, storage, distribution and enforcement of policies for network security

1 Scope

Most of current security research has been devoted to the development of security systems such as IDS (intrusion detection system) or firewall. Note, however, that those systems that are currently available are not generally interoperable because each system has its own special functionality and control mechanism. This proves to be greatly bothersome to operators who have to control one or more networks including several security systems.

As such, controlling different security systems effectively or easily managing them in a unified manner has become a hot issue. This Recommendation defines the network security policy information model (NSPIM) extended on the basis of policy core information model (PCIM) and PCIM extension (PCIMe) of IETF in representing several policies used in the policy-based network security system. NSPIM is highlighted as a solution for effectively controlling various network devices. NSPIM delivers consistent, unified, and an understandable view of a network without the implementation details. Such benefit of NSPIM is enhanced as the network grows increasingly complex and offers more services. To model the interaction between network elements, services, and clients of the network, the flexible and extensible information model for security policy is required for the design of each component of NSPIM. Management, signalling/control, and user planes as defined in [ITU-T X.805] can be used to determine the necessary controls needed to support a security policy.

The scope of this Recommendation covers the establishment of a set of security policies for protecting the network and proposal of a network security policy framework that creates, stores, distributes and executes these network security policies. The network security policy information model is also introduced to represent the security policies used for intrusion detection and response in several modules in the network security system.

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.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.810] ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.812] ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

- [IETF RFC 3060] IETF RFC 3060 (2001), *Policy Core Information Model – Version 1 Specification*, <<http://www.ietf.org/rfc/rfc3060.txt>>
- [IETF RFC 3460] IETF RFC 3460 (2003), *Policy Core Information Model (PCIM) Extensions*, <<http://www.ietf.org/rfc/rfc3460.txt>>

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 associations: [IETF RFC 3060]

3.1.2 aggregations: [IETF RFC 3060]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 action: This operation is governed by a policy rule. Any action evaluated to be TRUE based on a rule is triggered.

3.2.2 attack: An attack may either be a known attack or an unknown attack. The known attack means that the pattern or packet for attack is opened. Although the pattern or packet for attack is not opened for the unknown attack, it refers to the behaviour related to worsening network situation.

3.2.3 condition: This is an expression of a condition type; its values are used to specify a constraint within a policy rule. A given condition can be negated using the NOT operator.

3.2.4 information model: This is an abstraction and representation of the entities in a managed environment as well as their properties, attributes and operations, and way of relating to each other. It is independent of any specific repository, application, protocol or platform.

3.2.5 policy: A policy defines one or more rules. Each rule binds one or more actions to sets of conditions describing by whom (users), for what (systems, applications), and under what circumstances (time, day of the week, date) the actions may be triggered.

3.2.6 policy conflict: It defines the actions of two rules contradicting each other. The entity implementing the policy will not be able to determine which action to perform. To prevent this situation, the implementers of policy systems must provide conflict detection and avoidance or resolution mechanisms.

3.2.7 role: This is a string characterizing a particular function of a network element or an interface that can be used to identify particular behaviours associated with the element. It is a selector for policy rules to determine the applicability of the rule to a particular network element. Roles abstract the capabilities and/or use of network devices and resources.

3.2.8 rule: This is a policy component that binds an action to the conditions governing whether or not the action is performed. When controlling network resources, the action is usually intended to provide a service. The following is a simplified expression for a rule: IF condition, THEN action.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CIM	Common Information Model
COPS	Common Open Policy Service
DMTF	Distributed Management Task Force

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
LDAP	Lightweight Directory Access Protocol
NSPIM	Network Security Policy Information Model
PBNM	Policy-Based Network Management
PCIM	Policy Core Information Model
PCIMe	PCIM extension
PDU	Policy Decision Unit
PEP	Policy Enforcement Point
PES	Policy Enforcement System
PIB	Policy Information Base
PMU	Policy Management Unit
PR	Policy Repository

5 Conventions

None.

6 Network security policy

The network service and system can be protected by monitoring known attacks blocking harmful packets and limiting traffic congestion. Security policies play an important role in enabling intrusion detection and automated responses. Depending on the role, the network security policy is divided into 5 sub-policies, each of which is expressed as condition/action pairs.

This can be generated by administrators or security managers and enforced by the security agents. The condition attribute and action classified according to the types of policies are shown in Table 1.

Table 1 – Network security policies

Name	Condition attribute	Action
Attack Detection Policy	Packet Header Fields, Packet Payload Fields	Alert Drop
Access Control Policy	Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Direction, TCP 6 Flags, ICMP Type, ICMP Code	Permit Deny
Alert Control Policy	Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Attack ID	Filtering Sampling
Traffic Control Policy	Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Direction	Forward Rate Limit
Routing Control Policy	Destination IP Address	Drop

Attack Detection Policy can be used to detect and mitigate the known attacks. The access control policy, traffic control policy and routing control policy can be used to detect and mitigate the unknown attacks.

6.1 Attack detection policy

In detecting known attacks, the attack detection policy can refer to the attack detection rules from intrusion detection systems. The monitoring device drops a packet and/or sends an alert to the policy server after comparing the packet with the pattern defined in the attack detection rule.

6.2 Access control policy

The access control policy decides on permission or denial for incoming packets to a firewall or a router in accordance with the value of packet header fields.

6.3 Alert control policy

The alert control policy controls the transmission of alerts from IDS. This policy allows a policy enforcement system to send the sample of alerts or to filter alerts.

6.4 Traffic control policy

The traffic control policy prescribes the control against excessive traffic in a router or a traffic control device. This policy limits network traffic and helps increase network performance. In other words, it provides a basic level of security for network access.

6.5 Routing control policy

The routing control policy forwards a packet to a router's bit bucket for manipulating bad traffic. In other words, it discards unwanted packets. This policy works only on the destination address since it is actually part of the forwarding logic.

7 Network security policy information model

The network security policy information model (NSPIM) referred to as a common information model is constructed based on policy core information model (PCIM, [IETF RFC 3060]) and PCIM extension (PCIMe, [IETF RFC 3460]) of IETF in representing the policies used in the policy-based network security system and schema of a policy repository based on NSPIM. PCIM presents the object-oriented information model for representing policy information under joint development in the IETF policy framework working group and as extensions to the common information model (CIM) activity in the distributed management task force (DMTF). NSPIM defines two hierarchies of object classes: structural classes representing policy information and control of policies, and association classes indicating how instances of the structural classes are related to each other. Properly designed and implemented security mechanisms (dimensions), as defined in [ITU-T X.805], can be used to support security policy and facilitate the classes and rules set by security management.

7.1 Class definitions of NSPIM

The classes of CIM and PCIM/PCIMe are not covered by the scope of this Recommendation. Therefore, only newly defined classes in NSPIM are described.

7.1.1 Class "AlertControlRule"

NAME	AlertControlRule
DESCRIPTION	The class is defined for the associated condition and action for alert control
DERIVED FROM	PolicyRule
PROPERTIES	(none)

7.1.2 Class "PacketFilteringRule"

NAME	PacketFilteringRule
DESCRIPTION	The class is defined when dropping or permitting a specified packet or session
DERIVED FROM	PolicyRule
PROPERTIES	FilteringPriority

7.1.2.1 Property "FilteringPriority"

NAME	FilteringPriority
DESCRIPTION	This indicates whether to drop or permit a specified packet or session
SYNTAX	uint16

7.1.3 Class "TrafficControlRule"

NAME	TrafficControlRule
DESCRIPTION	The class is defined for the control of network traffic congestion
DERIVED FROM	PolicyRule
PROPERTIES	(none)

7.1.4 Class "AttackDetectionRule"

NAME	AttackDetectionRule
DESCRIPTION	The class is defined for Attack Detection
DERIVED FROM	PolicyRule
PROPERTIES	IntrusionImpact, Msg, Reference, AttackName, SignatureID, Revision, Priority, ClassType

7.1.4.1 Property "IntrusionImpact"

NAME	IntrusionImpact
DESCRIPTION	This is an enumeration indicating the effect of intrusion
SYNTAX	uint16
VALUES	Very Large (1), Large (2), Middle (3), Small (4), Very Small (5)

7.1.4.2 Property "Msg"

NAME	Msg
DESCRIPTION	This property is used to describe the contents of detection rules
SYNTAX	string

7.1.4.3 Property "Reference"

NAME	Reference
DESCRIPTION	This property presents the system referred to in detection rules
SYNTAX	string

7.1.4.4 Property "AttackName"

NAME	AttackName
DESCRIPTION	This property presents the name of the attack
SYNTAX	string

7.1.4.5 Property "SignatureID"

NAME	SignatureID
DESCRIPTION	This property is used for an identifier of the attack signature
SYNTAX	uint16

7.1.4.6 Property "Revision"

NAME	Revision
DESCRIPTION	This property is used to identify the revision of the rules
SYNTAX	uint32

7.1.4.7 Property "Priority"

NAME	Priority
DESCRIPTION	This property is used to present the priority of the rules
SYNTAX	uint32

7.1.4.8 Property "ClassType"

NAME	ClassType
DESCRIPTION	This property presents the category where the rule belongs
SYNTAX	uint32

7.1.5 Class "RoutingControlRule"

NAME	RoutingControlRule
DESCRIPTION	The class is defined for the routing control
DERIVED FROM	PolicyRule
PROPERTIES	(none)

7.1.6 Class "AlertControlCondition"

NAME	AlertControlCondition
DESCRIPTION	The class is defined for filtering alerts. The AlertControlCondition class instance consists of combinations of the source IP address, destination IP address, source port, destination port, protocol and attack ID.
DERIVED FROM	CompoundPolicyCondition
PROPERTIES	(none)

7.1.7 Class "PacketFilteringCondition"

NAME	PacketFilteringCondition
DESCRIPTION	The class represents the condition of an access control policy for special packets or sessions. The PacketFilteringCondition class instance consists of combinations of the source IP address, destination IP address, source port, destination port, protocol, direction, TCP flags, ICMP type and ICMP code.
DERIVED FROM	CompoundPolicyCondition
PROPERTIES	(none)

7.1.8 Class "TrafficControlCondition"

NAME	TrafficControlCondition
DESCRIPTION	The class is defined for congested traffic control. The TrafficControlCondition class instance consists of combinations of the source IP address, destination IP address, source port, destination port and protocol.
DERIVED FROM	CompoundPolicyCondition
PROPERTIES	(none)

7.1.9 Class "RoutingControlCondition"

NAME	RoutingControlCondition
DESCRIPTION	The class is defined as a condition of routing control rule. The RoutingControlCondition class instance consists of the destination IP address.
DERIVED FROM	CompoundPolicyCondition
PROPERTIES	(none)

7.1.10 Class "PacketMonitoringCondition"

NAME	PacketMonitoringCondition
DESCRIPTION	The class is defined for the condition of AttackDetectionRule. This PacketMonitoringCondition consists of DetailedPacketFilter and/or ExtendedHeaderFilter through FilterList association.
DERIVED FROM	PolicyCondition
PROPERTIES	(none)

7.1.11 Abstract Class "AlertControlAction"

NAME	AlertControlAction
DESCRIPTION	The class is an abstract class for alert transmission
DERIVED FROM	PolicyAction
PROPERTIES	(none)

7.1.12 Class "AlertSamplingAction"

NAME	AlertSamplingAction
DESCRIPTION	The class represents an action that aggregates the same alerts and transmits the alert
DERIVED FROM	AlertControlAction
PROPERTIES	TimeInterval

7.1.12.1 Property "TimeInterval"

NAME	TimeInterval
DESCRIPTION	This property presents the collection time of the associated information
SYNTAX	uint16

7.1.13 Class "AlertFilteringAction"

NAME	AlertFilteringAction
DESCRIPTION	The class is defined for the alert filtering action
DERIVED FROM	AlertControlAction
PROPERTIES	(none)

7.1.14 Class "PacketFilteringAction"

NAME	PacketFilteringAction
DESCRIPTION	This class is defined when representing for packet filtering action
DERIVED FROM	PolicyAction
PROPERTIES	AccessStatus

7.1.14.1 Property "AccessStatus"

NAME	AccessStatus
DESCRIPTION	This indicates whether to block or permit a specified packet or session
SYNTAX	uint16
VALUES	1[Permit], 2[Block]
DEFAULT VALUE	2[Block]

7.1.15 Class "TrafficControlAction"

NAME	TrafficControlAction
DESCRIPTION	This class is defined for traffic control
DERIVED FROM	PolicyAction
PROPERTIES	AverageRate, PacketRate, NormalBucket, ExtendedBucket, ConformAction, ExceedAction, AccessControlAction

7.1.15.1 Property "AverageRate"

NAME	AverageRate
DESCRIPTION	This is a non-negative integer for the average number of bits per second
SYNTAX	uint16
DEFAULT VALUE	0

7.1.15.2 Property "PacketRate"

NAME	PacketRate
DESCRIPTION	This is a non-negative integer for the average number of packets per second
SYNTAX	uint16
DEFAULT VALUE	0

7.1.15.3 Property "NormalBucket"

NAME	NormalBucket
DESCRIPTION	This is a non-negative integer for the size of a normal bucket
SYNTAX	uint16
DEFAULT VALUE	0

7.1.15.4 Property "ExtendedBucket"

NAME	ExtendedBucket
DESCRIPTION	This is a non-negative integer for the size of an extended bucket
SYNTAX	uint16
DEFAULT VALUE	0

7.1.15.5 Property "ConformAction"

NAME	ConformAction
DESCRIPTION	This property presents the action for conformity. It passes or drops the excess size of the normal bucket
SYNTAX	uint16
VALUES	1[Pass], 2[Drop]
DEFAULT VALUE	1[Pass]