

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1125

(01/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Correlative Reacting System in mobile data communication

Recommendation ITU-T X.1125

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.1125

Correlative Reacting System in mobile data communication

Summary

In a mobile network environment, while core networks are able to manage security threats, mobile stations (MSs) that access the mobile network have little defence capability due to limited hardware resources. Compromised mobile stations can themselves easily become virus agents and threaten the entire network. The Correlative Reacting System (CRS) defined in this Recommendation aims to protect mobile networks against the threats of insecure terminals that do not conform to the security policy of the network, such as terminals that have been compromised.

Source

Recommendation ITU-T X.1125 was approved on 13 January 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/>.

© 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	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	Conventions	6
6	Overview of the Correlative Reacting System	6
7	CRS description.....	8
7.1	Preconditions	8
7.2	CRS objectives	8
7.3	CRS system architecture.....	9
7.4	CRS entities	10
7.5	CRS interfaces.....	14
8	CRS policy.....	15
8.1	Security evaluation policy	15
8.2	Security control policy	18
8.3	Group attribute management	21
9	Communication between SCA and SCS	22
9.1	Message carrier protocol	22
9.2	Security	22
9.3	Messages.....	22
10	Communication between the NAC/ASC and the SCS	25
10.1	General	25
10.2	Message security	25
10.3	Messages.....	25
11	General procedures in CRS	27
11.1	The discovery of SCA/SCS	27
11.2	SCI report and MS control procedure	28
11.3	SCA auto-installation and auto-updating	30
11.4	Generation and delivery of control policy	32
11.5	MS security updating.....	32
11.6	MS leave data network	34
12	Special processing procedures.....	34
12.1	Large-scale updating	34

	Page
13 Handling CRS roaming	38
13.1 CRS roaming definition.....	38
13.2 CRS roaming within one CRS-deployed network.....	38
13.3 CRS roaming between CRS-deployed networks.....	39
13.4 CRS roaming between CRS-deployed network and CRS-undeployed network	41
Annex A – CRSAP messages	42
A.1 XML schema definition.....	42
A.2 The equivalent ASN.1 specification of the CRSAP messages.....	44
Appendix I – Some considerations on CRS implementation.....	48
I.1 Deployment of SCA	48
I.2 Deployment of SCS.....	50
I.3 Deployment of CRS in mobile IP networks	52
Appendix II – An example of CRSAP message exchange	53
II.1 An example SCI report.....	53
II.2 An example SCI response	53
Bibliography	54

Recommendation ITU-T X.1125

Correlative Reacting System in mobile data communication

1 Scope

Focusing on end-to-end data communication in mobile networks, this Recommendation describes the open architecture of the Correlative Reacting System (CRS), which protects the network against potential security threats from insecure mobile terminals. This architecture provides operator networks with enhanced security capability through mobile station (MS) security updates, network access control and application service restrictions. This results in a mechanism that prevents viruses or worms from spreading rapidly through the network operator.

This Recommendation provides an abstract level architecture and is an application of current implementation-level protocols in the wired/PC world, e.g., trusted network connection (TNC) specifications for the mobile network scenario. Where appropriate, existing proven concepts and elements from the wired world should be reused as much as possible in the design and implementation of CRSs.

This Recommendation specifies Correlative Reacting System application protocol (CRSAP) messages which can be transferred using XML or compact binary encodings as specified in Annex A.

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.680] Recommendation ITU-T X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- [ITU-T X.691] Recommendation ITU-T X.691 (2002) | ISO/IEC 8825-2:2002, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.
- [ITU-T X.693] Recommendation ITU-T X.693 (2001) | ISO/IEC 8825-4:2002, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.
- [ITU-T X.694] Recommendation ITU-T X.694 (2004) | ISO/IEC 8825-5:2004, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.
- [ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

- [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.
- [RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.
<<http://www.ietf.org/rfc/rfc2748.txt>>
- [W3C XSD] W3C XML Schema (2004), *XML Schema Part 0: Primer Second Edition*.
<<http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [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 application service [ITU-T X.1121]: A service like mobile banking, mobile commerce, and so on.

3.1.3 application server [ITU-T X.1121]: An entity that connects to an open network for data communication with mobile terminals.

3.1.4 application service provider (ASP) [ITU-T X.1121]: An entity (person or group) which provides application service(s) to mobile users through an application server.

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

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

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

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

3.1.9 privacy [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 rights of individuals, it cannot be very precise and its use should be avoided except as motivation for requiring security.

3.1.10 mobile network [ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

3.1.11 mobile security gateway [ITU-T X.1121]: An entity which relays data communication between a mobile terminal and an application server, changes security parameters or communication protocol from a mobile network to an open network, or vice versa, and can perform security policy management functions for mobile end-to-end data communication.

3.1.12 mobile terminal [ITU-T X.1121]: An entity that has wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

3.1.13 mobile user [ITU-T X.1121]: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

3.1.14 system security function [ITU-T X.803]: A capability of a system to perform security-related processing, such as encipherment/decipherment, digital signature, or the generation or processing of a security token or certificate conveyed in an authentication exchange.

3.1.15 security communication function [ITU-T X.803]: A function supporting the transfer of security-related information between open systems.

3.1.16 security transformation [ITU-T X.803]: A set of functions (system security functions and security communication functions) which, in combination, operate upon user data items to protect those data items in a particular way during communication or storage.

3.1.17 threat [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 application service controller (ASC): A mobile network element that performs application service access control on mobile subscribers. By correlatively reacting with the security correlation server (SCS), it imposes service restrictions on specified unsafe users based on the application service control policy of CRS.

3.2.2 controlled object: The mobile station (MS) controlled by the CRS. A controlled object may be a single MS or a group of MSs.

3.2.3 Correlative Reacting System (CRS): A mechanism that enables mobile terminals or devices and the network to cooperate together against potential security threats, such as viruses, worms, Trojan-horses, user misbehaviour and other network attacks.

3.2.4 Correlative Reacting System application protocol (CRSAP): An application layer protocol for CRS message encapsulation and transport between the SCA and the SCS.

3.2.5 dedicated security device (DSD): A device that provides dedicated security functions for the network (e.g., firewalls, IDs, security gateways, and security management servers).

3.2.6 mobile station (MS): Any mobile device, such as a mobile handset or computer, which is used to access network services.

3.2.7 mobile station operating system (MSOS): Functionality that can automatically perform self-update, patch installation or SAS updating in cooperation with the MSOS-US and the SAS-US according to SCS instructions received by the SCA.

3.2.8 mobile station operating system updating server (MSOS-US): A server that provides service patches, software updates, and upgrades for the MSOS.

3.2.9 network access controller (NAC): A mobile network element that provides control of user access to the network. It has the capability to perform data-bandwidth-access limitation upon a specified unsafe user, according to network access control policies. The network access device is normally a network gateway, e.g., SGSN in the mobile network.

3.2.10 policy: A collection of rules applied in CRS to enforce the proper control on MSs.

3.2.11 security application software (SAS): Software that provides a specific class of security function for a terminal or device within the network system. For example, anti-virus software.

3.2.12 security application software updating server (SAS-US): A server which is located on the network side to provide security files or profile updating and other online security services to terminals or devices.

3.2.13 security correlation agent (SCA): A module embedded in mobile terminals to collect the security-related environmental information, to communicate with the security correlation server (SCS) in the mobile network for security evaluation, and to provide the terminal or device with updated security information.

3.2.14 security correlation information (SCI): Information correlated with the security environment for mobile terminals or devices, such as the version control of the operating system and anti-virus software used in the mobile terminal or device.

3.2.15 security correlation server (SCS): A server in a mobile network that communicates with the security correlation agent (SCA) for evaluating the security degree and environment of mobile terminals or devices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and accounting
API	Application Programming Interface
ASC	Application Service Controller
ASP	Application Service Provider
CN	Core Network
COPS	Common Open Policy Service
COS	Chip Operating System
CRS	Correlative Reacting System
CRSAP	Correlative Reacting System Application Protocol
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSD	Dedicated Security Device
GGSN	Gateway General Packet Radio System Support Node
GPRS	General Packet Radio System
H-ASC	Home Application Service Control
H-NAC	Home Network Access Control
H-SCS	Home Security Correlation Server
HLR	Home Location Register
Ic	CRS communication Interface between SCA and SCS
Ica	Communication interface between SCA and other SAS
Ics	CRS communication interface between SCS and NAC/ASC
IP	Internet Protocol
IPSec	Internet Protocol Security
L1	Layer one, i.e., physical layer

L2	Layer two, i.e., data link layer
MS	Mobile Station
MSOS	Mobile Station Operating System
MSOS-US	Mobile Station Operating System Updating Server
NAC	Network Access Controller
OS	Operating System
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
P-TMSI	Packet TMSI
QoS	Quality of Service
RAN	Radio Access Network
RBAC	Role-Based Access Control
SAS	Security Application Software
SAS-S	Security Application Software Server
SAS-US	Security Application Software Updating Server
SCA	Security Correlation Agent
SCI	Security Correlation Information
SCS	Security Correlation Server
SDB	Security Data Base
SGSN	Serving General Packet Radio System Support Node
SIM	Subscriber Identity Module
SOC	Security Operation Centre
SUS	Security Updating Server
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Station Identity
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
V-ASC	Visited Application Server Control
V-NAC	Visited Network Access Control
V-SCS	Visited Security Correlation Server
WLAN	Wireless Local Area Network
XSD	eXtensible Markup Language Schema Definition
WiMAX	Worldwide Interoperability for Microwave Access

WTLS	Wireless Transport Layer Security
XML	eXtensible Markup Language

5 Conventions

None.

6 Overview of the Correlative Reacting System

Along with the popularization of wireless data networks, an increasing number of people use mobile terminals to enjoy new network services. Packet data services will eventually replace the traditional circuit-switched services; meanwhile, mobile telecommunication networks tend to be unified IP-based networks. The traditional specifications for security mechanisms proposed by 3GPP, WLAN and WiMAX ensure the security of user access, authentication and message transmission. However, application layer threats (e.g., viruses, worms, hacker attack, and hijacking user information) are still emerging endlessly, which result from the openness of mobile network architecture and the inherent security vulnerabilities of IP technology. Since every node/host/user is equal, there exists a risk that one compromised node can threaten the whole network. Unfortunately, the security mechanisms referred to in this Recommendation cannot deal with these problems.

It is easy to manage the security threats from inside operator core networks, but it is difficult to do this from mobile stations that have access from the core network or via the access network. Due to the limited resource, mobile stations (MSs) have little defence ability. Hence, if the operating system (OS) or security application software (SAS), e.g., host firewall is not updated in a timely manner, the MS will be more vulnerable to a successful virus attack. Furthermore, if an MS with significant mobility becomes virus-infected, it could itself become a virus vector and endanger the network operator. Therefore, it is very difficult for the operator to make an appropriate compromise between network security guarantees and high services-quality guarantees for the users.

In the field of classical wired networks, the specifications of trusted network connect (TNC) architecture processed by Trusted Computing Group (TCG) provide terminal integrity for a host (e.g., a personal computer) that accesses a network, i.e., only those who are authenticated on the network side and conform to network security policy are allowed access to the network. However, there is little consideration of the problems that are specific to a mobile network, such as mobility, roaming, hardware capability of terminals, and unreliability of the link via air interface, etc. Referring to the end-to-end security features of mobile data services described in [ITU-T X.1121], the proper service features of the mobile network user will require further consideration. For example, after an MS is infected by some viruses or worms, it may send junk messages or attack messages to the data network, which can result in unreasonable charges, or sharply reduce the capability of the mobile network or cause other problems. In addition, there can be other issues, such as the split between SIM card and mobile terminal, as well as the independent wireless access protocol. These issues will also require further consideration.

Due to the rapid development of wireless applications and the increasing number of the third party ASPs, business tends to focus on value-added services and sophisticated management. As a result, there is an increasing number of threats against MSs and mobile networks, while mobile subscribers are using diverse services. For example, a corporation may disclose the interior resources to unauthorized users, such as the identity of an employee who accesses the Intranet via wireless network. Furthermore, there is the potential for application systems to be abused or to be destroyed, resulting in a reduction in application quality or unavailability of the application.

Because of rapid development, virus technology can generate mass traffic in a network when a virus breaks out in large scale. The mass traffic resulting from junk data or attack traffic flow will have a severe negative impact on the efficiency and the security of the operator's network and will also negatively impact the security and the application of mobile users.

The Correlative Reacting System (CRS) aims to protect mobile networks against the threats of insecure terminals that do not conform to the network security policy, such as the terminals that are virus-infected or that have been otherwise compromised. Meanwhile, CRS also aims to prevent the MSs from becoming infected through periodical evaluation and updating of the MS's security configuration and through assisting those virus-infected MSs to recover.

Attacks can be divided into two categories: network-layer-based network attacks and application-layer-based service attacks. The former take place during the course of establishing a wireless network connection and before the network provides the application service; the latter happen after the wireless connection is established and during the period of service. Such division of attacks into two main categories is to emphasize that CRS can provide different types of access control services: access to the network bearer resources; and access to the network service resources via NAC and ASC, respectively. Similar to the PC/wired world, the main purpose of CRS is to counter the network attacks limited to connection establishment. However, through periodical SCI reports (see clause 8.2.3, SCI report policy) and evaluation of the terminal security status, CRS can support the capability for the network operator to counter other attacks such as those during communication (and even some system attacks) by virtue of the collected user terminal security information.

To resist the threats resulting from insecure terminals, CRS provides multi-layer access controls: network access control (NAC) and application service control (ASC) to ensure that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications (see [ITU-T X.805]). These two types of control complement each other. In one instance, NAC supplements the limitations of ASC and effectively controls the risk from the complex mechanisms such as network worms and hacker attacks. In the other instance, ASC makes it possible to limit the impact on network traffic that is caused by an attack against some specific network service(s) as well as to prevent the spread of any infection.

Aiming at the mobile end-to-end application data service, the CRS establishes an infrastructure to protect against the threats described as follows:

- for the mobile subscriber, compromise of private information of the subscriber; and abuse of subscriber toll services;
- for the terminal system, protects against the mobile station becoming a denial of service (DoS) attack agent when the MS system is defective or unavailable;
- for the mobile network system, protects against the spread of viruses or worms that cause network congestion and waste network resources (i.e., QoS reduction); and
- for the application service system, loss of availability of application and server services due to service layer attacks or virus infection in the server or the MS; unauthorized disclosure of subscriber information; and integrity impairment.

The essence of CRS is to control network access and to restrict access to the application services of mobile stations by correlatively reacting between mobile stations and the network, so that the CRS can provide the network with the capability to counter network threats such as viruses and other network attacks.

The global AAA architecture defined in [b-IETF RFC 2903], [b-IETF RFC 2904], [b-IETF RFC 2905] and [b-IETF RFC 2906] has some relationship with CRS in that they share common user information. The CRS procedures should be combined with AAA-related authentication and authorization procedures, usually after the AAA user authentication and before authorization to the terminal to access the network resources. However, such issues should be considered in the implementation phase of CRS and this is currently out of the scope of this Recommendation.

7 CRS description

7.1 Preconditions

The implementation and the performance of CRS services rely on the correlative reacting cooperation with a number of other external functions as described below:

- the network can enforce network access control for the network based on the network layer;
- the network can enforce control on application service access for the network based on the application layer;
- the security application software updating servers (SAS-USs) and mobile station operating system updating servers (MSOS-USs) can provide automatic and timely security updating services for user terminals¹;
- dedicated security devices (DSD) deployed on the network side can provide specialized security functions for the network. Examples of DSDs include firewalls, security gateways, security operation centres (SOCs) and intrusion detection and prevention systems;
- the security application software (SAS) can provide the security correlation agent (SCA) with particular security information about the terminal, and can automatically perform security updating in cooperation with an SAS-US according to CRS instructions; and
- The mobile station operating system (MSOS) can provide the terminal's security-related system configuration information, and can automatically perform security updating in cooperation with the MSOS-US according to CRS instructions.

The entities that can achieve these external functions are able to communicate with CRS entities (e.g., SCA and the security correlation server (SCS)) via the interfaces defined in this Recommendation and it is assumed that the entities, in cooperation with CRS, can enforce CRS security policies via the interfaces.

In addition, the transmission of a CRS message is based on current transport layer protocols, e.g., TCP and UDP; while, the security of the CRS message is protected by security protocols, e.g., TLS (see [b-IETF RFC 4261]), IPSec (see [b-IETF RFC 4301]), and WTLS (see [b-OMA WTLS]).

7.2 CRS objectives

The following objectives are used to guide the design of CRS:

- by using real-time security evaluation of the terminal side of the air interface and real-time control on the MS, the CRS has the ability to limit the spread of network threats, and thus assure the security of the network;
- the network side of the air interface assists MSs in related security updating;
- the CRS has the ability to ensure that mobile data service and CRS message transmission can keep running as normal while the MS moves between CRS-enabled network and a network that does not have CRS enabled;
- the CRS has the ability to guarantee the availability of the SCA. Specifically, the CRS must detect the SCA configuration when an MS connects to the network. If the MS is not SCA-enabled, the SCA should be installed and enabled. If the MS is SCA-enabled, the CRS must keep the SCA up to date; and

¹ Unless otherwise noted, the term *security updating* in this Recommendation means software updating and upgrading, which includes program updating, program upgrading, patch installation, and so on.

- one SCS may simultaneously control a single or multiple NAC/ASCs. Each NAC/ASC has a default SCS to connect, but one NAC/ASC must simultaneously connect to multiple SCSs. This will allow security policy to be enforced without interruption even if the default SCS encounters problems.

7.3 CRS system architecture

The aim of the Correlative Reacting System is to solve the potential security threats against mobile networks that are caused by insecure mobile stations. Based on the security evaluation of the MS, the CRS can direct network equipment to process network access control and application control on the MS, and to assist the MS in related security updating. The CRS provides both the mobile network and the MS with some specific security enhancements. Furthermore, CRS provides a mechanism to limit the spread of network security threats, such as viruses and worms.

Figure 1 illustrates the CRS architecture and environment.

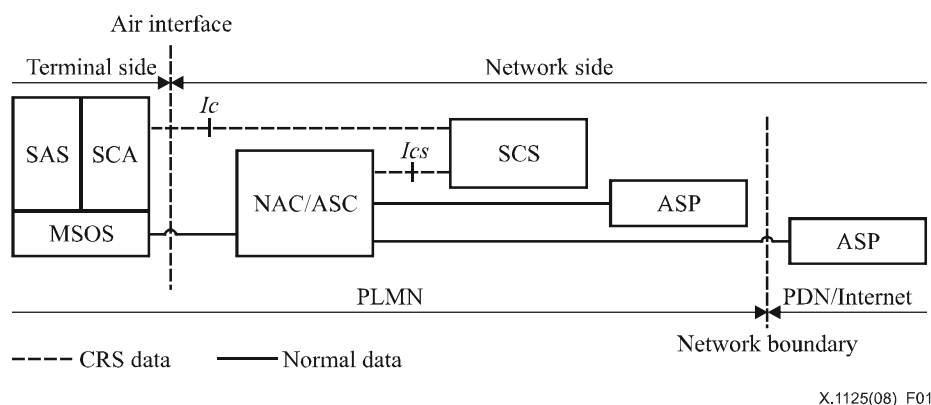


Figure 1 – CRS architecture and its environment

A CRS system comprises four entities:

- a security correlation agent (SCA). The SCA is installed on the MS;
- a security correlation server (SCS). The SCS processes the control on the NAC/ASC and SCA;
- a network access controller (NAC). The NAC executes the control on the MS network access; and
- an application service controller (ASC). The ASC executes the control on the MS application service access.

The SCA lies in the terminal side, while the SCS, NAC, and ASC are located in the network side.

The SCA communicates with the SCS via the interface I_c (see clause 7.5.1), and the SCS communicates with other network elements via the interface I_{cs} . By their communication and interaction, the CRS provides the function of security-focused control on mobile stations.

The SCA is responsible for collecting security-related environmental information and communicating it to the SCS. This collection is essential for the SCS to evaluate the terminal's security level and to further determine what network services can be accessed.

After receiving the SCA security report on the mobile terminal, the SCS carries out the evaluation for the MS. If it decides that the terminal is not secure enough, the SCS will notify the SCA and request the NAC or ASC to enforce the specified user control policy (see clause 8.2.2). In addition, if the SCS decides that the terminal needs upgrading, a process that relies on the SAS-US or MSOS-US, the SCS will instruct the SCA to initiate the necessary upgrading immediately.

If there are applicable security updates, such as OS patches, component updates or security-related patches for the application software, the SCS must direct the SCA to assist the MS in processing related upgrading or updating. All update programs are stored in the SAS-US and the MSOS-US, which also provides a security updating service.

The updating of the SCA is also closely associated with the MS's security. When the SCS detects that the SCA's software is not the latest applicable version, it will instantly inform the SCA and instruct the SCA to upgrade or update the software.

As shown in Figure 1, application service providers (ASPs) may deploy their own services in a mobile network, while the operator of the mobile network can also be considered as an ASP. These ASPs should configure their *Ics* interface, via which they can communicate with the SCS and acquire some information (such as a list of insecure mobile stations). In this way, it is possible for the ASP server to enforce application access control.

Network access or application service access control on mobile users is achieved through the SCS's control on the user's mobile station. Related security information is primarily acquired from the SCI report sent from the SCA to the SCS. For those SCA-enabled mobile stations, the SCA will be initiated as soon as the MS connects to the data network.

Practical network entities functioning with the CRS include, but are not limited to, the following dedicated security devices (DSD):

- firewalls (provide security protection for network boundary);
- security gateways (terminate connections and operate as proxies);
- security management servers (provide knowledge of network side and the support of policy for the SCS); and
- intrusion detection and prevention systems, anomaly detection systems (analyse network traffic, detect network intrusion or attack, and filter its virus traffic or attack traffic).

7.4 CRS entities

7.4.1 Security correlation agent (SCA)

7.4.1.1 Functions of a security correlation agent

Figure 2 shows the functional structure of a security correlation agent.

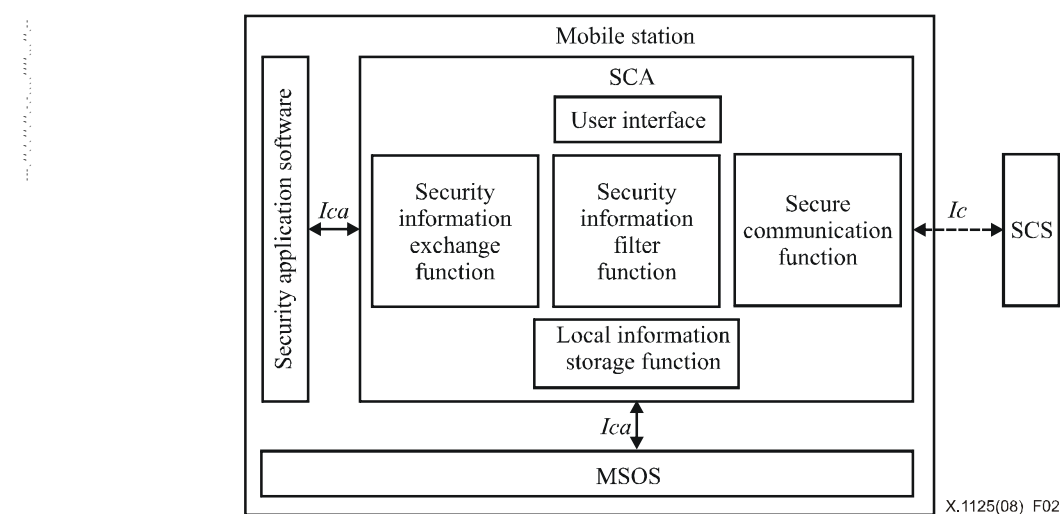


Figure 2 – SCA functions

The SCA has five primary functions as described below:

1) *Exchange security-related information*

The SCA collects security-related information from the MS. This information includes: MS security events; the OS version and patch; the version of the SAS; SAS log information; the mobile user's ID; and the MS's ID, etc. Based on security upgrading information and information received from the SCS, the SCA provides the MS's OS and security application software with security updates or upgrading information via the interface *Ica*. In the real world, security application software has its own update/upgrade channel. *Ica* is a logical interface which can be used to bear such a SAS-specific message exchange channel.

2) *Analyse and filter information*

According to local policy or policy received from the SCS, the SCA is able to process and organize the MS security-related information, which will be filtered and reported to the SCS. Meanwhile, the SCA also has the ability to receive the information from the SCS, which includes security status and upgrading information, the result of the security evaluation of the MS, and access control information, etc. After filtering, the information must be reported to the mobile user or must generate a local security report/log, that can be queried by the user.

3) *Secure communication*

This function is responsible for the security transformation, the mutual authentication with the SCS, and to negotiate and establish the secure communication tunnel with the SCS, and thus ensure that the transmission of the CRS message between the SCA and the SCS is reliable.

4) *User interface*

This function enables information to be exchanged between the user and the SCA, providing the user with security-related information and enabling the user to query security-related information, including the SCI report, and the security evaluation result, etc. The SCA has the capability to generate a MS security status report for each user query based on the collected MS security-related information and the SCS. Generally, the security status report is stored as an SCA running log. If the SCS decides that the MS has a lower security level or if severe security events happen on the MS, the SCA can notify the user in order to alert the user to possible threats.

5) *Local data storage*

This function stores SCA-related security information, logs and various policies.

7.4.1.2 Requirements for the security correlation agent (SCA)

The SCA has the capability to:

- collect security-related information from the mobile station;
- report MS security-related information to the security correlation server (SCS);
- automatically discover the existence of the SCS;
- respond to SCS messages;
- report related information to the user when necessary;
- assist mobile terminals in updating OS and security-related software;
- guarantee the authenticity of data from the *Ica* interface;
- guarantee the confidentiality and integrity of locally-stored information; and
- forbid the user to modify the configuration of the SCA.

NOTE – The configuration can be dynamically modified only by the SCS according to the evaluation of the security conditions of both the MS and the network.

7.4.2 The security correlation server (SCS)

7.4.2.1 Functions

The security correlation server (SCS) is a logical entity comprising several functional modules as follows, each of which can be physical equipment. The SCS functional architecture is described in Figure 3.

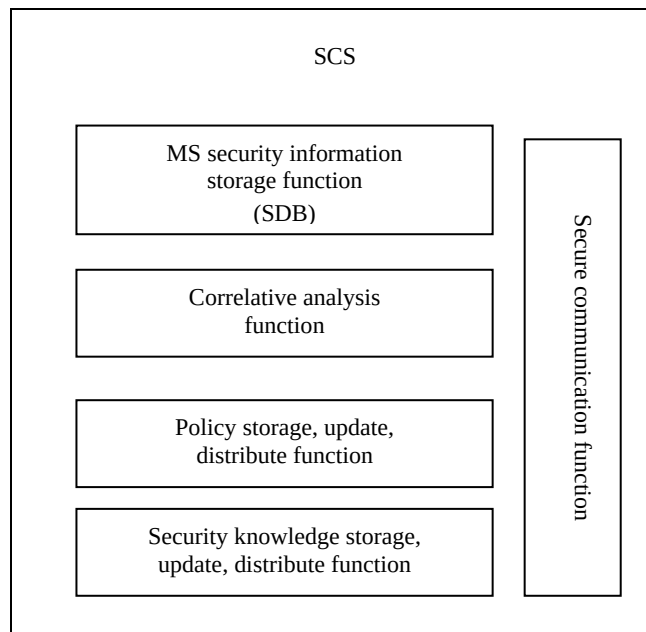


Figure 3 – SCS functions

The SCS has five primary functions as described below:

1) *Communication function*

This function is responsible for establishing a reliable and secure tunnel between the SCS and the SCA, as well as between the SCS and NAC/ASC. It guarantees the integrity and the confidentiality of the CRS messages. It also enables the information exchange among different SCS functional modules.

2) *Storage function of MS security-related information*

The SCS comprises one security database (SDB). This database is used to store SCI reports sent by the SCA, the security evaluation result of the MS and the current active control policy for MSs. There may be one particular sub-database to describe the current and historical relationship among mobile user identities, mobile terminals, and SCA IDs.

3) *Correlative analysis*

According to the stored security policy and security knowledge, the SCS utilizes SCI reports to evaluate the security level of a single MS. Furthermore, the SCS may determine the security condition of certain areas of a mobile data network by correlatively analysing SCI reports sent from multiple MSs and the security evaluation result of a single MS.

4) *Storing, updating and delivering policy*

The policy comprises policy for system control and policy for security evaluation (see clause 8.1). The policy should be defined and stored in the SCS. Utilizing the SCS communication function, the SCS can deliver the policy to the SCA, NAC and ASC. These policies are then used to guide their behaviours. An interface for policy management should be provided to help either administrators or the exterior policy management unit to update the stored policy, either manually or automatically.

5) *Storing, updating, and delivering security knowledge*

Security knowledge comprises all security knowledge and information provided by the network side of the air interface. It includes:

- i) diverse and known network security threats and their solutions;
- ii) patches, information about the upgrading package and the URL of the resource for MSOS;
- iii) patches, information about the upgrading package and the URL of the resource for MS security-related software; and
- iv) SCA version information and the URL for download.

For the CRS, it is very important to keep security knowledge updated. Security knowledge affects how fast the CRS can react to known security threats. OS producers, SAS producers and third party security research institutions should provide most of security knowledge for the CRS.

Security knowledge is used to guide the MS process security-related updating. Meanwhile, it acts as reference information that is utilized for SCS correlative analysis and for constituting security policy.

An example of the SCS protocol stack structure is illustrated in Figure 4. The SCS has a static IP address in the core network (CN). This IP address is used by the SCS for communication within the core network area. Moreover, the SCS has another kind of IP address. Above the layer of tunnel protocol, the SCS has some other static IP addresses (IP1 for PDN1, IP2 for PDN2, ..., IPn for PDNn). Each IP address is associated with one PDN which is directly connected to the mobile network or core network. These IP addresses are used by the SCS to communicate with mobile stations or with network elements accessing or belonging to the associated PDN. The packets of this kind of communication are encapsulated as tunnel protocol (IP-in-IP encapsulation) packets within the core network area and are unencapsulated into normal IP packets outside the core network area.

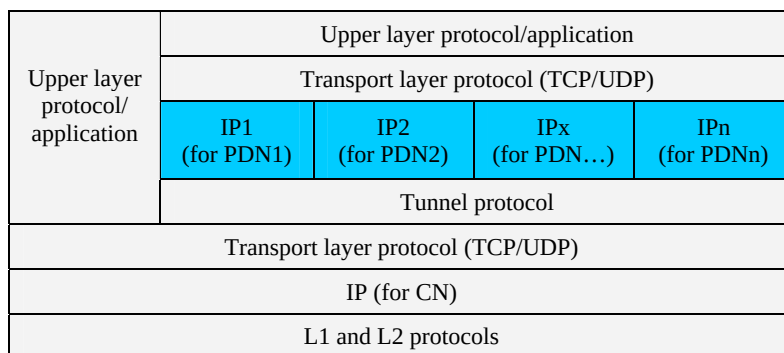


Figure 4 – SCS's protocol stack structure

7.4.2.2 Requirements for the security correlation server

The SCS has the capability to:

- acquire security-related information of the MS;
- acquire security policy and security knowledge on the network side;