Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	6N15587
Date:	2013-03-11
Replaces:	
Document Type:	Text for PDTR ballot
Document Title:	Text for PDTR ballot of ISO/IEC 29181-5, Future Network: Problem Statement and Requirements - Part 5: Security
Document Source:	Project editor
Project Number:	
Document Status:	SC 6 NBs are requested to cast a vote on the SC 6 e-balloting system no later than 2013-06-11.
Action ID:	LB
Due Date:	2013-06-11
No. of Pages:	13

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)
Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;
Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

6N15587

13-7LON-12

ISO/IEC JTC 1/SC 6

TELECOMMUNICATION AND INFORMATION EXCHANGE BETWEEN SYSTEMS

Title:	Text for DTR ballot of ISO/IEC 29181-5, Future Network: Problem Statement and Requirements - Part 5: Security
Source:	Editors
Contact:	Yadong Liu (ydliu915@vip.sina.com, China) Mang Hao (wanghaonet@163.com, China)
SC/WG:	ISO/IEC JTC 1/SC 6/WG 7
Type:	Output Document

Summary:

This is the text for PDTR ballot of ISO/IEC 29181-5 (Future Network: Problem Statement and Requirements – Part 5: Security), which was produced in the JTC 1/SC 6/WG 7 February 2013 London meeting.

As per the Resolution 6.7.6 of 2012 Graz JTC 1/SC 6 meeting, this text is scheduled for the PDTR ballot processing by JTC 1/SC 6 Secretariat.

Reference number of document: ISO/IEC 29181-5

Committee identification: ISO/IEC JTC 1/SC 6/WG 7

Editors: Yadong Liu (China) and Wang Hao (China)

Information Technology — Future Network: Problem Statement and Requirements — Part 5: Security

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: Technical Report
Document stage: Preparation
Document language: E

Contents

Page

Forward

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29181-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, Telecommunications and information exchange between systems.

This second edition cancels and replaces the first edition ISO JTC1 SC6 6N15459, clause5-clause10 including subclauses, table and figure have been technically revised.

ISO/IEC TR 29181 consists of the following parts, under the general title Future Network — Problem statement and requirements:

— *Part 1: Overall aspects*

— *Part 2: Naming and addressing*

— *Part 3: Switching and routing*

— *Part 4: Mobility*

— *Part 5: Security*

— *Part 6: Media transport*

— *Part 7: Service composition*

Introduction

This part of TR 29181 (Future Network: Problem Statement and Requirements) describes the problems of the current network and the requirements for Future Network in the security perspective. The general description on the problem statement and requirements for Future Network is given in the TR 29181-1. In addition, this TR 29181-5 establishes the problem statement and requirements for Future Network in the viewpoint of architecture and functionality for security support.

In general, network security includes information security and network's own security. Network security is concerned with hardware, software, basic communication protocol, network frame structure, communication mechanism factors of the network, and involving a wide range of. This report will focus on changing the security mechanism of network security from the perspective of the future.

This Technical Report may be applicable to the overall design of Future Network architecture.

Information technology — Future Network: Problem Statement and Requirements — Part 5: Security

1 Scope

This Technical Report describes the problem statements of current network and the requirements for Future Network in the security perspective. This Technical Report mainly specifies

- Problems of the current network in security environment; and
- Requirements for security support in Future Network.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC TR 29181 (all parts), *Information technology — Future Network: Problem Statement and Requirements ISO/IEC TR 29181*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Future Network (FN) [ISO/IEC TR 29181-1]

The FN is the network of the future which is made on clean-slate design approach as well as incremental design approach. It should provide futuristic capabilities and services beyond the limitations of the current network including the Internet.

4 Abbreviations

FN	Future Network
ID	Identifier
IP	Internet Protocol
TR	Technical Report
DNS	Domain Name Server
KMI	Key Mangement Infrastruture

PKI	Public Key Infrastructure
USB-key	Universal Serial BUS Key
IC card	Integrated Circuit Card
Net Space	Future Network Space

5 General

5.1 Security environment in FN

For the future network, people have various assumptions.In all imagination they have one thing in common, that is the future network must be a reliable and secure network. It can provide reliable and effective support to a variety of political, economic, cultural, business and social activities for people, at the same time, provide security for the application and personal privacy as well.

In the future network, drawbacks of existing network security will be overcome, people don't have always to face the threat of cyber crime, because the new security system has made such a network environment in which all criminal behavior such as the wanton peeping and plunder of information, attacks etc, and network war simply can not exist. Even if there are malicious activities, it will be detected and deterred immediately. The future network will realize "data security", "network security" and "application security". People can safely use the network engaged in all kinds of business and exchange information between each other at ease.

5.2 Related works on security in FN

In the framework of the current network, the communication protocol and the security protection means is impossible to meet the demand of future network security. Therefore to gain the future network security we must break through the limitations of the existing mechanism and system, to design a brand-new architecture, basic communication protocol and rules with new concept. So the construction of future network security system is not only a complicated and difficult system task but also a revolution of mechanism and system.

6 Problem statement of current network in security environment

6.1 The existing problems and reasons of network security

At the beginning of the development of network technology, since the network application range was small and in relatively closed environment, security problem was not concerned. As the ability of original computer and network equipment was very limited, it is very reasonable to use the limited resources to improve the basic function and convenience. The popularity of the Internet has brought a completely open application environment, which made the security a crucial problem. Because the original design has not systematically consider the security factor, now the only choice is to take remedial measures for security problems as mending holes in a clothes with patches. As time passed, although the system has become fully covered with patches, but the information security problem remained the same as before. The final and the only way is to design a new system with security mechanism.

6.1.1 The existing internet no security mechanism, network users to undertake the security risk and protection responsibilities

The existing internet has no security mechanism the network user has to undertake the security risk and protection responsibility. This congenitally deficient is the intrinsic reasons and restricts for the network security.

The current network operation is very similar to the postal system. As long as someone posted a letters or parcels, the post office will sent them to the recipient, regardless whether he is willing or not. The letter or parcels are expected to be opened and inspected by the recipient who assumed security responsibility. As long as a people send e-mail or has the communicating requirements, regardless of the content of the message is good or bad, no matter whether it contains malicious acts, network system will deliver the mail , or establish communicating connection. As the network users generally do not have such special ability, they will do unpacking verifying and security judgment with other third party means of protection. But if the user can not keep highly synchronization with the provider, he can not respond effectively against cyber attacks with new means.

6.1.2 The random number addressing can only be explained by the designated DNS.

A big flaw in IP communication system is that IP address is a random number which can only be explained by the designated DNS. People only know he is communicating with a IP address but does not know with whom he is communicating. Unless the communicator himself shows his identity, even if the network user knows the actual place of this IP address through query, he can not make clear who the communicator is.

6.1.3 IP protocol does not provide truly proof of origin address, can not prevent illegal access.

6.1.4 The tree network architecture with single central control may lead to Security disaster

Because the existing network control system applied the tree architecture with a single center, there is possibility to bring security disaster to the whole network once the control center failure or in trouble

The above defects are main cause for viruses and Trojans overflowing ,witch opens the convenient door for plundering information, low-cost attack and network crime. Network can even be manipulated to wage cyber war, this is certainly not what the world people are willing to accept.

6.2 The current network security protection measures and effect

The existing network security protection system is a dynamic self information protection system, which is designed for private network and LAN, using those technologies for detection, response and recovery against network attack under the guidance of defense-in-depth strategy. Since there is no consideration about Internet as a whole, it is difficulty to establish a stable, large-scale trusted system with interconnection, intercommunication, mutual trust and interoperability.

6.2.1 Current security protection means of common network user

Common network user:

Protection means：Firewall ＋Upgrading anti-virus software；

Protection methods: Very old comparison method；

This kind of protection means has congenital defects；

Firewall is mostly used security device on the network, witch can allow or restrict the data transmission according to certain rules. But it’s also a computing device or an executive program in a computer, so it can't prevent threat by its vulnerability, cannot prevent the attack using defect in standard operating systems and network protocols. Firewall implements security strategy through open or closed some protocol and port but can not prevent attacks using some permitted protocols and access port to the server (or computer); in addition it cannot prevent the file which is infected by the virus to be transmitted.

The existing anti-virus software applied typical one to one solution. When a Trojan or virus detected, it is analysed, the virus feature code is taken and kept in virus-base followed by seeking out the virus killing method. Network user should constantly update anti-virus software and use it to scan all executive program If the virus and Trojan have been found it must be removed with special antivirus tools.

The disadvantages of this approach is: First it can only detect knowing viruses which can be found only after been infected; Second the new and upgraded virus increase continually and quickly ,even breakthrough millions. The maintenance work of upgrading antivirus software and tools is arduous; Third finding and killing the virus has to spend a lot of time and waste valuable system resources which greatly decrease the efficiency of the system.

6.2.2 Current security protection means of professional users

Professional network users:

Protection means：Encryption system＋Third party certificate；

Protection method：Digital signature，CA certificate and Key exchange based on Authenticating Center (Third party), and belong to the trusting mechanism.

Professional network protection system is built on two basic technology: key management infrastructure / public key infrastructure (KMI/PKI) used in the production, distribution and management of keys and security certificates, as well as infrastructure for the early warning, detection, identifying of possible network attacks, make effective response and detection on the investigation and analysis of aggressive behavior. The former focuses on issues of information authenticity and security, the latter mainly focuses on defending network security problem. Because these two are relatively independent, they can neither support each other, nor share resources.

6.3 Three main disadvantages of existing network security defense system

The current network security protection system based on passive defense strategy and completely gave up the initiative. There are three major disadvantages in it：

6.3.1 The direct result of passive defense strategy is the complete losing of initiative and the effective reaction ability against attack

6.3.2 To confront with computer technology, witch has low threshold, means the attack always has the absolute advantage.

6.3.3 Solution strategies for the corresponding means of each threat caused complicated system and the cost black hole.

The above three points determines the existing security system is built on the premise of the failure, can only improve the safety probability and cannot provide security guarantee.

7 The goal and requirements of future network security

7.1 The goal of future network security

Future network is a common subject explored by global scientific community.

Future network is not only a technical network but also a social network. It is a new one-dimensional space-time system (Net Space or Cyber Space) created by human with wisdom and technology. It will become the main bearing space for information activities of human society, and the virtual world corresponded with the physical world. Therefore, the future network security system should be the comprehensive system oriented to social management, which includes security, trust and management functions in one. It is the extension of the social security system of the physical world to Net Space.Therefore, in the premise of Net Space integrity and order, it should provide technical support to safeguard national sovereignty and the right of management, guarantee the legitimate rights and freedom to engage in information activities for individuals and groups,under the law frame and give them the ability to protect their information security.

7.2 To achieve trusted identity management, lay the foundation for future network security

In the Net Space, all the entities in the physical would are expressed as abstract Identites. Set up the proving relationship between identity and entity and guarantee the authenticity of identities with authentication technology is the foundation and precondition of future network security. On the basis of above the following problems neede to be solved:

7.2.1 To prove the authenticity of identity and address

To provide proof of authenticity of identity and address and create conditions for authentication, trusted connection, clear security responsibility;

7.2.2 Changing after-verifying communication rules

Changing after-verifying to pre-verifying communication achieves trusted connection;

7.2.3 Establish a new future network security system to realize three changes:

7.2.3.1 From passive defense to active management

With the help of identity authentication system, the whole security system will be established based on strict identity authentication management and achieve from passive defense to active management.

With the help of identity authentication system, the whole security system will be established on strict identity authentication management basis and achieved the transformation from passive defense to active management.

7.2.3.2 Replace computing confrontation with authentication technology

Replaces computing confrontation with authentication (the core is crypto technology) completely changes the premise of security.

7.2.3.3 Unify the security strategies and methods on the authentication technology, form a one to more system solution

At present, when a new virus appears on the Internet, the global 18-20 million computers will have to upgrade virus database and take new means for protection, that will consume a lot of resource and energy. For every kind of virus, the security experts will looking for the corresponding method to kill the virus. Future network will change the passive situation, and unify the security strategies and methods on the authentication technology, form a one to more system solution, greatly reduce the construction and maintenance cost, and gain initiative

7.3Technical architecture and function requirements for Future network security

Future network security technology system is based on identity authentication system and consists of platform security(Trusted Computing), trusted connection and trusted application.

7.3.1 Identity Authentication system

By constructing authentication infrastructure to Issue electronic ID cards for each subject (including **people** and things) witch gave them the ability for digital signature and key exchange..

7.3.2 Platform security (Trusted Computing)

Through digital signature and authentication for each executable program, prevent the Trojan virus and other illegal program from loading and execution, ensure the security of computing platform;

7.3.3 Trusted connection

Through pre-authenticating and encrypting the transmission content, ensures the trusted connection and the security for transmission content.

7.3.4 Trusted application

Through embedding authentication system into the application system to achieve application security.

7.3.5 The functional requirements of Future network security

- No limitation for the scale and architecture of security system. On prerequisite of standardization, it can meet the requirement to construct secure network information system crossing countries, sectors, and systems;
- Cell level security. People, equipment, device and even software process will be a security unit, which can be used to construct any scalable cell level independent security system;
- Private secret service. With the help of digital signatures and key exchange ability, which is provided by Identification Authentication System, anyone can enjoy privacy and share information with each other securely.
- Simple and efficient. Through constructing of standardized public authentication infrastructure to minimize the cost for construction, maintenance, operation;

8 Consideration of Key technology for future network security Implementation

In the Net Space, all the entities in physical space are expressed as abstract identities. Therefor, it is necessary to establish the binding relationship between identity and entity with authentication system. The identity authentication system that can directly generate public-private key pair from identity, and support direct authentication is the key technology. In order to establish an integrated system that can support global trusting environment, the Authentication System must meet the following conditions:

8.1 Support the real-name and anonymity authentication

Support the real-name and anonymity authentication to match the current social management system and meet the cognitive habits of people and society.;

8.2 Support large-scale application

Able to support global or large-scale application, and can meet large social requirement.

8.3 Support end-to-end directly authentication and key exchange

Support end-to-end direct authentication and key exchange, can provide technical support for the new generation of security system;

8.4 Support management domain segmentation and end-to-end cross-domain direct authentication

Support management domain segmentation and end-to-end direct cross-domain authentication in order to meet the requirements for sovereignty and the management right of different countries, regions, units etc. and the need to build a large globalized security system.

8.5 Simple structure, convenient use, low cost, and easy popularized

Identity Authentication System is the core of future network security, its basic function will be achieved through distribution and embedding. The distribution is to distribute key device containing authentication system and identity key (can be encapsulated into a variety of forms such as USB-key, IC card etc.) to each person or piece of equipment. The embedding is to embed the authentication system into a variety of devices and applications through standardized interfaces to achieve security function.