TECHNICAL REPORT

ISO/IEC TR 29181-5

First edition
2014-12-15

Information technology — Future Network — Problem statement and requirements —

Part 5: Security

Technologies de l'information — Réseaux du futur — Énoncé du problème et exigences —
Partie 5: Sécurité

Reference number
ISO/IEC TR 29181-5:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Terms and definitions **1**

3 Abbreviations **1**

4 General **2**
4.1 Security environment in FN 2
4.2 Related works on security in FN 2

5 Problem statement of current network in security environment **2**
5.1 The existing problems and reasons of network security 2
5.1.1 Network users undertake the security risk and responsibilities 3
5.1.2 Irregular Address and no truly proof for origin 3
5.1.3 Central control may lead to security disaster 3
5.2 The current network security protection measures and effect 3
5.2.1 Current security protection means of common network user 3
5.2.2 Current security protection means of professional users 4
5.3 Disadvantages of existing network security defense system 4

6 The goal and requirements of FN security **4**
6.1 The goal of FN security 4
6.2 The requirements of FN security 5
6.2.1 From passive defense to active management 5
6.2.2 Replace computing confrontation with authentication technology 5
6.2.3 Forming one to more system solution with authentication technology 5
6.3 FN security technical system 5
6.3.1 Identity Authentication system 5
6.3.2 Platform security (Trusted Computing) 5
6.3.3 Secure connection and transmission 5
6.3.4 Application security 5
6.3.5 The functional requirements of FN security system 5

7 Consideration of Key technology for FN security implementation **6**
7.1 Support the real-name and anonymity authentication 6
7.2 Support large-scale application 6
7.3 Support end-to-end directly authentication and key exchange 6
7.4 Support management domain segmentation and cross-domain authentication 6
7.5 Simple structure, convenient use, low cost, and easy popularized 6
7.6 The application method to realize Identity Authentication 6

Foreword

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 6, *Telecommunications and information exchange between systems*.

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*

Additional parts, dealing with quality of service and networking of everything are planned.

Introduction

This part of ISO/IEC 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 ISO/IEC TR 29181-1. In addition, this part of ISO/IEC 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 the 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 many things. This part of ISO/IEC TR 29181 will focus on changing the security mechanism of network security from the perspective of the future.

This part of ISO/IEC TR 29181 can be applicable to the overall design of Future Network architecture.

Information technology — Future Network — Problem statement and requirements —

Part 5: Security

1 Scope

This part of ISO/IEC TR 29181 describes the problem statements of current network and the requirements for Future Network in the security perspective. This part of ISO/IEC TR 29181 mainly specifies

— problems of the current network in security environment, and

— requirements for security support in Future Network.

2 Terms and definitions

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

2.1
Future Network
FN
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

[SOURCE: ISO/IEC/TR 29181-1:2012, 3.1]

2.2
Net Space
new dimensional time-space system created by humans with communication, computer and other information technology, which provides new space for human information activities (including information gathering, processing, storing, transmission etc.) and is becoming an ever important part of the survival and development environment for human society

Note 1 to entry: Net Space is derived and expended from network.

Note 2 to entry: It is becoming an ever important part of the survival and development environment for human society.

2.3
FN Space
FN
main space for information activities of human society and finally developed to the virtual world corresponding to and closely interacted with the physical world

Note 1 to entry: FN Space will be the development and improvement of Net Space.

Note 2 to entry:

3 Abbreviations

FN Future Network

ID	Identifier
IP	Internet Protocol
TR	Technical Report
KMI	Key Management Infrastructure
PKI	Public Key Infrastructure
USB-key	Universal Serial BUS Key
IC card	Integrated Circuit Card

4 General

4.1 Security environment in FN

For the FN, people have various assumptions. In all imagination there is one thing in common, that is the FN 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 FN, drawbacks of existing network security will be overcome, people don't have always to face the threat of net 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 cannot exist. Even if malicious activities happened, it will be detected and deterred immediately. The FN will realize "data security", "network security" and "application security". People can safely use the network to engage in all kinds of business and exchange information between each other at ease.

4.2 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 FN security. Therefore to gain the FN 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 FN security system is not only a complicated and difficult system task but also a revolution of mechanism and system.

5 Problem statement of current network in security environment

5.1 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 so serious. 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. At present, when a new virus appears on the Internet, the global 1,8 - 2 billions computers have to upgrade virus database and take new means for protection, that will consume a lot of resource and energy.

5.1.1 Network users undertake the security risk and responsibilities

The existing internet has no sufficient 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 network user 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 have no ability for security judgment, they have to use security tools and services from the third party. But if the user cannot keep highly synchronization with the provider, he cannot respond effectively against net attacks with new means.

5.1.2 Irregular Address and no truly proof for origin

A big flaw in IP communication system is that IP address is irregular number. People only know he is communicating with an 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. Besides the existing IP protocol provides no proof for origin address, it cannot prevent illegal access.

5.1.3 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 fails or in trouble.

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

5.2 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, and 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 difficult to establish a stable, large-scale trusted system with interconnection, intercommunication, mutual trust and interoperability.

5.2.1 Current security protection means of common network user

Common network user:

Protection means: Firewall plus upgrading anti-virus software;

Protection methods: Very old comparison method;

This kind of protection means has congenital defects;

Firewall is the mostly used security device on the network. It can allow or restrict the data transmission according to certain rules. But it is 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 cannot 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 and analyzed, the virus feature code is taken and kept in virus-base followed by seeking out the virus killing