NEWS RELEASE

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION

June 1, 2001

NTT Develops Network Security Technologies for providing Advanced Commercial Services in IPv6 Internet

-Enabling use of the Internet for secure leased lines and paid multicast networks-

NTT has developed a new IPv6 secure network construction technology called 'DVPN' and multicast stream usage control technology called 'InfoPrism' (both code names) for commercial use. These new technologies are at the forefront of the current IPv6 development trend shifting from interconnectivity toward the development of new network services that make use of the special characteristics of IPv6. As people use the Internet in every corner of their lives with the widespread use of HIKARI network(optical network) and broadband mobile communications in the future, these new technologies will help realize the next generation Internet society where people can communicate seamlessly at anytime, anywhere, irrespective of communications device.

The explosive increase in the popularity of the Internet has resulted in a depletion of IP addresses and an increased load on routers. As a means of dealing with these problems, activities targeting the introduction and propagation of the next-generation Internet protocol Ipv6 have been progressing at a rapid pace, based on interconnectivity experiments taking place in countries throughout the world.

NTT Information Sharing Platform Laboratories has been working since 1996 in the field of IPv6 network construction technologies as well as operation and management technologies, and has constructed an empirical testing network, the largest in the world, linking the Asian, American, and European continents.

Recently, the trend in research related to IPv6 networks is shifting away from basic interconnectivity toward the development of new network services that make use of the special characteristics of IPv6. These newly developed technologies are at the forefront of this trend.

DVPN (Dynamic Virtual Private Network) technology enables secure and flexible network construction while taking advantage of the end-to-end communication capabilities featured in of IPv6 terminals. It enables safe connections between any terminals (or any users) by introducing a system in which a third-party validation agency can provide simultaneous authentication for various community participants with regard to whether or not the terminals conducting end-to-end communication have the appropriate access privileges from a certificate authority. By using this technology, it enables connections at any time, in any location, by anyone (or via any electronic device). Unlike the case of the existing Internet, it will be possible to conduct secure communications between specified terminals as though on a leased line, regardless of whether or not those terminals are a part of a LAN. This will dramatically expand the potential applications of the Internet.

InfoPrism is a usage control technology that allows only users with the appropriate usage privileges to access contents when applying stream distribution services for video images and other contents using IPv6 multicast transmission functions. The contents being distributed are encrypted differently for each user, and the encryption keys are changed at regular intervals; these and other measures have been taken to enable usage control for each individual user, a function that had been difficult to achieve in the case of multicast transmissions. A wide range of applications is conceivable, including paid Internet broadcast services with limited user memberships.

Both of these technologies will be displayed in NTT Communications' booth at NetWorld+Interop 2001 Tokyo, to be held from June 6.

<Main Features of DVPN> (Ref. Figs. 1 & 2)

Unlike traditional security technologies that validate digital certificates for each individual IPv6 terminal, DVPN adopts a method by which digital certificates for community participants are automatically verified by a third-party validation agency when a terminal begins to communicate. In addition to allowing VPN (Virtual Private Network) services using the Internet as though it were a leased line, this enables a number of useful features, including the following.

1) End-to-End CUG (Closed Users Group) configurations

An Internet application method called CUG, or " Closed User Groups" is used for communications involving confidential content. When private addresses are used on the existing Internet, as a rule it is only possible to configure a CUG within individual LANs, but with DVPN CUGs can be formed using the necessary terminals regardless of whether or not they are on the same LAN. Furthermore, because digital identification is carried out automatically by the authorization agency and the CUG management system, even parties that have never come in contact before can easily form a CUG if they are members of the same community.

2) Eliminate the bottle neck for encryption and authentication transaction

By encrypting and authenticating transactions at end hosts, DVPN system enables direct communications that do not require an encoding/authentication gateway--a communication style considered suitable for peer-to-peer applications. For this reason, there is no need for expensive high-performance encoding gateways, and substantial cost reductions are attainable across the entire network. This arrangement also resolves the problem of " traffic tie-ups" due to server overload.

3) Cost reductions through outside contracting of the CUG management system

Up to now, it was necessary to install security equipment within the LAN, and it was difficult to contract network operations to an outside party while maintaining confidentiality of organizational and management information. With DVPN, however, it is possible to isolate the network operation system from this CUG management information and contract the operation of the system alone to an outside party, allowing reductions in management costs.

4) Providing detailed services appropriate to a variety of end-to-end communication styles

Because the CUG management system centrally controls the status of communication usage, it is possible to gather accounting information in keeping with VPN service usage. This allows the operator to provide detailed services appropriate to time or amount of communication.

<Main Features of InfoPrism > (Ref. Fig. 3)
InfoPrism is usage control technology for each user by encryption to resolve the problem of unauthorized usage in the context of multicast transmissions.

1) Achieving usage control by encryption
As in the case of standard broadcasts, " Multicasts" --also referred to as " Internet broadcasts" --do not allow the operator to control the distribution of information only to specified users. In order to prevent unauthorized usage, it is necessary to establish a system to prevent the contents from being used even after they have been distributed. InfoPrism encrypts the contents using a common key, encrypts that common key using a individual key for each user that has usage privileges, and then distributes these " encrypted common keys" along with the encrypted contents in stream format. This way, users with usage privileges can decrypt the encrypted common key using their individual key, and then decrypt the encrypted contents using the common key that they have retrieved, allowing them to use the contents. Users without usage privileges, however, are unable to decrypt the contents.

2) Encrypted keys changed at regular intervals
InfoPrism is designed such that the key for encrypting the contents is changed at regular intervals. This not only allows greater security against unauthorized usage resulting from persons acquiring encryption keys at some point on the communication route, it also responds to the specific needs of users, for example with regard to situations where only a part of the contents will be used.

3) Sending key beforehand assures that key is safely received
Because the key information sent to each user is different, a time lag occurs when this information is transmitted, and when there are large numbers of users involved, there is a possibility that the key information will not be received in time to decrypt the distributed contents. To resolve this problem, the key is sent to the user ahead of the encrypted contents.

<Plans for the Future>
(The future of DVPN)
NTT Information Sharing Platform Laboratories plans to make numerous improvements including increasing the scale of the communities covered by CUG management systems, and at the same time incorporate DVPN into specific application services.
NTT Communications has been providing Internet connections services using IPv6 since April 2001. The company plans to conduct tests using DVPN technologies as a part of the VPN tests being carried out jointly with Tekenaka Corporation in the context of these activities.

(The future of InfoPrism)
Having established the basic principles of this technology, NTT Information Sharing Platform laboratories plans activities such as expanding functions and establishing ties with accounting systems to allow InfoPrism to be incorporated into application services.
Both of these technologies will be displayed in NTT Communications' booth at NetWorld+Interop 2001 Tokyo, to be held from June 6.

- Figure1. DVPN Service Aspects and Features
- Figure2: Example - Internet based and secure teleconferencing
- Fig. 3: InfoPrism System Configuration

For inquiries related to this matter:

NTT Information Sharing Laboratory Group
Planning Department, Public Relations: Kurashima, Sano, Ikeda
TEL: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE