

IPN creates New Information Security concept



Trinity Security Systems, Inc.
Vice President Takeshi Nakamura

Trinity Security Systems has developed IPN (Identified Private Network™ or the Intelligent Packet Network™). IPN is a flexible system that it can be used as a centralized system in enterprise network as well as a decentralized system such as P2P network. One of the IPN's distinctive characteristics is that it can provide mutual authentication under pure P2P environment. Therefore, IPN has a potential for changing the existing information security concept and providing a completely new concept in information security.

Idea of expanding Trusted zones within the world of Untrusted zone

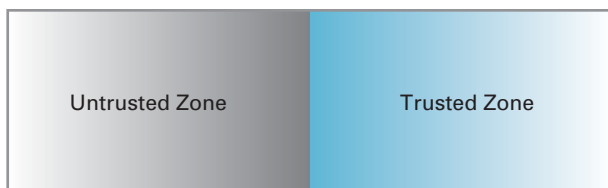


Figure 1: Concept of Trusted and Untrusted zone in IPN

In the information security world, only two zones exist. One is the 'Trusted zone' and the other is the 'Untrusted zone' (figure 1).

In the Trusted zone, information security would be safely maintained. Malicious people are nonexistent in the Trusted zone. Of course, there is a possibility of insiders with no malicious intent inadvertently leaking protected information, and we should consider this possibility when we design the information security policy and systems. One example of the Trusted zone is inside LAN. To protect information leakage, for example, we need to consider protection against intrusion from the Untrusted zone into the Trusted zone. Also, information must not be brought into the Untrusted zone from the Trusted zone unless some security measure has been adopted on the information. Many technologies have been established and implemented to ensure the information security.

As a basic rule, we need to consider eliminating all possible security holes. Security holes are not only on systems, but on process, policies, and physical environment. To ensure information security, one should

consider people movement. As technology has been progressed to allow people access information anywhere and anytime, concept of ubiquitous availability of information should be maintained, but at the same time, the information must be securely managed when we design the information security.

People physically move from the Trusted zone to the Untrusted zone. If the person who has classified information move out from the Trusted zone and he didn't put any protected measure on the classified information, then he is in the Untrusted zone with classified information unprotected. IPN concept is to provide secure environment regardless of the person's location whether he is in the Trusted zone or the Untrusted zone.

Ubiquitous concept with security

The basic idea of ubiquitous security is to allow people access to the Trusted zone from the Untrusted zone, or extend the Trusted zone to cover the person who is in the Untrusted zone. One of the technologies that can achieve the ability of ubiquitous access are VPNs (Virtual Private Network) such as IP Sec VPN and SSL VPN which is called remote access. In this case, information remains in the Trusted zone and the VPN provides the means to access the Trusted zone. If a person moves out from the Trusted zone to the Untrusted zone with classified information, then the information itself is in the Untrusted zone. Then, the Trusted zone must be

created so that the information remains in the Trusted zone.

When the information that must be protected are defined, IPN can create the environment where the information is accessible only in the Trusted zone. In other words, the information is not accessible by anybody if they are in the Untrusted zone. IPN makes it possible to access to the Trusted zone, or to create the new Trusted zone so the information becomes accessible.

IPN creates new security zone

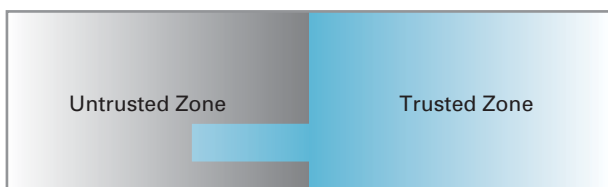


Figure 2: Extended trusted zone

IPN can create a new Trusted zone in the Untrusted zone, or create new access to the Trusted zone. Therefore, people can have a secure environment even if they are in the Untrusted zone as they can create or have access to the Trusted zone (figure 2).

We define this as 'creation of the extended Trusted zone'. The prerequisite to enabling this Trusted zone extension is to have mutual authentication capability between the person who wants to access the Trusted zone or to extend the Trusted zone in the Untrusted zone, and the authenticator who grants the access or the extension or the Trusted zone. Reciprocally, the authenticator must be authenticated by the person who wants to access to the Trusted zone. In other words, the authentication must be mutual authentication. IPN enables the mutual authentication without having third party involvement such as CA and/or RADIUS server. This is similar to what happens in our daily life when we recognize individual persons. Whenever we meet people who we already know, we can recognize the person without asking the third party if we know the person. IPN mutual authentication works in a similar manner. The two devices can mutually recognize each other without consulting third party once they have necessary information concerning each other. It is important to understand that the mutual authentication enabled by IPN is between devices but not between people. IPN

enables mutual authentication between things that can be digitized, so things that cannot be digitized are beyond IPN mutual authentication capability. As people are basically not the ones to be digitized, IPN doesn't provide mutual authentication between people. Regardless, IPN can create a security zone that can be defined as the Trusted zone up to the digital world.

One of the IPN's distinctive characteristics is that it is very light in terms of required computing power. Therefore, IPN can be applied on many things that have less computer processing power. To realize the Extended Trusted Zone, first, the two devices or digital files need to be mutually authenticated. If mutual authentication is unsuccessful, then the files or the data are encrypted so that nobody but the person who has decryption key can read the data. Someone who has decryption key is the one who is in the Trusted Zone. With this, the Trusted Zone is effectively extended, or the new Trusted Zone is created in the Untrusted Zone. If this concept is applied where the two devices are connected to communicate each other, communication would be only possible when two devices are mutually authenticated. This concept is similar to VPN. When IPN is applied on the document files in digital form, then mutual authentication would be done between the digital files and the devices attempting to access to the files. When the mutual authentication is successful, then the files would be decrypted. In other words, the Trusted Zone would be created or extended when the mutual authentication is successful.

IPN is flexible so that it can be applied on decentralized information security

IPN enabled information security can be managed in a decentralized manner as the mutual authentication can be done between the two parties concerned without third party involvement. There are merits and demerits on managing the information security in decentralized manner. Notable demerits on managing the information security in a decentralized manner is that it would be very difficult to manage security policy consistently as each party can employ his/her own policy – that's the basic meaning of decentralization when the security policy is managed in decentralized manner. But one

thing for certain is that the IPN has a potential for exponential growth because of the fact that the IPN can be managed in decentralized manners. As an analogy, the Internet has grown exponentially because of its ability to be managed in decentralized manner. The Internet has grown with tremendous speed as networks connected to the Internet are managed locally with good degree of freedom. IPN can create a closed area in P2P environment. P2P community connected with IPN would expand exponentially in a similar manner as the Internet had grown.

What is good about using IPN is that it can create the Trusted zone in Internet space easily. The Internet space is considered to be the Untrusted zone. To create the Trusted zone with the currently available information security technologies, highly skilled network engineers have to design a secure network with certain infrastructure investments. The work requires up-to-date and extensive knowledge in network and information security. Because designing and implementing up-to-date and state of the art information security systems is complex and require extensive knowledge on IT managers, there is a possibility of misconfigurations of the systems where it would become a security hall. Therefore, the fact that the IPN can create the Trusted zone easily and anyone without having extensive knowledge in the information security can create the Trusted zone is a huge difference between the existing technology and the IPN.

Can IPN create absolute secure environment?

IPN can create the Trusted zone easily. Then, can IPN create absolute secure environment? The answer is 'NO'. In the information security, the absolute secure environment is essentially nonexistent. However strongly security systems are established, security holes would exist. The security hole may be in the systems itself, may be in the work processes, or may be in physical security. In IPN, the mutual authentication can be done between two devices that can be explained in digital form but not the user oneself. For user authentications, some security measure is necessary in parallel to the IPN device authentication. In other words, user identification such

as using biometrics identification would be necessary to ensure validity of the mutual authentication. But that doesn't mean that IPN has a security hall. As the IPN can securely maintain the Trusted zone and allow the extension of the Trusted zone only for the person who has the mutually authenticated device, this fact alone provides one of the most secure environments among the existing technology. As is always the case for any security measure, we should consider not only on the systems and technology but also on the human factors and security process. IPN is no exception.

Strength of the IPN security

What follows are the capability of IPN that can characterize the strength of IPN security.

1. Mutual authentication

As we explain in the previous sections, the mutual authentication capability is the prerequisite for enabling access to the Trusted zone or to extend the Trusted zone. Mutual authentication capability is, therefore important for information security. IPN can provide mutual authentication safely and securely with very simple and light method such that low CPU devices such as PDA can have the mutual authentication capability. This capability is the core of the IPN technology.

2. Impersonation is completely blocked.

Even if the system has the capability of mutual authentication, if the system doesn't have the capability of detecting impersonation, it has a big security hole in authentication. IPN can completely (in device level) exclude the possibility of impersonation such as MAC address spoofing. In IPN enabled security, even if the user ID and password are stolen, unauthorized access would be blocked as the device is authenticated with different measure which is technically secure and doesn't allow impersonation.

3. Mutual authentication is done in each session

Mutual authentication should be done in each session to ensure that we communicate with known party every time we connect with each other. IPN goes through the mutual authentication process in each TCP session and each time the mutual authentication is done, the

authentication key changes, enabling TKIP solution.

4. Authentication and encryption keys changes dynamically.

As the keys for authentication and encryption changes dynamically for packet by packet basis, it is virtually impossible for the cracker to steal these keys. In addition, the keys are never transmitted in the network. Only hash values are transmitted. Thus the possibility of the keys being stolen during mutual authentication and/or data transmission is null. Also as the keys changes for packet by packet basis with strong encryption, eavesdropping is virtually impossible.

5. Detection of data alteration

IPN has the capability of detecting unauthorized data alteration. If the data alteration is detected, the data is discarded. IPN communication between two parties are done such that the two devices are mutually authenticated in the beginning of the session and that the data are transmitted without alteration.

There is no existing technology but IPN available that can change authentication and encryption keys for packet by packet basis. IPN has achieved one of the highest security levels in the information security world.

Where can IPN be applied? – example of IPN application -

We have discussed that the IPN expands the possibility of improving information security. Let's talk about how the IPN is applied in the information security.

First, the IPN can be applied in place of VPN (Virtual Private Network) such as IP Sec. You would be interested to know the difference between IPN and VPN. In terms of what IPN and VPN can achieve, they are similar in that both achieve a secure communication via Internet, preventing eavesdropping and dispensing packets that are forged, allowing only authorized party communicate each other. Therefore, there isn't much difference between the two when functionalities are compared. Clearly, IPN is much easier in configuring the network, keys are securely managed and there is no possibility of the keys being stolen. In addition, IPN encryption is stronger as the decryption keys changes for packet by packet basis.

As IPN can provide mutual authentication capability easily, IPN fits nicely when it is applied on remote access. Since IPN can verify authorized device securely, without fail, it is applicable for the services that require secure mutual authentication such as online banking, online games, etc. where not only the authentication of the server but also the authentication of the user is strongly required. Also, IPN fits in the P2P applications as IPN can provide mutual authentication without having third party authentication such as CA and/or RADIUS server. IPN fits also for wireless LAN applications.

Comparison between IPN, IP-Sec and SSL-VPN

When IPN is used on VPN-like application, people would be interested in how IPN is compared with the existing VPN technologies such as IP-Sec and SSL-VPN. The table 1 indicates the comparison on remote access applications.






















	IPN	IP Sec-VPN	SSL-VPN
Easiness of configuration	-Requires client software -Client software requires low processing power -Configuration is easy and simple 	-Requires client software -Client software requires high processing power -Configuration is complicated 	-No client soft is requires if web applications only used. But if applications other than web is used, reverse proxy, or virtual L2 interface is required. Then client software is required. -Client software requires high processing power and configuration is complicated 
Remote access client	-Equipment that can use client software -PC and PDA, etc. (As software requires low processing power, PDA can be used.) 	-Equipment that can use client software. -PC, etc. (As the software requires high processing power, it is difficult to use low CPU equipment such as PDA.) 	-Equipment that runs web browser (PC, PDA, cell phone, etc.) – if only web application is used.  -If other than the web applications are used, it would be more difficult than if IP-Sec is used.
Access controls on contents and/or servers	Easy 	Difficult 	Easy 
Initial cost	Lower than IP Sec 	Low 	High 
Cost for operation	low 	High 	Low 
on the existing network	Can be applied seamlessly 	Need some consideration on NAT and firewall 	If the application is only web application, then it can be applied seamlessly. If other than web application is considered, it would be more complicated than IP Sec/ 
Throughput	Higher than IP Sec 	Higher than SSL-VPN 	Lowest of the three 

Table:1 Comparison between IPN,IP Sec and SSL VPN

We have discussed about the concept of information security and how IPN fits in this concept. IPN can be applied both on centralized information security and decentralized security network such as P2P, and thus it has a good potential to expand. We have also compare with the existing technology in remote access area and showed the potential of IPN.