Firewall-Friendly VoIP Secure Gateway and VoIP Security Issues

● Noriyuki Fukuyama ● Shingo Fujimoto ● Masahiko Takenaka

(Manuscript received September 26, 2003)

IP telephony services using VoIP (Voice over Internet Protocol) technologies have rapidly spread over the last several years. However, interoperation of an IP-PBX (Private Branch eXchange) service and a consumer IP telephony service has not yet been achieved. This is because typical intranets are protected by firewalls and IP telephony protocols are not firewall-friendly—because, among other reasons, they use UDP (User Datagram Protocol)-based protocols. In this paper, we explain the technologies of the VoIP Secure Gateway, which makes IP telephony protocols firewall-friendly and enables an enterprise IP-PBX service to interoperate with a consumer IP telephony service through a firewall. Also, we look at other security problems that need to be solved in order to expand IP telephony services in the future.

1. Introduction

IP telephony services using VoIP (Voice over Internet Protocol) technologies have rapidly spread over the last several years. Many IP telephony services have recently been started: for example, consumer IP telephony services provided by legacy telephone carriers, IP-PBX (Private Branch eXchange) services provided by enterprises, and IP telephony outsourcing services for enterprises (IP Centrex services) provided by ISPs (Internet Service Providers)/carriers.

In the case of IP-Centrex services, ISPs/carriers provide not only IP-Centrex services but also consumer IP telephony services, so ISPs/carriers can provide secure interoperation between an enterprise IP phone and a consumer IP phone. However, apart from IP-Centrex services, IP-PBX services cannot interoperate with consumer IP telephony services.

This is because typical intranets are protected by firewalls and IP telephony protocols are not firewall-friendly—because, among other reasons, they use UDP (User Datagram Protocol)-based protocols. Consequently, interoperation services are achieved by using legacy telephone lines.

In this paper, we describe the technologies of the VoIP Secure Gateway, which makes IP telephony protocols firewall-friendly and enables an enterprise IP-PBX service to interoperate with a consumer IP telephony service through a firewall. Also, we look at other security problems that need to be solved to expand IP telephony services in the future.

2. Problems associated with interconnections between IP telephony services

IP telephony services use IP networks as their infrastructure. Therefore, interoperation of IP networks is required for interoperation of IP telephony services. Since an IP network is “open,” it increases the risk of illegal accesses. In this section, we explain the security risks when an IP-PBX service interoperates with a consumer IP telephony service through a firewall and the problems with previous methods.

2.1 Interconnections between the Internet and an intranet through a firewall for data traffic

Generally, when an enterprise connects its intranet to the Internet, administrators install a firewall to filter out unwelcome packets and thereby protect the intranet against illegal accesses from the Internet.

From the users viewpoint, the firewall should prevent illegal accesses from the Internet while at the same time enable the system it protects to provide e-mail and Web services. Therefore, the firewall is set to permit passage of packets from the intranet to the Internet (outgoing packets) and, with one exception, reject all packets coming from the Internet (incoming packets). This one exception is TCP (Transmission Control Protocol) packets of the SMTP (Simple Mail Transportation Protocol), which is the protocol for e-mail services. Therefore, users can establish intranet-to-Internet TCP connections over the firewall, but apart from SMTP TCP connections, Internet-to-intranet TCP connections are not possible.

However, in order to prevent direct illegal access from the Internet, the firewall only permits Internet-to-intranet SMTP TCP connections via the mail gateway in the DMZ (De-Militarized Zone).

2.2 Incompatibility between firewalls and IP telephony protocol

Unlike HTTP (Hypertext Transfer Protocol) for Web browsing and FTP (File Transfer Protocol), an IP telephony service that only enables outgoing calls is not useful. To receive incoming calls, a firewall is needed to pass an IP telephony protocol such as SIP (Session Initiation Protocol) or H.323 from the Internet. If the IP telephony protocol uses TCP for its call signaling protocol, it is similar to SMTP. However, many firewall administrators think it is undesirable to add a firewall rule that permits Internet-to-intranet TCP connections. On the other hand, if the IP telephony protocol uses UDP for its call signaling protocol, the same problems as the ones that affect the voice media protocol will occur (**Figure 1**).

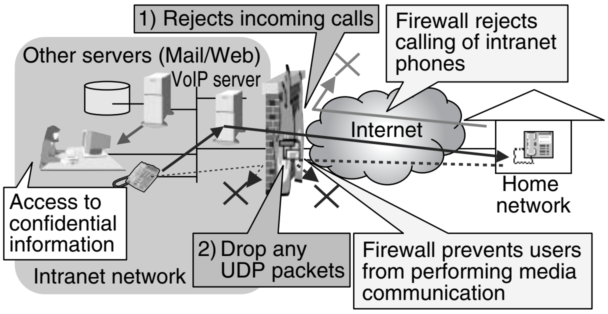
1) Rejects incoming calls
Firewall rejects calling of intranet phones
Other servers (Mail/Web)
VoIP server
Internet
Home network
Access to confidential information
Intranet network
2) Drop any UDP packets
Firewall prevents users from performing media communication

Figure 1
Incompatibility with typical firewall configurations.

Because an IP telephony service provides real-time communication, it is suitable for transferring voice media packets using UDP rather than TCP. For communication between a terminal on the Internet and an intranet terminal through a firewall, the firewall must permit the passage of UDP packets. As described in Reference 1), UDP packets do not have handshake mechanisms or sequence numbers, so it is much easier to make fake UDP packets than fake TCP packets. Therefore, fields such as the source address field of UDP packets must be carefully checked. This is why conservative administrators reject UDP packets at the firewall.

The coupling of IP telephony protocols is another problem. Typical IP telephony systems use different protocols for call signaling (SIP or H.323) and media communication using RTP (Real-time Transport Protocol). Since RTP packets must be routed by destination IP address and port number for each call, the IP telephony system needs to use a wide range of port numbers. However, typical intranet security policies do not allow such a wide range of port numbers to be opened on the firewall.

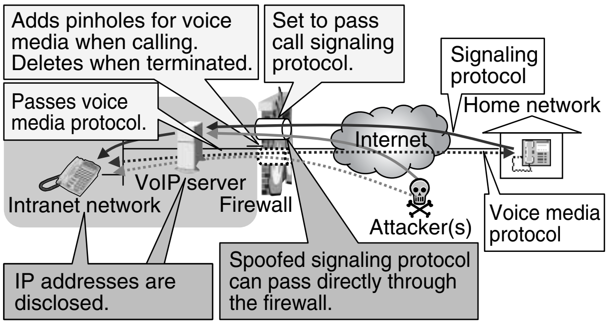
Adds pinholes for voice media when calling. Deletes when terminated.
Set to pass call signaling protocol.
Signaling protocol
Home network
Passes voice media protocol.
Internet
VoIP server
Intranet network
Firewall
Attacker(s)
Voice media protocol
IP addresses are disclosed.
Spoofed signaling protocol can pass directly through the firewall.

Figure 2
Making pinholes in a firewall.

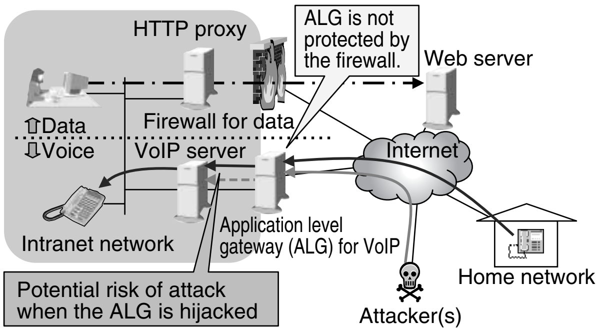
HTTP proxy
ALG is not protected by the firewall.
Web server
⇧Data
⇩Voice
Firewall for data
VoIP server
Internet
Intranet network
Application level gateway (ALG) for VoIP
Home network
Potential risk of attack when the ALG is hijacked
Attacker(s)

Figure 3
Application level gateway (ALG).

2.3 Existing strategies and their problems

There are several strategies for interconnecting IP telephony services through a firewall. We will now explain two major strategies and their problems.

2.3.1 Making pinholes in a firewall

The method of making pinholes is shown in **Figure 2** and consists of the following steps:

1) Instruct the firewall to pass the IP telephony call signaling protocol,
2) use the signaling protocol to exchange session information that includes communication parameters, IP addresses, and port numbers. (This strategy captures the session information and uses it to add or delete firewall rules.)
3) pass the voice media protocol through the rule while the call is being established, and
4) delete the permission rule (close the pinhole) to pass the voice media protocol when the call is terminated.

However, this strategy has several weaknesses that can be used to attack servers and terminals. For example,

1) A spoofed signaling protocol can pass directly through the firewall, and
2) the IP addresses of IP-PBXs and IP telephone terminals are disclosed.

2.3.2 Application level gateway (ALG)

In this strategy, the IP telephony system has an application level gateway (ALG) that is separate from the firewall. The ALG acts as an intermediary for IP telephone calls between the Internet and the intranet (**Figure 3**).

Because the ALG is not protected by the firewall, this method can be attacked if the ALG becomes hijacked.

3. VoIP Secure Gateway

In the previous section, we described the problems of interoperability of IP-PBX services and consumer IP telephony services. These problems come from the fact that IP telephony protocols are not firewall-friendly.

We developed the VoIP Secure Gateway (VoIP-SGW) to make IP telephony protocols friendly for common firewall configurations. Because our system only requires the minimal addition of the rule that is typically used for TCP-based applications, security will not be weakened.

In this section, we describe the VoIP-SGW technologies shown in **Figure 4**.

3.1 Connection control technology

SIP and H.323 based IP telephony services use UDP packets and incoming TCP connections, but most enterprise firewalls do not allow them to pass through. Therefore, it is impossible to interoperate over firewalls using these protocols. Our approach to this problem is to convert these transports into outgoing TCP connections, which are usually accepted by firewalls when they are used in major Internet applications such as HTTP

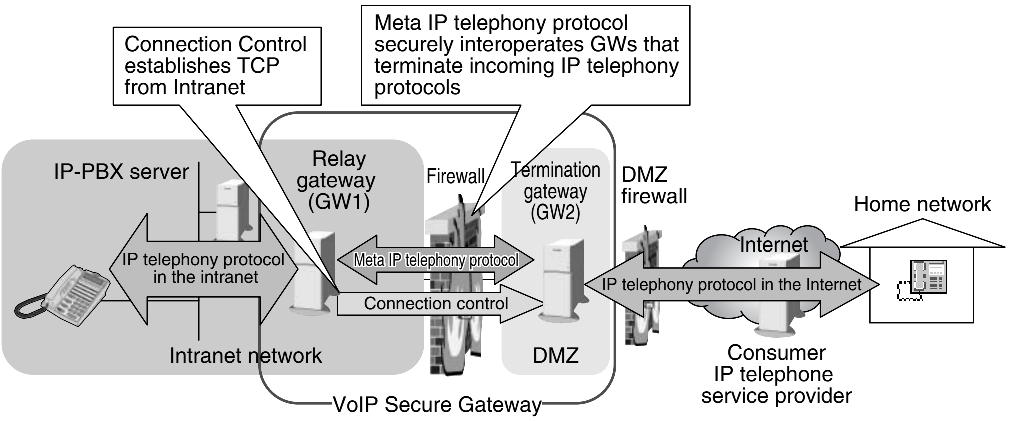
Connection Control establishes TCP from Intranet
Meta IP telephony protocol securely interoperates GWs that terminate incoming IP telephony protocols
IP-PBX server
Relay gateway (GW1)
Firewall
Termination gateway (GW2)
DMZ firewall
Home network
Internet
IP telephony protocol in the intranet
Meta IP telephony protocol
Connection control
IP telephony protocol in the Internet
Intranet network
DMZ
Consumer IP telephone service provider
VoIP Secure Gateway

Figure 4
VoIP Secure Gateway (VoIP-SGW).

and FTP. We call this approach "Connection Control."

The VoIP-SGW consists of a relay gateway (GW1) located in the intranet and a termination gateway (GW2) located in the DMZ. The main idea of Connection Control is to make TCP connections from GW1 to GW2 (intranet-to-DMZ). Usually, TCP transports cause critical transmission delays in real-time applications. However, under a well-managed LAN network environment, which rarely loses packets, TCP connections can provide good transmission. There are several implementation approaches, but it is important to simplify the filtering rules for VoIP service on the firewall to protect the intranet from illegal accesses. In our implementation, the VoIP-SGW uses two TCP connections: one for the call signaling protocol and another for the voice media protocol. In this case, the firewall will have a filtering rule to allow TCP connections from GW1 to GW2 using two specific ports.

3.2 Meta IP telephony protocol

To prevent Internet-to-intranet passage of IP packets, GW2 terminates incoming calls, examines them carefully, and then converts them to the IP telephony protocol of the intranet. We call this internal IP telephony protocol the Meta IP telephony protocol.

IP telephony protocols are terminated to prevent direct passage of IP telephony protocol messages to the intranet hosts. GW2 examines incoming IP telephony messages and reconstructs them as Meta IP telephony protocol messages. These messages are sent to the relay gateway, GW1. Then, GW1 communicates with the appropriate intranet IP telephone using the internal IP telephony protocol. During this process, unsupported options and illegal protocol messages are filtered out.

GW2 also examines incoming media communication messages and filters them before forwarding them to GW1. The Meta IP telephony protocol is designed to be transferred over a TCP connection. The TCP connection for the Meta IP telephony protocol is established from GW1 (located in the intranet) to GW2 (located in the DMZ). This TCP connection is usually accepted in typical firewall security policies.

These features enable VoIP communication over a firewall without compromising security.

3.3 Features of the VoIP Secure Gateway

The VoIP-SGW has two unique characteristics: 1) the administrators do not need to configure the firewall to pass packets from the Internet to the intranet for VoIP communication, and 2) it only accepts incoming calls on gateway servers located in the DMZ network. If a gateway has been attacked and hijacked, the firewall can still guard the intranet and limit access from the gateway server.

Moreover, the VoIP-SGW system terminates incoming protocol messages and converts them to Meta IP telephony protocol messages. GW1 can convert the Meta IP telephony protocol into any major VoIP protocol for the IP-PBX system, for example, SIP and H.323. Therefore, this method can be used when the IP telephony protocol used in the intranet is different from that used in the Internet, or the IP version in the intranet is different from that in the Internet (e.g., IPv6 vs. IPv4).

4. Other VoIP security issues

We have explained how VoIP-SGW protects an IP telephony system against illegal accesses from the Internet through a firewall. In this section, we describe the security problems related to an IP telephony service.

According to Reference 2), when evaluating the security of an IP telephony service, we should consider six aspects (availability, authentication, confidentiality, integrity, non-repudiation, and access control) (**Table 1**).

Legacy PSTN (Public Switched Telephone Network) telephone systems achieve high security levels regarding these aspects because they use single-purpose, physically secured communication lines provided by a trusted telephone office.

On the other hand, since IP telephony systems use open IP networks as their communication infrastructure, an IP telephony system does not achieve the security level achieved by legacy PSTN telephone systems (**Figure 5**). We therefore suggest that IP telephony services reinforce their security in terms of availability, authentication, and confidentiality.

4.1 Availability on IP telephony

Because IP networks are "open," they do not provide the required level of security that dedicated PSTN-based networks provide. VoIP-SGW improves the availability of an IP telephony system; however, it cannot solve some of the security problems that affect IP telephony services.

Attacks such as DoS (Denial of Service) attacks and network congestions caused by computer viruses and worms are serious problems because telephone services are lifeline services. Especially, ensuring the priority of emergency phone calls is a problem that should be solved immediately.[3)]

Most of these problems are common to IP-based systems, and we can solve them by integrating standard IP security technologies and IP telephony technologies.

4.2 Authentication for IP telephony services

In general, IPsec (IP security) protocol, TLS

Table 1
Security functions in IP telephony.

Security services	Security functions in IP telephony
Availability	Countermeasures against interruption of network access and DoS attacks (including VoIP-SGW)
Authentication	Terminal, VoIP servers, and message authentication.
Confidentiality	Privacy functions for communication data, protocol parameters, correspondents, and calling activities.
Integrity	Countermeasures against session hijacks and replay attacks
Non-repudiation	Session logs to be charged for
Access control	Permission to make calls and use additional services

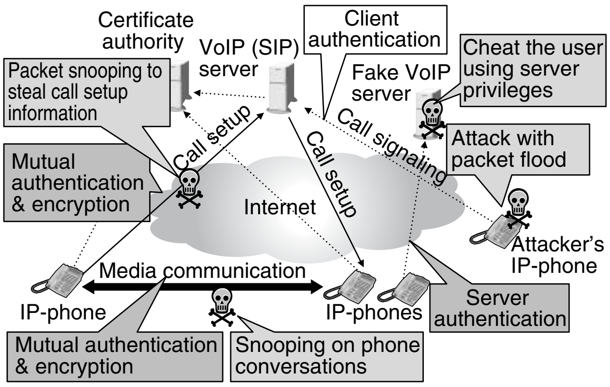

Figure 5
Other security issues for IP telephony services.

(Transport Layer Security), and S/MIME (Secure/Multipurpose Internet Mail Extensions) are considered to be powerful tools that add security features such as authentication and encryption. However, it is not commonly known that system security depends on how these tools are used.

In legacy PSTNs, each phone line is given its own phone number (ID), so phone numbers are matched to the physical location of the telephone set connected to the line. Additionally, the lines are physically secured against illegal accesses and the telephone numbers are centrally controlled at the telephone office.

On the other hand, the IP telephony system assigns an IP address to each IP phone user instead of a phone number. Since attackers can easily spoof an IP address, an IP telephony service requires peer-to-peer authentication. However, it is difficult to share the secret information used for authentication between end-users. Therefore, an integrated authentication system, for example, PKI (Public Key Infrastructure), could be used for peer-to-peer authentication and encryption for secure IP telephony services.

For example, in Japan, there is a kind of nationwide integrated authentication system called the “JuKi-Net, Basic Resident Registration Database.” However, various privacy problems must be solved before this database can be used for commercial systems.

Currently, many people regard interoperability as the most important problem of IP telephony services; however, we believe that security is even more important. Especially, mobile IP phones and software IP phones cannot work safely without security enhancements, and one-stop authentication will be required when IP telephony services are used with other IP services such as Web services.

4.3 Confidentiality on IP telephony services

Another major security problem is confidentiality. We categorize confidentiality on IP telephony services into four levels. The lowest level of confidentiality hides the conversation context and is achieved by encrypting the media communication. The second level hides protocol parameters that may give hints for further attacks, for example, the IP addresses, port numbers, CODEC (COder/DECoder) names, and data formats used in a call. This confidentiality level is achieved by encrypting call signaling protocol messages.

Encryption technologies make it difficult to obtain original data contents, but the third level goes one step further by hiding the src/dst pair of VoIP traffic. This level of confidentiality can be achieved by multiplexing media communication packets from several users, sending them to an intermediate server, and then switching them. The highest level of confidentiality hides the calling activities themselves. This can be achieved by additionally transmitting fake packets so an unauthorized receiver cannot easily detect calling activity. However, this method requires a lot of extra bandwidth and computation power and is therefore not normally acceptable.

We will research and develop technologies to solve these problems by considering the balance between requirements and cost. Also, we will keep up with the relevant standardization activities to guarantee interoperability.

5. Conclusion

In this paper, we explained the technologies of our VoIP Secure Gateway. The VoIP-SGW solves the incompatibility problem between typical enterprise firewalls and IP telephony protocols and enables an IP-PBX service to interoperate with other IP telephony services on the Internet. To make practical use of these technologies, the consumer IP telephony service providers and enterprises that use IP-PBXs should agree on the parameters that are to be exchanged, for example, the parameters for mutual authentication, accounting, caller/callee information, and bandwidth.

We also described the general security problems related to interoperation between IP telephony services. These problems are related to the service availability, authentication infrastructure, and privacy functions and are not only technological problems but also political ones. Since telephone services are lifeline services, it will be necessary for the Government to institute guidelines and new laws concerning IP telephony services.

6. References

1) W. R. Cheswick and S. M. Bellovin: Firewalls and Internet Security. AT&T Bell Laboratories, 1994.

2) W. Stallings: Cryptography and Network Security: Principles and Practice. Second Edition, Prentice-Hall, 1999.

3) T. Kikuchi, M. Noro, H. Sunahara, and Shinji Shimojo: Lifeline Support of the Internet. in Proceedings of SAINT2003 workshops, p.323-327, January 2003.

Noriyuki Fukuyama received the B.E. and M.E. degrees in Communication Engineering from Osaka University, Osaka, Japan in 1986 and 1988, respectively. He joined Fujitsu Ltd., Kawasaki, Japan in 1988, where he has been engaged in research and development of communication systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan. He is currently working at Fujitsu Laboratories Ltd., Kawasaki, Japan.

Shingo Fujimoto received the B.E. and M.E. degrees in Computer Science from the University of Electro-Communications, Tokyo, Japan in 1992 and 1994, respectively. He joined Fujitsu Laboratories Ltd., Akashi, Japan in 1994. In 1996, he worked at Fujitsu Laboratories of America, where he helped standardize the protocol specifications for Internet applications at the Internet Engineering Task Force (IETF). He returned to Akashi in 2000. He is currently engaged in research and development of security enhancing technologies for Internet applications.

Masahiko Takenaka received the B.E. and M.E. degrees in Electronic Engineering from Osaka University, Osaka, Japan in 1990 and 1992, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1992, where he has been engaged in research and development of cryptography and information security systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan. He is currently working at Fujitsu Laboratories Ltd., Akashi, Japan.