コンピュータセキュリティ　17－1
（２００２．５．２３）

在宅テレワーク用境界システムのセキュリティ確保

力武 健次　菊地 高広　永田 宏　濱井 龍明　浅見 徹

株式会社 KDDI 研究所
〒356-8502 埼玉県上福岡市大原 2-1-15
email: kenji@kddilabs.jp

在宅テレワークは会社員やパートタイム勤務者の働き方の主流の一つになった。高速なインターネットへのアクセス手段が普及するにつれ、勤務者が自宅から作業を行うのに十分な帯域を使うことができるようになった。しかしその一方で、家庭の機器は企業内ネットワークのそれらに比べ十分に守られておらず、セキュリティ攻撃の格好の対象になっている。本稿では、まず在宅テレワーク用の一般的なシステム設定が持つ技術的弱点を分析し、それをふまえた上で在宅テレワーク用システムのネットワークセキュリティを強化するための基本的な要請事項を述べ、家庭内と外部の双方のネットワークの境界にゲートウェイシステムを使った構成例を提案する。

キーワード: テレワーク、アクセス制御、ネットワークセキュリティ

Secure Gateway System Design for Home Teleworking

Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, Tatsuaki Hamai and Tohru Asami

KDDI R&D Laboratories, Inc.
2-1-15 Ohara, Kamifukuoka City, Saitama 356-8502 JAPAN
email: kenji@kddilabs.jp

Home Teleworking has become a major workstyle for corporate and part-time workers. As high-speed access methods to Internet become popular, workers can utilize sufficient bandwidth to perform their tasks from home. On the other hand, home equipments are not well-protected as those of the corporate networks, and have been major victims of security attacks. In this paper, we first analyze the technical weakness of common system configurations for home teleworking. We then address the basic requirements to enforce network security of home teleworking systems, and propose the configuration examples using the gateway system at the border of the home and the external networks.

Keywords: Teleworking, Access Control, Network Security

1 Introduction

Teleworking means using computer networks such as Internet as a medium for performing business tasks. Teleworking enables the workers to work without being bound to commuting and working hours.

Teleworking is gaining popularity in Japan as well as other developed nations. Japan Telework Association reported more than 3 million corporate workers were working from home in the year 2002 [6]. This means more than 5 percent of Japanese workforce (67.66 million in the year 2000) have already been working form home. The report indicates about 13 percent of Japanese corporations have allowed employees to work from home in the year 2000.

Teleworking is referred as a viable alternative in the White Paper of the National Lifestyle [27] to improve the quality of life of the individuals. The white paper also indicates that teleworking contributes reducing everyday commuting hours, increasing time available for taking care of the family members, reducing the traffic congestion of urban highways and trains, and increase overall productivity of individual workers.

Connecting networks for teleworking to an organizational network should be done with implementing adequate precautional security protection measures, since the system configuration of each teleworker has different settings and vulnerabilities. The interconnection should be defensive as possible and should not allow unnecessary services or protocols to be accessible from unexpected users.

The Internet systems of typical teleworkers, however, are still premature for business and prone to security attacks. Recent increase of available bandwidth to home networks by high-speed media such as ADSL (Asynchronous Digital Subscriber Line), Cable TV, and FTTH (optical Fiber To The Home) have opened the opportunity for malicious attackers to abuse the home systems for their own activities [2], while they provide sufficient bandwidth for the production-level activities of legitimate users.

One of the reasons that unsecure systems are used in teleworking environment is that most of the business workers have little awareness of Internet technology [9]. While more people have become aware of the possibilities of security attacks such as wiretapping and packet forgery over Internet links, very few actually protect themselves against those security exploitations.

A Wired News article [26] reports a good example of how an ordinary corporate worker knows little about network security. The story tells about a former dot-com company employee who has been given a computer as a severance pay. The computer was configured for use in a *firewall-protected* corporate network, but the employee connected the computer to the home network *with no security protection*. The machine eventually caught some network viruses, but the owner only felt that the machine was *just acting funny*. The owner could only take the machine to a computer repair shop because the person *didn't know what to do*. This story shows that an ordinary business worker doesn't know much about how the computer network the person uses is protected.

Since April 2001, we connect the home network of one of the authors Rikitake, who lives in Toyonaka City, Osaka, Japan as a home teleworking branch of our corporate research environment in Kamifukuoka City, Saitama, Japan [8]. We perform a field test of teleworking to evaluate how it affects to the productivity and quality of the results. So far we have achieved successful results on improving the quality-of-life of the workers, as well as providing the mobility and portability of the working environment, while maintaining the secure and productive working condition at the same time.

In this paper, we first analyze the technical vulnerabilities of the common current practice on home networks, which only uses packet-filtering routers. We then address the requirement of adding a gateway system and isolating the home teleworking systems in a private network to enforce security protection. We also propose the configuration examples of the gateway system for well-known Internet services, and discuss a model for extending the system to support multimedia communication.

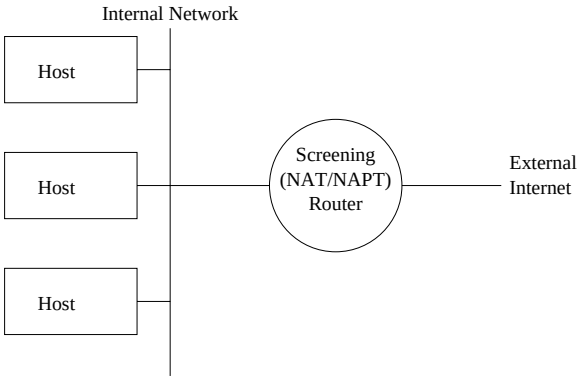

Fig. 1 A Simple Screening-Router-Based System

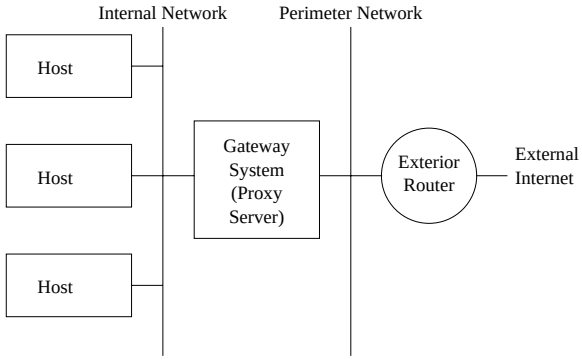

Fig. 2 A Screened Subnet Architecture with A Gateway System

2 Weakness of Screening-router-based Architecture

A typical network configuration on home teleworking, shown in Figure 1, is based on a screening router which performs the packet filtering and NAT/NAPT (Network Address Translation / Network Address and Port Translation) and the internal hosts with the RFC1918 private addresses [18]. While this configuration is fairly easy to set up and operate, it has the following fundamental vulnerabilities [1]:

- Each host in the internal network and the screening router itself have to be carefully protected to prevent security incidents. This sort of protection is not likely to be achieved on a home teleworking system, since the administrator of a home network usually knows little about the security issues.
- The screening router has to put out the logging information to an internal host to record the possible intrusion and irregular activities. If none is available, the trace information is lost. Even if a host is available for logging, the logs may be easily stolen when an intrusion to the host occurs.
- The screening router requires correlating NAT/NAPT translation table information with the logs to figure out which internal host is actually involved in an activity. This makes the log analysis difficult and complex.
- NAT/NAPT blocks packets from the external network if they are not matched with the entries of the address-and-port translation table. This means a static mapping has to be set up to run a server within the internal network. It may also reduce the strength against external port exploitation.
- A simple NAT between the internal and external networks, which allows all ports to be forwarded, can be a loophole for an external intruder to access into the internal network. For example, if a UDP (User Datagram Protocol) [10] packet is sent from the internal host to an external host as a protocol request, the screening router must also enable the address translation to accept the response packet from the external host to the internal host, for a certain amount of time (i.e., 30 seconds to 1 minute). During the mapping is enabled, the external host can abuse the mapping to penetrate the screening router and to intrude inside the internal network.
- A complex NAPT, such as IP Masquerading of Linux [5], handles non-trivial protocols such as FTP (File Transfer Protocol) [14] which requires simultaneous bidirectional TCP (Transmission Control Protocol) [13] connections in the non-PASV transfer mode, by monitoring and rewriting the contents of data packets. While this functionality adds convenience for the external access from the internal networks, it also makes the overall system complex and prone to possible security attacks.

We propose configuring home teleworking systems using the *screened subnet architecture* as

shown in Figure 2, rather than a simple screening router architecture, to solve the issues mentioned above. Screened subnet architecture, which is common among corporate firewall systems, uses up a separate external perimeter network to isolate the internal network from the perimeter with a gateway system by prohibiting allow direct IP (Internet Protocol) [11] [12] packet exchange between the two networks.

3 Gateway System Requirements and Suggested Configuration

Internet application protocols required for teleworking are well-known. They can be handled by running proxy servers on the gateway system. The following shows our basic principles of how to treat the major protocols for teleworking:

- The gateway system should not forward any IP packet between the internal and external networks. This means no NAT/NAPT at the gateway system, and no UDP-based services is allowed except for mandatory ones such as DNS (Domain Name System) [15] [16] and NTP (Network Time Protocol) [17]. All cross-boundary traffics are handled by the proxy servers running at the gateway system. The operating system of the gateway system should be robust and adequately secure, such as FreeBSD [4].
- The external IP address of the gateway system can be dynamically or statically assigned, depending on the ISP (Internet Service Provider) to which the system is connected. While the dynamic address assignment service is cheaper, the static address assignment service is suggested, since having a fixed address on the gateway system makes it accessible from the Internet and enables it to provide services from the external client hosts, such as receiving electronic mail messages.
- About the DNS configuration: the internal DNS space should be isolated from the Internet. Only the gateway system should be accessible from the Internet; internal hosts should be registered into a private DNS space. The internal/private DNS server should only be accessible from the internal network. Reference to the `in-addr.arpa` zones for unused RFC1918 private address spaces should be internally resolved and never be forwarded to the DNS Root Servers.
- Running a DNS cache on the gateway system is strongly suggested to maximize the performance of name references by the proxy servers. The reference of external names from the internal hosts is not needed in our configuration, though allowing it does not hamper the security of the gateway system. Rikitake uses djbdns [3] on his system for the DNS services.
- About the electronic mail services: running an SMTP (Simple Mail Transfer Protocol) [22] server on the gateway system is sufficient to forward e-mail messages between the internal and external hosts. The SMTP server should prohibit third-party relaying to prevent forwarding unsolicited commercial messages, and should only accept the cross-boundary and the internal forwarding requests. Rikitake uses qmail [7] on his system as the SMTP server.
- Running a server for a mailbox-retrieval protocol such as POP3 (Post Office Protocol Version 3) [19] is suggested, though *not* required, if the gateway system has a fixed IP address. The mailbox server should not be directly accessible from the external network to prevent possible intrusion.
- Although logging into the gateway system should be minimized to prevent security incidents, SSH (Secure Shell) [24] provides sufficiently secure remote login and execution facilities, either from the internal hosts or from the external clients on the Internet. Only the public-key authentication should be allowed.
- SSH is also effective to provide relays for TCP services, such as forwarding a POP3 connection from an internal host for an external server. The number of relays, however, should be minimized.
- About the external Web access: HTTP (HyperText Transfer Protocol) [21] and outgoing FTP can be handled well by running a proxy server such as Squid [23] on the gateway system. Squid also works as a web cache and is effective to reduce redundant outgoing traffics to retrieve Web graphics and popular pages. The internal hosts do not have to con-

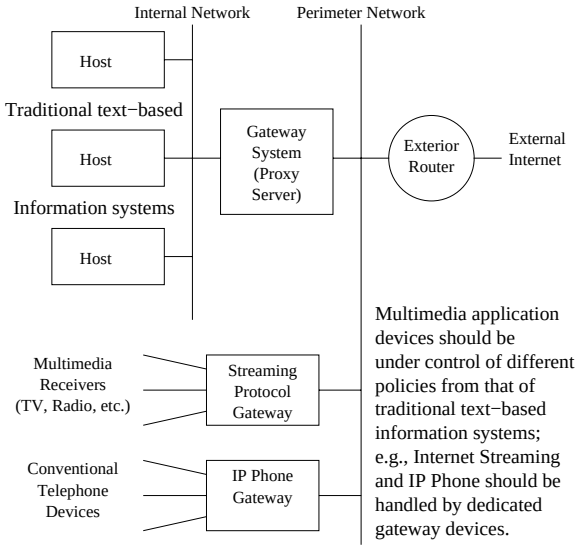

Fig. 3 A Model for Supporting Multimedia Teleworking

sider the bidirectional nature of FTP so long as using HTTP for the proxy access.

- About the time synchronization: running an NTP server is the ideal solution for obtaining the best accuracy. Practically speaking, however, periodically running an SNTP (Simple Network Time Protocol) [20] client program once per hour for referring to a Stratum-2 NTP server is sufficient to keep the internal clock of the gateway system synchronized within 50-millisecond offset.
- To provide the time source for the internal clients, broadcasting/multicasting time information to the internal network by running an SNTP broadcast program synchrozed to the internal clock of the gateway system works well. Programs listening to the SNTP broadcast packets are publicly available such as Tardis 2000 or K9 for Windows2000 [25].

Rikitake has been performing his teleworking tasks of documentation and software development using Web, electronic mail, and other traditional applications, based on his system configured as described in this section without serious security incidents. Various kinds of intrusion attempts, however, such as port scanning and illegal access, have been logged on the gateway system. This shows a corporate-level defense system is required and strongly suggested also for home teleworking.

4 A Future Issue: Supporting Multimedia Protocols

Extending a screened-subnet system solely depending on proxy servers to multimedia use is not practical. The major applications such as the audio-visual streaming and the IP phone are heavily dependent on isochronous packet delivery using UDP packets. Workload of the gateway system can be greatly increased due to the increase of the amount of traffic transferred through the proxy servers, if the system has to relay multi-Mbps packet streams such as audio-visual data.

Figure 3 shows an example of a model for providing support for multimedia applications for teleworking. Using a dedicated gateway for each multimedia protocol provides both load balancing and isolation for keeping the home system secure. Each gateway is attached to the perimeter network so that it can choose the own packet filtering policy.

In this example, the streaming gateway provides conversion between multimedia receiver devices such as traditional TV and radio and the Internet broadcast streams. The IP phone gateway acts as the phone exchange between the traditional phone devices and the Internet phone links. Since IP phone protocols such as ITU-T H.323 requires almost all ports above the port number 1023 be opened to the external Internet, a specific gateway configuration is suggested to support the H.323, which is also used for Microsoft's NetMeeting, a popular realtime teleconferencing tool.

We need to evaluate this model by further experiments.

5 Conclusion

In this paper, we analyzed the weakness of the current screening-router-based configuration of teleworking systems, and proposed that screened-subnet-based configuration with proxy servers was sufficient for providing the infrastructure for Web, electronic mail, and other TCP-based tasks. We also proposed that adding multimedia functionalities to our system would require dedicated gateways for each protocol, because of the fundamental difference of the protocol nature.

Acknowledgements

Our thanks go to Dr. Hiroki Nogawa of Osaka University Cyber Media Center, Mr. Koji Nakao and the members of Network Security Laboratory of KDDI R&D Laboratories, Inc. for reviewing the draft paper.

References

[1] E. D. Zwicky, S. Cooper, and D. B. Chapman: *Building Internet Firewalls (2nd Edition)*, O'Reilly & Associates, ISBN 1-56592-871-7 (2000).

[2] CERT/CC: *Continuing Threats to Home Users*, CERT Advisory CA-2001-20 (last revised: July 23, 2001). http://www.cert.org/advisories/CA-2001-20.html

[3] D. J. Bernstein: *djbdns*. http://cr.yp.to/djbdns.html

[4] The FreeBSD Project: *The FreeBSD Operating System Release Information*. http://www.freebsd.org/releases/

[5] D. A. Ranch: *Linux IP Masquerade HOWTO, v2.00.041902*, April 19, 2002 (2002). http://www.tldp.org/HOWTO/IP-Masquerade-HOWTO/

[6] Nihon Keizai Shimbun: *NIKKEI NET Article*, April 6, 2002 (2002). http://www3.nikkei.co.jp/kensaku/kekka.cfm?id=2002040601482

[7] D. J. Bernstein: *qmail*. http://cr.yp.to/qmail.html

[8] K. Rikitake, T. Kikuchi, H. Nagata, T. Hamai, T. Asami: *Practical DNS Support for Dialup ADSL*, Proceedings of IPSJ Computer Security Symposium 2001 (CSS2001), IPSJ Symposium Series, Vol. 2001, No. 15, pp. 73–79 (2001).

[9] K. Rikitake, T. Kikuchi, H. Nagata, T. Hamai, T. Asami: *Security Issues on Home Teleworking over Internet*, IEICE Technical Report IA2001-20, Vol. 101, No. 440, pp. 9–16 (2001).

[10] J. Postel: *User Datagram Protocol*, RFC768 (also STD6) (1980).

[11] J. Postel: *Internet Protocol*, RFC791 (also STD5) (1981).

[12] J. Postel: *Internet Control Message Protocol*, RFC791 (also STD5) (1981).

[13] J. Postel: *Transmission Control Protocol*, RFC793 (also STD7) (1981).

[14] J. Postel, J. Reynolds: *File Transfer Protocol (FTP)*, RFC959 (also STD9) (1985).

[15] P. V. Mockapetris: *Domain names – concepts and facilities*, RFC1034 (also STD13) (1987).

[16] P. V. Mockapetris: *Domain names – implementation and specification*, RFC1035 (also STD13) (1987).

[17] D. L. Mills: *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, RFC1305 (1992).

[18] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear: *Allocation for Private Internets*, RFC1918 (Also BCP5) (1996).

[19] J. Myers, M. Rose: *Post Office Protocol – Version 3*, RFC1939 (Also STD53) (1996).

[20] D. L. Mills: *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*, RFC2030 (1996).

[21] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: *Hypertext Transfer Protocol – HTTP/1.1*, RFC2616 (1999).

[22] J. Klensin, *Simple Mail Transfer Protocol*, RFC2821 (2001).

[23] D. Wessels: *SQUID Frequently Asked Questions* (2000). http://www.squid-cache.org/Doc/FAQ/FAQ.html

[24] D. J. Barrett, and R. E. Silverman: *SSH, The Secure Shell: The Definitive Guide*, O'Reilly & Associates, ISBN 0-596-00011-1 (2001).

[25] HC Mingham-Smith Limited: *The Tardis Home Page*, http://www.kaska.demon.co.uk/tardis.htm

[26] Michelle Delio: *Beware That Company Box You Took*, Wired News, September 4, 2001 (2001). http://www.wired.com/news/print/0,1294,46417,00.html

[27] Quality-of-Life Bureau, Cabinet Office, Government of Japan: *White Paper on the National Lifestyle Fiscal Year 2001*, March 26, 2002, Chapter 4, Section 2 (2002).