テレワーク環境でのインターネットセキュリティ管理

Internet Security Management on Teleworking Environment

力武 健次 [1 2]　野川 裕紀 [3]　田中 俊昭 [2]　中尾 康二 [4]　下條 真司 [3]

Kenji Rikitake[1 2], Hiroki Nogawa[3], Toshiaki Tanaka[2], Koji Nakao[4], and Shinji Shimojo[3]

[1] 大阪大学大学院情報科学研究科
Graduate School of Information Science and Technology, Osaka University
rikitake@ist.osaka-u.ac.jp
[2] （株）KDDI 研究所セキュリティグループ
Security Laboratory, KDDI R&D Laboratories, Inc.
kenji@kddilabs.jp, tl-tanaka@kddi.com
[3] 大阪大学サイバーメディアセンター
Cybermedia Center, Osaka University
{nogawa,shimojo}@cmc.osaka-u.ac.jp
[4] KDDI（株）情報セキュリティ部
Information Security Department, KDDI Corporation
ko-nakao@kddi.com

Abstract: The number of security incidents on the Internet rapidly increases every year, and the threats become more serious and intense. Teleworking environment is also affected by this change of Internet security incidents as well. In this paper, we describe the emerging Internet security issues under the teleworking environment for each technology, such as unwanted emails, wireless LANs, P2P software, and VoIP. We then propose a set of practical solutions against the security threats.

キーワード：テレワーク，インターネットセキュリティ，セキュリティ管理
Keywords: Teleworking, Internet Security, Security Management

1 Introduction

Teleworking through Internet has been getting more popular, as the cost of Internet connection at home and small offices decreases and the amount of available bandwidth increases. 100Mbps-class Internet access are now available for urban apartments and office building, with a combined solution of optical-fiber building-level links and per-room access links using Ethernet or VDSL. ADSL and Cable TV links still plays a major role to provide 10Mbps-class access. Even on a notebook PC, 10Mbps-class access using WLAN (Wireless LAN) technology and 128kbps-class access using PHS links are widely deployed. The amount of available bandwidth especially in urban areas is vastly increasing.

The increasing security incidents, however, significantly undermine the usability of Internet. The trend of the incidents gets more pervasive and ubiquitous, so are the access methods to the Internet. For example, SPAMs or unsolicited commercial messages and virus-generated emails are filling up the mailboxes and render the email system completely useless. WLANs have become easy targets of wiretapping and stealing private information. P2P (Peer-to-Peer) software tools are abused and have become a medium of disseminating random files, including copyrighted and private items, from anonymous sources to anonymous destinations. VoIP (Voice-over-IP) and teleconferencing systems are prone to external attacks and can be a security threat if not properly managed.

Most of the newly-emerged threats, nevertheless, can be effectively mitigated by applying a traditional security principle of Internet: *divide and isolate*. The new issues are that many systems are provided without removing the vulnerabilities, and that contamination of security environment cat be easily occurred as many computer systems are being shared among multiple social-or-organizational

contexts, such as home and workplaces, which can degrade the level of security in an administrative zone. Regarding these new issues, a new security principle on Internet should be: *divide, isolate, and sanitize*, to keep the integrity of all systems.

In this paper, we describe the emerging security and usability threats of Internet teleworking for recent emerging technologies, and the practical migigation/workaround methods to cope with the threats. We first describe the general principle of the traditional Internet security and the necessary enhancement in Section 2. We focus on the detailed issues of the emerging technologies and show the practical workarounds in Section 3. We then describe an example of Internet teleworking system in Section 4, and conclude the paper in Section 5.

2 Traditional Internet Security Model and The Limitations

Most of the teleworkers connect their systems to an organizational network for doing their jobs. In this scenario, teleworking systems are mission-critical as well as the other organizational computer systems are. Teleworking systems should keep the adequate level of security standards required by the organization. The general principles of maintaining the integrity of organizational network systems are also applicable to the teleworking systems.

Cheswick et. al. [1] describes two models for securing computer systems: *host-based security* and *perimeter security*. The host-based security model means that each host should be capable to defend themselves from possible attacks even if it is not externally protected by other devices such as firewalls. On the other hand, the perimeter security model means to set a zone of protection inside a limited network, explicitly guarded by firewalls, and isolating the vulnerabilities within the perimeter from possible exposure. Since no security model is complete by itself alone, system administrators usually take a multi-layer approach combining the host-based and perimeter security models.

One of the problems on connecting a teleworking system into an organizational network is that the connection means breaking the organization perimeter, which may introduce a new vulnerability to the organizational systems. Figure 1 shows an example of how a teleworking system can be an organizational threat, by adding a route of exposure to an external threat. Since the organization usually trusts the teleworking system, if the system

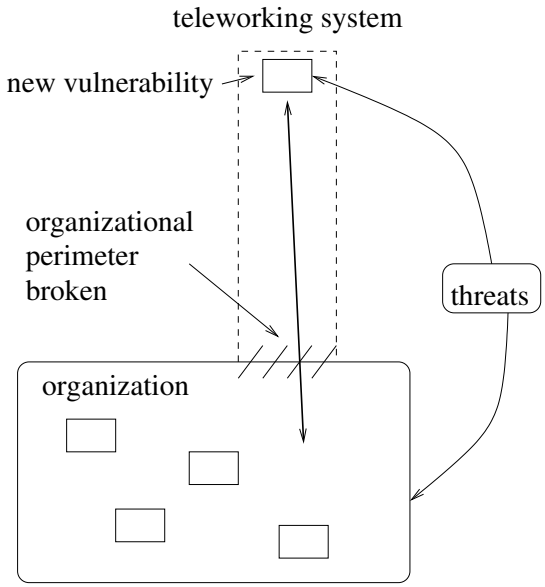

Fig. 1 A teleworking system can break a security perimeter.

contains a virus or anything contagious through a network, the epidemic can affect many other organizational systems. Note that the contamination is bi-directional and may occur from the organization to the teleworking system, which may make the teleworking environment, such as the home network of the teleworker, also vulnerable to the existing problems in the organizational network.

To solve the mutual-contamination problem, each system connected to the organizational network, *including the teleworking systems*, should be regularly and thoroughly sanitized. The sanitization includes, but not is limited to, virus-contamination checking in the file systems and the running programs (e.g., *Services* in Windows OS), activity monitoring and prevention of infecting other systems, auditing of the systems with external simulated attacks, and application of proper fixes (e.g., *patches* and *Windows Update*). Without these sanitization activities, a computer can easily be compromised and will become an incubator of unwanted viruses.

The contamination problem can even get worse if a teleworker works for multiple organizations and has to connect his working environment to the organizational networks. The teleworker should be extremely careful to avoid contamination of each organizational networks not only to prevent spreading computer vulnerabilities, but also to avoid unwanted sharing of sensitive information among the

multiple unrelated client organizations.

3 Recent Security Threats and Workarounds on Internet Teleworking

In this section, we describe the emerging threats and the workarounds of the Internet teleworking.

3.1 Unwanted email messages

Automatically-generated email messages are now flooding into the everyone's mailbox. The following list shows some typical sources:

- SPAM or unsolicited commercial email, which contains advertisements of commercial or political natures, such as selling illegal drugs and illegal software copies;
- Messages generated by computer viruses including infectious contents as the attachments and with fabricated message headers including false `From:` field;
- Messages generated by virus-checking programs of mail servers, notifying the rejection of virus messages, though practically of no use, since the messages are sent to the address of the `From:` field of the fabricated message headers, which has very little relationship with the actual offender.

To cope with those unwanted messages, the following server-side workarounds have been widely implemented:

- disabling third-party relaying capability of mail servers, by restricting the acceptable sender-destination pair by the client IP (Internet Protocol) address and the destination mail address;
- rejecting mail from widely-available blacklists (e.g., the MAPS RBL [2]), maintained by user reports and the blacklist administrators.

Those restrictions, however, are solely based on the IP and mail address information and does not screen the contents. Recent unwanted mail messages usually pass these address-based tests and cannot be blocked solely by these server-based restrictions. End-user filtering tools of incoming messages are required for rejecting unwanted messages, such as:

- virus-checking software monitoring and inspecting the contents of incoming POP3 and outgoing SMTP ports of each mail client host, and blocking incoming/outgoing viruses;
- auto-learning SPAM-filtering software, such as SpamProbe [3], distinguishing unwanted messages by learned criteria using Bayesian analysis [4] with the user assistance of telling the software which message is a SPAM or not.

Without the filtering mentioned above, a mailbox can easily be occupied by junk messages. Rikitake, one of the authors of this paper, received 528 unwanted messages filtered out during the 7-day period of May 11th to May 18th, 2004, to one of his mailboxes. Some ISPs (Internet Service Providers) have the option menu for users to block and reject the suspicious SPAM and virus-contaminated messages. These options are effective workaround to keep the noise level at minimum.

We should note that using the virus-checking and SPAM-filtering software is still insufficient for the messages including virus-rejection warnings from legitimate mail servers, and that DoS (Denial-of-Service) problem caused by flooded messages and quota-exceeded mailboxes cannot be solved by the end-user filtering. Source-level mitigation by implementing sender-verification methods such as SPF [5] are under development.

3.2 Wireless LAN Security Issues

WLANs based on IEEE 802.11b and other related technologies have been widely deployed at office, home, and public access points such as in airports, train stations, hotels, and urban cafés. WLAN has become an essential medium for Internet access.

While the connectivity without wires largely enhances usability of a portable computer especially where network wiring is restricted, however, some facts based on the nature of WLAN as the follows should be seriously considered:

- Any WLAN device can wiretap into the network exchange, as long as the airwaves transmitted from an access point or a WLAN interface card is decodable. Although mitigation methods by avoid broadcasting ESSID of WLAN access points and using the shared-key encryption called WEP are well-known and implemented, those methods cannot prevent an extensive exploitation by a stealth listening-only device decoding the traffic among the legitimate nodes. WEP has been widely-known as cryptographically weak [6].

- The reachability of airwaves emitted from each WLAN node cannot be precisely controlled as in the case of wired networks. Every node should be considered as a *broadcast device* rather as a point-to-point communication device.
- DoS attacks against the WLAN link can be easily performed by using an ordinary WLAN device [7]. Various unlicensed devices using the 2.4GHz band allocated for WLAN, such as wireless surveillance cameras and microwave ovens, can be a source of a harmful interference which degrades the WLAN communication quality.

To prevent unwanted security incidents by using the WLAN, precautional measures as in the following list should be taken:

- restricting the protocol and access ranges allowed on a WLAN as narrow as possible, which also means to *never* connect a WLAN to a publicly-accessible Internet unless making it a public access point;
- always making the WLAN as low-profile as possible, which means to keep the ESSID secret and to frequently change the WEP key, so that the chance of WLAN to be exploited is minimized;
- *any* WLAN should be considered a *hostile* environment, which means an end-to-end encryption protocol (e.g., SSH and SSL/TLS) or a secure VPN (Virtual Private Network) must be used for a remote access over WLANs.

To summarize, a WLAN should be used only in a well-controlled environment under regular inspection of skilled administrators. Direct exposure of WLAN to a public Internet, such as linking through a WLAN-included router with no proxy capability, should be avoided as possible.

3.3 P2P Software Tools, the Illegitimacy and Vulnerabities

P2P has been one of the hottest trends of Internet, which allows end-to-end communication between independent hosts without intervention of a centralized server. If Web is a set of server-client systems, the P2P systems are doing the best to get away with the server-controlled model.

Unfortunately, current P2P systems are mostly deployed as file exchange or sharing systems among anonymous sources and destinations [*1], which can easily be abused as a medium of illegal duplication of copyrighted items. Napster [8], Gnutella [9], and recently Winny [*2] has been a target of legal persecution against mass copyright infringement [11].

While an uncontrolled anonymous file exchange software may be of little use for teleworking, many lessons as follows are learned from the P2P software incident reports:

- The popularity of Winny and other P2P tools suggest many Internet users expose their computers with little or no protection against incoming connections or packets. Most of the P2P software tools require direct public Internet access, which is not necessarily required for performing most of the teleworking tasks.
- Winny acts as a file distribution cache gathered from anonymous sources. Since the sources are uncontrollable and unidentifiable by the nature of Winny, the administrator of computer running a Winny can unintentionally involve in illegal file trafficking, including copyright infringement.
- Users of P2P tools may erratically expose *any* files in the computer running the tools, often including the sensitive information which can be of legal persecution if disclosed to public [12].

Regarding the above lessons, the general principles of file sharing for teleworking suggested from the P2P software tool incidents are:

- *prohibiting the anonymous posting* to the computer systems whenever possible, including *not* running Web BBSes or blog trackbacks, etc.;
- minimizing the range and people of sharing information, even if the identities are well-known and authenticated;
- blocking incoming connections and packets from external networks, as well as from the *internal* networks, to prevent unauthorized incoming and outgoing traffics.

[*1] The anonymity of P2P system is incomplete; it is provided as a set of computational difficulties to track down the participants.

[*2] No protocol detail of Winny is officially available online, though Winny is told to employ a combination of multi-level proxy and content cache [10], over weak (RC4) cryptographic links.

3.4 VoIP and Teleconferencing

VoIP and teleconferencing tools, such as Microsoft's Netmeeting and Polycom's ViaVideo II [13], can effectively help remote multipoint audio-visual communication. These tools, however, have the following known vulnerabilities and usability issues:

- *No equipment-level encryption* is provided, so the communication channel can be easily wiretapped.
- Since these devices must use direct UDP packet exchange for communicating with each other, exposure to the public Internet is inevitable, especially if a device has to wait for incoming calls. This means those devices are easy target for vulnerability exploits, and at least one vulnerability has been publicly addressed [14].
- Full-duplex audio communication are prone to annoying feedbacks, especially on Netmeeting and other products designed for headset microphones and headphones, which is not capable to perform long-delay echo-cancelling [15].
- VoIP telephone services provided by telephone companies do not guarantee inter-provider connectivity, which can be an annoying restriction between two users subscribing to the different service providers.

To cope with these weaknesses mentioned above, the following methods are suggested:

- Using a teleconference over VPN is strongly suggested to prevent wiretapping. SoftEther [16], a virtual Ethernet linking system over various underlying protocols such as HTTP, can be an effective solution to protect a teleconferencing traffic.
- An application-level protection is provided by a VoIP product called Skype [17], with a strong encryption scheme AES. While skype uses a P2P technology to discover the neighbors, the voice transferred through is protected.
- Disabling the duplex capability will significantly reduce the burden of preventing audio feedbacks. Some VoIP-based tools which relays communication between simplex amateur radio transceivers, such as eQSO [18] and EchoLink [19], only allows one-way simultaneous communication, which contributes to prevent forming feedback loops. While these products are restricted for amateur radio use, similar products which explicitly controls who to speak over a voice channel will become an effective group-conferencing tool.

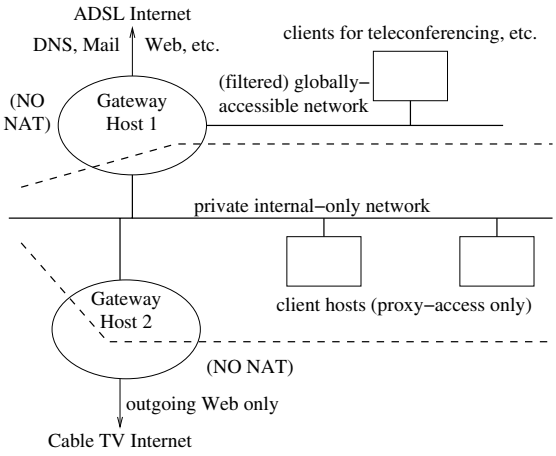

Fig. 2 An example of Internet teleworking system.

4 A Working Example of Internet Teleworking System

Rikitake, one of the authors of this paper, has been running his Internet teleworking system since 1993 from home [20]. Fig. 2 shows the configuration of his home systems as of May 2004. The system is configured on the following principles [21]:

- Expose only trusted systems to the public Internet. The always-connected gateways are built on FreeBSD. For the systems which needs public access to the Internet, they are on a filtered external network segment, used only on a limited basis with full administative attendance.
- Keep untrusted systems, such as the Windows-based client hosts, inside the internal network isolated from the public Internet with the gateway hosts, which only allows limited protocols solely by proxies.
- NAT (Network Address Translation) is *prohibited* to block unwanted connection attempts of internal hosts to external hosts, for preventing uncontrolled external connections.
- WLAN is currently banned inside the house except for an experimental use [22].

While these principles are far from complete, the thorough defensive policy against vulnerabilities has been effectively working since 1993, by succeeding to protect the internal syetems from possible intrusion attempts.

5 Conclusions

In this paper, we described the emerging technologies and the threats of Internet teleworking, and showed a set of practical workarounds to mitigate the vulnerabilies to solve the security issues. For a secure teleworking environment, non-Internet security issues [23] should also be addressed as well.

Acknowledgements

Our thanks go to Mr. Tohru Asami, the president and CEO of KDDI R&D Laboratories, Inc., for supporting our research activities.

References

[1] Cheswick, W. R., Bellovin, S. M. and Rubin, A. D.: *Firewalls and Internet Security*, Addison-Wesley, 2nd edition (2003).

[2] Mail Abuse Prevention System, LLC: MAPS Realtime Blackhole List (RBL). http://mail-abuse.org/rbl/.

[3] Burton Computer Corporation: SpamProbe. http://spamprobe.sourceforge.net/.

[4] Graham, P.: A Plan for Spam (2002). http://www.paulgraham.com/spam.html.

[5] Lentczner, M. and Wong, M. W.: Sender Policy Framework (SPF). http://spf.pobox.com/.

[6] Arbaugh, W. A., Shankar, N. and Wang, J.: Your 802.11 Network has no Clothes, *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, pp. 131–144 (2001). http://www.cs.umd.edu/~waa/pubs/no-clothes.pdf.

[7] AusCERT: Denial of Service Vulnerability in IEEE 802.11 Wireless Devices. AusCERT Advisory AA-2004.02, http://www.auscert.org.au/4091.

[8] drscholl@users.sourceforge.net: Napster Messages (2000). http://opennap.sourceforge.net/napster.txt.

[9] Kirk, P.: Gnutella Protocol Development. http://rfc-gnutella.sourceforge.net/.

[10] tnishita@yahoo.co.jp: P2P Basic (sic). http://homepage3.nifty.com/toremoro/p2p/p2p.html (written in Japanese).

[11] Slashdot.org: Winny P2P Software Creator Arrested (2004). http://yro.slashdot.org/yro/04/05/10/0157259.shtml.

[12] Leyden, J.: Japanese finger virus for police document leak. The Register, 7th April 2004, http://www.theregister.co.uk/2004/04/07/japanese_keystone_cops/.

[13] Polycom, Inc.: ViaVideo II. http://www.polycom.com/products_services/0,1443,pw-35-4368,00.html.

[14] CERT/CC: Multiple H.323 Message Vulnerabilities. CERT Advisory CA-2004-01, http://www.cert.org/advisories/CA-2004-01.html.

[15] Rikitake, K., Kikuchi, T., Nagata, H., Hashimoto, K. and Asami, T.: Solving Management Issues of Inexpensive Internet-VPN Teleworking (written in Japanese), *Human Interface Society HIS2001 Symposium Proceedings*, pp. 593–596 (2001).

[16] SoftEther Corporation: SoftEther. http://www.softether.com/.

[17] Skyper Limited: Skype. http://www.skype.com/.

[18] Davies, P. (M0ZPD): eQSO. http://www.eqso.net/.

[19] Taylor J. P. (K1RFD): EchoLink. http://www.echolink.org/.

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

[21] Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T.: Secure Gateway System Design for Home Teleworking, *IPSJ SIG Notes 2002-CSEC-17*, Vol. 2002, pp. 1–6 (2002).

[22] Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T.: Secure Teleworking over Wireless Internet, *IEICE General Conference Symposium SB-12-3* (2002).

[23] Rikitake, K., Kikuchi, T., Nagata, H. and Asami, T.: Information Security Management under Teleworking Environment (written in Japanese), *IPSJ 63rd National Convention Proceedings*, Vol. 3, pp. 625–628 (2001).