

Potential Security Problem looms for users of PC-based VoIP products

1.0 Introduction



With the growing use of Voice over Internet Protocol (VoIP), even non-dialup users may soon find themselves with huge long distance bills for calls they did not make.

“Modem hijacking” victimizes users of regular dialup modems by enticing them to install a piece of software that promises to enable them to view, play or have access to games, videos, music, psychics or adult sites. If the user agrees with the installation without bothering to understand the fine print, then the modem dialer software gets installed and executed [1,2]. Without any additional permission from the user, the PC is then used to dial to a long distance internet provider number, a 1-900 number, or FTP site, to accrue per-use charges which the user will then be responsible for [3]. The user won’t be aware that his existing internet connection is dropped and that another connection has been redialed because the software will shut off the modem’s speaker [2] or it would wait until the user has moved away from the PC by detecting idle time.

Faced with the charges, the victimized users either pay up or lose their phone service. In the US, people have filed complaints with the FCC and FTC, and in Canada, with the CRTC. Generally though, the phone companies treat these on a case by case basis [5].

2.0 Why Voice Over IP?

VoIP allows you to make telephone calls using a computer network, over a data network like the Internet. VoIP converts the voice signal from your telephone into a digital signal that travels over the internet then converts it back at the other end so you can speak to anyone with a regular phone number. When placing a VoIP call using a phone with an adapter, you’ll hear a dial tone and dial just as you always have. VoIP may also allow you to make a call directly from a computer using a conventional telephone or a microphone [6].

An AT&T paper declares that since voice is now being treated as an IP network application, long distance and local service telephone providers run VoIP for an increasing portion of total traffic to save on circuit and toll costs. It also enables cable operators to offer VoIP and cable telephony services. Innovative IP-based applications like call routing and integrated messaging are written for the IP network. Phone numbers can be location independent and phone calls can be distance independent [7].

VoIP then generally means a win-win for both the consumer and the service provider in terms of costs and available features.

3.0 Emerging Threats - Recommendations

Until now, the modem hijacking victims were limited to dialup internet users because only the regular dialup modems could be used to rack up charges for the unsuspecting user. Presently, users of PC-based dialers of Voice over IP services could potentially find themselves in a similar situation. The fact they don’t even have a dialup modem and that they’re using an ADSL or a cable modem won’t offer them any shielding from this problem.

The old suggestion, “disconnect the dialup modem, you may leave the broadband connection on [4]” as a defence, may no longer hold true. Judging from the relative ease that new hacks are able to exploit Windows weaknesses [3], it is reasonable to expect that a VoIP version of the modem hijacking scam would soon surface.

Although this article is focused on Windows vulnerabilities, this doesn’t mean that Macintosh users are safe. There are enough threats to the Macintosh platform [8]. If a Mac-based VoIP dialer is released, that would certainly be targeted by hackers.

The potential headaches are ominous. Many companies in this field are envisioning major expansions of their VoIP hardware offerings for use in VoIP services. Among them are Texas Instruments [9], where VoIP is viewed as the next “killer app;” Comcast, which is “aiming to offer it to 40 million households by 2006 [10];” and Ace Comm, whose white-

by Dennis Estacion

Queen’s University, Kingston, ON

Abstract

As Voice over Internet Protocol (VoIP) technologies enjoy growing acceptance and increasing use, there’s an expectation that a variant of the modem hijacking problem that used to affect only the dialup modem users may soon surface. Those using PC-based VoIP dialers whose computer’s security weaknesses have been exploited could find themselves with significant VoIP long distance charges for calls they did not place. It is important that this issue be considered now to avoid problems for the users faced with the disputable charges; and for the VoIP service providers and government agencies who will have to deal with the resulting complaints. This article investigates the existing types of VoIP service offerings, cites some examples and assesses how vulnerable the user of each type could be. It then provides recommendations of what the service providers should make available to the users to help minimize any impact.

Sommaire

Comme les technologies de voix sur IP (VoIP) sont de plus en plus acceptées et utilisées, il est possible qu’une variante du problème de détournement de modem, qui n’affectait autrefois que les usagers de modems RTC, surgisse. Un usager de VoIP pourrait faire face à d’oùneux coûts d’interurbains pour des appels dont il/elle n’a pas eu connaissance si les faiblesses de son ordinateur ont été exploitées par des tiers. Il est donc important que cette problématique soit traitée dès maintenant pour éviter des problèmes potentiels tel qu’un usager qui reçoit des factures d’interurbains discutables et les compagnies de service VoIP et les agences gouvernementales qui doivent répondre aux plaintes. Le présent article présente une étude des différents types de services VoIP, cite quelques exemples et détermine le degré de vulnérabilité de l’usager pour chaque type de service. L’article propose aussi des recommandations quant aux solutions possibles au problème.

paper quotes a source that the worldwide VoIP equipment market for public networks will surpass US \$20 billion by 2012 [7].

Not all VoIP service providers are offering PC-based VoIP dialers, but it is hoped that if they do, that consumers are:

- Forewarned of the risks,
- Provided with tools to secure the VoIP dialer, and/or
- Provided with easier recourse procedures on how to contest questionable charges [2, 5].

From the Windows side of things: “Microsoft continues on its path of incorporating much of the nuts-and-bolts functionality now handled by third-party communications vendors -- like chat, Web conferencing, and VoIP players -- on the operating system level [11].” The current Microsoft white paper on VoIP mainly deals with Windows CE version 5 [12].

VoIP dialers therefore don’t rely on Microsoft (or Apple)-supplied utilities but are applications by themselves. The security of the VoIP dialer then depends on its own security features and that of the underlying Windows or Macintosh OS.

From what is now available, VoIP services could be categorized as follows in terms of being prone to a broadband modem hijacking scheme:

1. Dedicated VoIP hardware used exclusively with no need of a PC. This would be the safest. Users keep it secure the same way they keep their regular phone secure (i.e. be aware where is the portable handset, for example). An example would be the service provided by Primus Canada [13].
2. VoIP hardware with the option of using PC-based VoIP dialer. The hardware portion should be as secure as the one above, but users availing of the Windows-based dialer could expose themselves to upcoming threats. An example of an optional dialer would be the SoftPhone X-PRO utility which is the VoIP dialer included with the service provided by Vonage [14, 15].

A quick look at its features indicates that there is an option to block international call dialing, which should alleviate some concerns. Connection to 1-900 numbers is also not allowed [16]. However, the quick start guide for SoftPhone X-PRO [17] recommends allowing the software to remember the login phone number and password fields. This author did not check further if login access to SoftPhone would allow changes to the call blocks, but it would suffice to say that this may make it vulnerable to take-over tools, key-stroke monitors and other exploits. It is also to be noted that even though long distance and 1-900 call blocking have been available for the regular phone lines, people have not opted for them and so have been victimized.
3. PC-based VoIP dialer with option of using VoIP hardware. Being mostly reliant on the underlying PC operating system, it's more vulnerable to take-over tools, keystroke monitors and other exploits as mentioned above. An example would be the PC-to-Phone service of the iConnecthere consumer division of deltathree [18].

4.0 Concluding Remarks

In summary, broadband internet users availing of PC-based VoIP dialers need to be made aware of the possible risks arising from the PC's security vulnerabilities. They should be provided with step-by-step procedures that minimize the chances of success of any Windows or Macintosh hack or exploit. And if they still got victimized despite their best efforts, they should be accorded a smoother process to be spared the resulting disputable charges.

5.0 References

- [1]. Modem hijackers lurk on the Internet: <http://www.royalcityrecord.com/issues03/014203/news/014203nn11.html>
- [2]. Internet scam saddles victims with huge phone bills: <http://www.thewhig.com/webapp/sitepages/printable.asp?paper=www.thewhig.com&contentID=65692&annewspapername=The+Kingston+Whig-Standard>
- [3]. List of Expanded threats from Symantec web site: http://securityresponse.symantec.com/avcenter/expanded_threats/index.html
- [4]. How an online scam could run up your phone bill: http://reviews.cnet.com/4520-3513_7-5087866-1.html
- [5]. Filing a Complaint with the FCC <http://www.fcc.gov/cgb/consumerfacts/ModemScam.html>
- [6]. FCC VoIP FAQ: <http://www.fcc.gov/voip/>
- [7]. A number of VoIP-related white papers are available at: <http://www.voip-news.com/wp/wphome.html>, including those from AT&T, Ace Comm, Cisco, Lucent and Siemens.
- [8]. Virex for Macintosh: <http://www.mcafeesecurity.com/us/products/mcafee/antivirus/desktop/virex.htm>
- [9]. A Talk with TI's Rich Templeton: http://www.businessweek.com/bwdaily/dnflash/aug2004/nf2004086_0173_db008.htm
- [10]. Comcast: More Than Buffett Is Behind It: http://www.businessweek.com/bwdaily/dnflash/aug2004/nf20040823_3426_db035.htm
- [11]. Microsoft VoIP Introduction: <http://download.microsoft.com/download/b/0/6/b06e9c6e-cf9c-481f-a6ed-c674e82ed1d1/VOIP.doc>
- [12]. Microsoft Hangs Up on VoIP in Messenger: <http://www.instantmessagingplanet.com/public/article.php/1593651>
- [13]. Primus TalkBroadband FAQ: <http://www.primus.ca/en/residential/talkbroadband/faq.html>
- [14]. Vonage SoftPhone: <http://www.vonage.com/features.php?feature=softphone>
- [15]. Copy of Vancouver Sun, April 16, 2004 article: Internet Phone Service Battle On: Second Firm in Market Likely to Be Forerunner of many at: http://www.vonage.com/corporate/press_news.php?PR=2004_04_16_2
- [16]. Vonage does not provide service to toll area codes such as 900, 700, 500, etc; http://www.vonage.com/help_knowledgeBase_article.php?article=430
- [17]. Quick start guide for SoftPhone X-PRO: <http://www.vonage.com/identity/vonage/pdf/xpro-quickstartguide.pdf>
- [18]. How PC-to-Phone Works: http://www.icconnecthere.com/Non-Members/eng/popups/popup_pcp_dev.html

About the author

Dennis Estacion, BS in EE from the University of the Philippines, is a Technology Analyst with TELUS providing IT support. He is currently pursuing an MBA degree at Queen's University, Kingston, Ontario. He is also an MCSE on Windows 2000; an MCSE + Internet on Windows NT 4.0; and a Subject Matter Expert for CompTIA's A+ and Network+ Certification Programs. Previously, he has worked for IBM Canada, HP Canada through OAO Technologies, and General Dynamics through CSC Canada. His current interests include IT Security and Business Management.



Quelques mots du rédacteur en chef

Suite de la page 3:

autres, pour la traduction d'articles en français. Merci à Bob Alden pour avoir implanté le site Internet de la revue canadienne et avoir réalisé un si bon travail. Et merci à Bruce Van-Lane et son équipe pour leur soutien à l'édition.

Finalement, un gros merci à Vina pour avoir passé de longues heures à réaliser l'éditique, taper et re-taper, finaliser, expédier et organiser en général la revue canadienne. Ça n'aurait certainement pas été possible sans son soutien et habiletés. Aussi, pour m'avoir enduré durant ces longues heures quand j'étais loin de la maison et je négligeais mes autres tâches. Elle a été la colonne vertébrale de tout ce travail.

Ce fut un privilège et un honneur de servir en tant que rédacteur en chef de ce prestigieux magazine. Je remercie tous les lecteurs et les membres d'IEEE Canada qui m'ont rejoint par courrier électronique ou par la poste, et m'ont livré des messages d'encouragement et des suggestions pour améliorer la revue.

Je souhaite bonne chance et beaucoup de succès aux nouveaux rédacteurs de la revue canadienne (voir leurs profils dans ce numéro). A vous tous lecteurs et membres, je souhaite une bonne et heureuse année.

Vijay Sood
Redacteur en chef