Is the Federal Government Making VoIP Safer?

JONATHAN E. MEER

As Voice over Internet Protocol (VoIP) has increased in popularity and become a mainstream communications technology with more than eight million subscribers,[1] concerns have emerged about its security. VoIP technology has created security concerns in the past but recently such threats have extended beyond VoIP users to all telephone users. Incidents of spoofing (the use of fake caller ID information to defraud), denial of service, spamming over Internet telephony, and phreaking (breaking into the telephone network illegally) are becoming more widespread with VoIP. The federal government has begun to take action.[2] For example, on June 13, 2007, the House of Representatives unanimously passed a bill that would make caller ID spoofing a violation, punishable by $10,000 per each occurrence up to $1 million.[3] But does this latest legislative attempt to secure VoIP make the technology safer for phone calls? This article reviews the security threats that have arisen with VoIP and the federal responses to them.

Theft of Service

One early security issue that emerged from the widespread use of VoIP was phreaking, i.e., the theft of phone calls. Phreaking, a term that originated from the use of various audio frequencies to manipulate a phone system, has become widespread with the growing use of VoIP. The most notorious case of phreaking took place in 2006 and led to the arrest of Edwin Pena, who hacked into the computer networks of unsuspecting VoIP service providers to reroute his customers' calls. Pena sold more than ten million minutes of service at deeply discounted rates, netting more than $1 million from the scheme.[4] Stealth Communications reported that in 2007, thieves steal 200 million minutes a month, worth $26 million, by selling them to smaller telecoms that either sell printed phone cards or operate call centers.[5]

Although phreaking is not limited to VoIP, the latest rash of this crime has been through phone services on the Internet. Phreakers are stealing minutes and reselling them on the black market, but societal demands for faster phone lines has curbed this crime somewhat with the expansion of the traditional telephone network to T1 lines, which are commonly leased to Internet service providers.[6] However, updating the networks still has not stopped the external threat of phreakers using illicit phreaker programs to attack small telecoms, which many times lack the money for a secure gateway server that connect a carrier's telephone network to the Internet.[7]

Today, VoIP companies are placing the onus on consumers to uncover theft of service. Many VoIP providers include in their service contracts a provision that the consumer will be liable for all use of the service and "any and all stolen Service or fraudulent use of the Service" until the VoIP provider is notified.[8] Some companies have turned to private VoIP networks, instead of the public Internet, to protect themselves from phreakers.[9] Companies also use user verification and cryptographic capabilities to protect their VoIP clients.[10] Other growing protections include firewalls, encryption, and other software-based measures similar to those used for data security.[11]

Vishing

Although traditional concerns over VoIP safety come from the theft of service, new security concerns exist for all telephone users because of VoIP. A prevalent security issue with VoIP is voice fishing, also known as "vishing," which is the making of phone calls to solicit potential victims and gain access to their personal information. Fraudulent telephone calls soliciting personal information are not new. However, vishing has become even more of a problem because VoIP phone numbers and ID can be established without the same level of verification required on a traditional phone line.[12] For instance, some incidents of vishing involve criminals using a phone number with a similar area code, even the same prefix, as a local bank and tricking victims into offering their personal information.[13]

Some criminals have gone so far as to fool telephone identification services by taking on a completely different name and number through the use of legitimate software created to protect privacy and using it for illegal activities.[14] The *Washington Post* has collected a number of anecdotal reports about spoofing scams with misleading Caller ID and 1-800 numbers. These include calls threatening a bench warrant for failure to appear for jury duty and scams that warn of a violation of Bank of America's Acceptable Use Policy and then requests the account holder's PIN.[15] In Jefferson City, Missouri, more than 1,000 people received a phone call that appeared to be from a local bank, with the caller ID showing the bank's customer service line. The customers were told that their accounts would be deactivated unless they provided their personal information to the caller.[16] Although some customers did provide personal information, the bank was notified of the scam before the alleged criminals absconded with any funds.[17]

Government Regulation

The federal government has taken control of VoIP regulation. In 2004, the Federal Communications Commission (FCC) ruled that Vonage and its use of VoIP technology are exempt from state and local regulation.[18] On March 21, 2007, the U.S. Court of Appeals for the Eighth Circuit in *Minnesota Public Utility Commission v. FCC* upheld the 2004 FCC ruling, which bars states from regulating Internet-based phone services.[19] The court determined that because VoIP telephone calls can be made from nearly anywhere and are thus an interstate service, no single state can appropriately regulate VoIP services.[20] This ruling reaffirmed the federal government's responsibility to take action to make VoIP technology safe for the general public.

Congress has generally deferred the regulation of VoIP to the FCC although it has passed or considered some legislation that impacts VoIP. For example,

Jonathan E. Meer (lawclerk.lombardi@judiciary.state.nj.us) is the law clerk to the Honorable Sebastian P. Lombardi of the New Jersey Superior Court.

in 2004, both the House and the Senate considered bills that would disallow states to regulate VoIP or limit the FCC's authority to regulate VoIP, but neither bill was adopted.[21] In 2004, the FCC blocked the Minnesota Public Utilities Commission from applying its traditional telephone company regulations to Vonage service. This exempted the VoIP service provider from complying with the state's laws and regulations governing a "telephone company," such as those dealing with authority, tariffs, and 911 emergency services.[22]

The Telecommunications Act of 1996 mandated that VoIP be defined as either a telecommunications service similar to an incumbent or competitive telephone company, or as an information service exempt from state regulations.[23] The 2004 FCC order clarifies that VoIP providers are to be considered providers of information services, not telecommunications carriers as defined by the Telecommunications Act.[24] Still, Congress has proposed bills that do have the indirect effect of addressing VoIP service. H.R. 251, which would impose fines for spoofing, is currently before the Senate.

The FCC has taken steps to regulate VoIP, but many issues regarding privacy and security still remain. One early regulation of VoIP concerned 911 capabilities.[25] The FCC imposed Enhanced 911 (E911) obligations on providers of interconnected VoIP services, requiring the network to automatically provide a 911 caller's originating number and, in most cases, location information to emergency service personnel.[26]

In addition, VoIP providers must contribute to the Universal Service Fund that supports communications services programs such as E-Rate, which provides Internet access to public schools and libraries.[27] Further, the FCC requires VoIP providers to comply with the Communications Assistance for Law Enforcement Act (CALEA) of 1994. CALEA allows enforcement agencies to conduct electronic surveillance as similarly required for all traditional telephone providers.[28] This FCC requirement was reaffirmed in 2006, clarifying that May 14, 2007, was the CALEA compliance deadline for facilities-based broadband Internet access and interconnected VoIP services.[29] However, neither of these steps addressed regulations securing VoIP.

Future Regulation

With VoIP still largely unregulated, the next issue that the federal government will likely address in increasing the medium's security is Customer Proprietary Network Information (CPNI). CPNI is data specific to individual customers generated when customers make calls, including call detail records, call volumes, customer account information, billing information, technical information, service destination, and the service plans to which a customer subscribes.[30] Some industry insiders believe that with a little detective work, CPNI data can reveal customers' Internet service provider.[31]

The Telephone Records and Privacy Protection Act, which Congress passed last year, amended the federal criminal code to prohibit obtaining, or attempting to obtain, confidential phone record information from a telecommunications carrier for all phone customers, including VoIP subscribers.[32] In 2006, the Prevention of Fraudulent Access to Phone Records Act was proposed in Congress and was resubmitted in 2007.[33] This is one of the bills proposed to create new consumer data protection laws by placing stricter requirements on the collection of personal information. Privacy advocates and companies are at odds on the proposed national guidelines and their effect on states' regulation of privacy, but a bill such as the Prevention of Fradulent Access to Phone Records Act could provide a baseline of expected consumer protection.[34] Although the proposed act does not directly address VoIP, it seeks to address CPNI protection measures used by telecommunications carriers.[35] The act would permit a telecommunications provider to use aggregated data for its own usage, such as to improve service and solicit new business, but would require customer information to remain private.[36] The proposed measures include: (1) requiring telecommunications carriers to institute customer-specific identifiers to access CPNI; (2) encryption of CPNI or other safeguards to secure the data; and (3) deletion of CPNI after a reasonable period of time if storage is no longer necessary.[37] Representative John Dingell, chairman of the House Committee on Energy and Commerce, is optimistic that the Act will be brought to the House floor in 2007, and a similar bill is proposed in the Senate.[38] In summary, these proposed measures would require greater verification to access a person's proprietary information.

Conclusion

The recent proposals by Congress to regulate use of CPNI, impose the Records Privacy Act, and criminalize spoofing reflect the government's concern about the security issues present in VoIP usage. As our information society becomes more interconnected, these security issues must be addressed. As more people use VoIP for their telephone calls, the need for regulations and legislation protecting against the dissemination of private information and preventing fraud continues to increase.

Endnotes

1. Matt Richtell, *Skype's New Unlimited Calling Plan*, N.Y. TIMES, Dec. 13, 2006.

2. Nadeem Unuth, *Security Threats in VoIP*, at http://voip.about.com/od/security/a/SecuThreats.htm.

3. *Bill Targets ID Theft,* WAXAHACHIE (TX) DAILY LIGHT, June 13, 2007.

4. Preston Gralla, *The Inside Story of A Million-Dollar VoIP Scam*, Networking Computing, June 8, 2006, *at* www.networkcomputing.com/channels/networkinfrastructure/188702745; Sharon Gaudin, *Accused VoIP Fraudster Sought as Fugitive*, INFO. WK., Sept. 15, 2006.

5. Benjamin Sutherland, *Stealing the Minutes*, Newswk., Mar. 19, 2007.

6. *History of Phreaking*, at http://passivemode.net/phreaking; s*ee also Telecommunications Tutorial Guides*, *at* www.infosyssec.org/infosyssec/security/teletut1.htm.

7. Sutherland, *supra* note 5.

8. Axis VOIP Terms of Service, *at* www.axint.net/tos; Speakeasy VoIP Service Subscriber Agreement Highlights, *at* www.speakeasy.net/tos/voip.php.

9. *Id.*

10. Kevin Murphy, *Is VoIP a Security Risk?*, COMPUTER BUS. REV. ONLINE, Mar. 30, 2006.

11. Paul D. Kretkowski, *How Secure Are Your VoIP Calls?*, VOIP NEWS, Jan. 2, 2007.

12. *Just when you thought it was safe: Vishing makes a splash on the Web*, Emory Federal Credit Union Identity Theft Resolution Serv., *at* www.emoryfcu-identitytheft911.com/articles/article.ext?sp=707.

13. *Id.*

14. Mike Musgrove, *New Tricks Fool Caller ID*, WASH. POST, Oct. 30, 2004, at E01.

15. Brian Krebs, *'Vishing': Dialing for Dollars*, WASH. POST, June 26, 2006, *at*

http://blog.washingtonpost.com/securityfix/2006/06/vishing_dialing_for_dollars.html; Brian Krebs, *'Vishing': Dialing for Dollars*, WASH. POST, Mar. 8, 2007, http://blog.washingtonpost.com/securityfix/2007/03/vishing_dialing_for_dollars_pa_1.html.

16. Michelle Brooks, *Warning! Scam to Steal Personal Information Shows Bank on Caller ID*, JEFFERSON CITY NEWS TRIB., Mar. 1, 2007.

17. *Id.*

18. Carson Carlson and Ryan Naraine, *FCC: VOIP Is Not Subject to State Rules*, EWK., Nov. 9, 2004, *at* www.eweek.com/article2/0,1895,1748815,00.asp; Vonage Holdings Corp. v. Minn. Pub. Utils. Comm'n, 394 F.3d 568, 569 (8th Cir. 2004).

19. Minn. Pub. Utils. Comm'n v. FCC, 2007 U.S. App. LEXIS 6448 (8th Cir. 2007).

20. Patrick Condon, *Court Backs FCC over States in VoIP Case*, HOUS. CHRON., Mar. 21, 2007.

21. Roy Mark, *Congress Hangs Up on VoIP for 2004*, Internet News, Sept. 3, 2004, *at* www.internetnews.com/bus-news/article.php/3403911.

22. 19 FCC Rcd 22404 (FCC 2004).

23. *Id.*

24. *Id.*

25. Fed. Communications Comm'n, E911 Requirements for IP-Enabled Service Providers, May 19, 2005, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-116A1.pdf.

26. FCC Consumer Advisory: VoIP and 911 Service, *at* http://ftp.fcc.gov/cgb/consumerfacts/voip911.html.

27. Anne Broache, *FCC Approves New Internet Phone Taxes*, CNET NEWS, June 21, 2006, http://news.com.com/FCC+approves+new+Internet+phone+taxes/2100-7352_3-6086437.html.

28. Communications Assistance for Law Enforcement Act and Broadband Access and Services, FCC, Aug. 5, 2005, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf.

29. Press Release, Federal Communications Comm'n, FCC Adopts Order to Enable Law Enforcement to Access Certain Broadband and VoIP Providers, May 3, 2006, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-265221A1.pdf.

30. K.C. Halm, *Expanded Privacy Obligations for Telecom Carriers and VoIP Providers Under Consideration at the FCC*, *at* http://www.privsecblog.com/archives/federal-regulation-expanded-privacy-obligations-for-telecom-carriers-and-voip-providers-under-consideration-at-the-fcc.html.

31. *CPNI–The Gold Mine under LECs*, MEASURE X, May 12, 2006, *at* http://www.measure-x.com/newsletter/42.html.

32. Telephone Records and Privacy Protection Act, 18 U.S.C § 1039 (2006).

33. Prevention of Fraudulent Access to Phone Records Act, H.R. 4943, 109th Cong., 2d Sess. (2006); Prevention of Fraudulent Access to Phone Records Act, H.R. 936, 110th Cong., 1st Sess. (2007).

34. Matt Hines, *Debate Lingers over Federal Data-Handling Laws,* INFOWORLD DAILY NEWS, Apr. 3, 2007, *at* http://www.infoworld.com/article/07/04/03/HNfeddatasec_1.html.

35. *Hearings on Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act*, 110th Cong., 1st Sess. (Mar. 7, 2007) (statement of Marc Rotenberg, President, EPIC).

36. Prevention of Fraudulent Access to Phone Records Act, H.R. 936, § 203(h)(1)(B).

37. *Id.* § 201.

38. *Dingell Releases SEC Response on Hewlett-Packard Probe; Pledges Action on Pretexting Legislation*, STATES NEWS SERV., Apr. 13, 2007. Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. 1st Sess.