VoIP and Skype Security

By Simson L. Garfinkel

Introduction: VoIP and Skype

With the increased deployment of high-speed ("broadband") Internet connectivity, a growing number of businesses and individuals are using the Internet for voice telephony. This technique is called Voice over Internet Protocol (VoIP).

All telephone systems in the world use a microphone to turn sound waves into an electrical signals and a speaker to turn electrical signals back into sound waves at the other end. But the techniques used for connecting microphones and speakers has seen considerable development over the past one and a quarter centuries. Early systems connected the microphone directly to the speaker using a copper wire. In the 1970s AT&T deployed the first systems that could transmit multiple phone calls over a single wire by converting each phone call into a stream of digital data. VoIP systems continue this evolution by taking independent digital streams, compressing them, breaking the streams into packets, and sending those packets over the Internet. Naturally, the process is reversed at the receiving end.

With a VoIP system two people can speak with each other by using headsets and microphones connected directly to their computers. Alternatively, a VoIP adapter can be used to convert electrical signals from a standard analog telephone to Internet packets. VoIP gateways interconnect the Internet-based systems with the world-wide Public Switch Telephone Network (PSTN). Typically there is a fee for using such gateways. Companies like Vonage sell consumers a package that includes a VoIP adapter and use of the Vonage VoIP gateway, giving Vonage customers the illusion that they have a standard PSTN telephone --- the only difference being that the Vonage adapter connects to a cable modem or home network, rather than connecting to a pair of wires that leads back to the telephone company's central office.

There are many different and generally incompatible techniques for sending voice over the Internet. The International Telecommunications Union standard H.225 provides for voice and video teleconferencing; the Internet Engineering Task Force adopted an incompatible system called Session Initiation Protocol (SIP). Cisco developed a proprietary system called the Skinny Client Control Protocol (SCCP). An excellent overview of VoIP standards can be found at [6].

Skype is a proprietary VoIP system developed by Skype Technologies S.A., a corporation that claims to be registered in Luxembourg. The company was founded by Janus Friis and Niklas Zennstrom [1], the same entrepreneurs who developed the popular KaZaA file trading system. Like KaZaA, Skype is based on peer-to-peer technology: instead transmitting all voice calls through a central server, as Vonage does, Skype clients seek out and find other Skype clients, then build from these connections a network that can be used to search for other users and send them messages. But unlike KaZaA, which earns its revenue from advertisements, the Skype is currently free of adware and spyware. Instead, the Skype system earns revenue by charging for the use of the gateway that interconnects the Skype network with the PSTN.

Skype vs. Other VoIP Systems

Several key factors distinguish Skype from other VoIP systems:

1. Skype is wildly popular. Within its first week of operation in August 2003, more than 60,000 people downloaded the Skype client. Today Skype is available for Windows, MacOS, PocketPC and Linux, In October 2004 Skype's creators boasted more than a million users.

2. Both the Skype software and use of the Skype network is free; there is a nominal charge for calls made using the "Skype Out" and "SkypeIn" features that connect Skype to the PSTN network.

3. Skype is much easier to use than other VoIP systems. The Skype client is easily installed. Other than choosing a username, no configuration is required. And unlike the SIP system used by Vonage, Skype clients readily work behind firewalls and Network Address Translation (NAT) systems.

4. Skype has an astonishingly good voice compressor, giving it fidelity that in many cases surpasses traditional telephone systems when Skype is used with a high bandwidth connection.

5. In additional to voice telephony, Skype supports instant messaging, search, and file transfer

6. Skype is encrypted. Unlike traditional telephony and other VoIP-based systems, Skype claims to encrypt all communications with 128-bit or better cryptography ciphers, allegedly making it impossible for someone who passively intercepts a Skype conversation from deciphering or listening to its contents.

Skype vs. ISDN

ISDN is another form of digital telephony system that is popular in Europe and Asia. ISDN is similar to VoIP in that voice is digitized before it is sent over the network, and because ISDN telephone lines require special instruments in order to use them. ISDN lines can also be used for teleconferencing.

Voice calls placed over Skype are different from calls placed over ISDN telephones in several important ways:

1. While Skype uses the Internet, ISDN uses the PSTN.

2. While Skype is encrypted, ISDN phone calls are generally not encrypted unless special-purpose encrypting ISDN telephones or fax machines are used. (Such equipment is commercially available but is generally restricted.)

3. While Skype is free, ISDN phone calls are rarely free.

4. Skype does not support video conferencing, a feature found on both many ISDN systems and Apple's iChat.

Overall, Skype appears to be an exceptional value for individuals and organizations that need high quality voice communications and have access to broadband Internet service.

Skype vs. Peer-to-Peer

Although Skype uses peer-to-peer communications for locating other Skype users and for transmitting voice communications, there are many aspects to Skype that make it different from a "pure" peer-to-peer system:

1. Skype relies on a central authentication server to authenticate users and software distributions.

According to Skype's publicist, both user identities and software distributions are digitally signed by an RSA private key. The matching RSA public key is embedded into every Skype executable.

2. Some Skype "peers" are actually "super-nodes." When Skype is run on a computer that has a public IP address and is not otherwise behind a firewall, it can become a "super-node." These computers are used as rendezvous points so that computers behind firewalls can receive connections from other Skype users. Although Skype refuses to explain the details of their protocol, it is likely that computers behind firewalls scan the Internet looking for super-nodes, then form and maintain long-term connections with these other computers. The super-nodes then proxy connections to the encumbered connections behind the firewalls.

3. When the SkypeIn or SkypeOut features are used, these communications necessarily go through Skype's servers located in various countries and dialing areas.

Skype vs. KaZaA

KaZaA is a popular file trading program. Although some of the files that are traded over KaZaA are exchanged with the permission of the copyright holders, it appears that the primary use of KaZaA appears to be the illegal exchange of copyrighted songs and movies.

KaZaA and Skype appear to be related businesses. The companies were founded by the same individuals, there appears to be an overlap in the technical staffs, and much of the technology employed in Skype was originally developed for use in KaZaA. Version 3.0 of the KaZaA includes a Skype client; KaZaA 3.0 can make and receive voice calls through the Skype network.

Two versions of KaZaA are distributed. A free version of the program is supported through advertising, while a version costing approximately US$25 is distributed that does not have advertising. The advertisements displayed in the free version of KaZaA are displayed by software developed by a company called GAIN. This software has often been called “spyware” because it monitors the websites that a computer user visits and displays advertisements related to the website. KaZaA disputes the claim that GAIN is spyware: they assert that the program does not capture keystrokes, analyize files on the users’ hard disk, or report user-identifiable information back to third parties. What’s more, the software can be easily removed using the standard Windows Add/Remove feature.

It seems unlikely that GAIN has an impact on either the privacy or the security of phone calls made from Skype users to KaZaA 3.0 users: there is no practical way that the contents of a conversation could be “data mined” for displaying of targeted advertisements without having them monitored by a human being, and the cost of such monitoring would be prohibitive compared to any possible advertising revenues.

Nevertheless, Open Society organizations should avoid using KaZaA in general. Because KaZaA is used primarily to trade files against the wishes of copyright owners, it is highly likely that the users of computers running KaZaA will accumulate illegal copies of songs and movies. It is ill-advised for any organization to permit such information to be present on its computer systems because of the potential legal liability that such collections present.

Skype over Dial-Up

Skype was tested over an analog telephone line connected to a dial-up ISP at 26kbps. At this speed Skype's voice quality was significantly degraded. However, Skype did provide acceptable voice quality for a two-way phone conversation that could be understood.

In order to be used over a dial-up telephone line, it is advisable to turn off all other programs that might also try to use the Internet connection. Internet browsers and programs that check mail should be exited, for example. Skype will also work better if the conversant are careful to avoid speaking at the same time, as this will minimize bandwidth requirements.

Used in this manner over a low-speed dial-up line, Skype offers sound quality that is noticeably inferior to a normal analog telephone lines. Nevertheless, Skype still has the advantage of low-cost and security as the result of encryption. In situations where international calls are prohibitively expensive or where eavesdropping by government or telecommunications officials is a serious concern, this use of Skype should be encouraged.

Skype Security

Is Skype secure? Is the program safe to use? Is Skype more secure than a telephone call made with an analog or ISDN telephone? How does the security of Skype compare with other VoIP-based systems?

Answering these questions is difficult. Security is not some abstract quality that can be analyzed in isolation: to evaluate the security of Skype it is necessary to consider specific threats and to then to determine whether or not the design or operation of Skype will protect from those threats.

What's more, a security analysis of Skype is complicated by several factors. First, the overall security of a Skype conversation depends on many factors, including the security of the computer on which Skype is running and the network over which the Skype conversation follows. Second, because the Skype protocol is both proprietary and secret, the only sources of information are statements from the company about its security and what can be found by reverse-engineering the software. Third, because Skype is mostly a peer-to-peer system, the overall security can be affected by third parties that are in the network (but that are unknown to those in a particular phone conversation). Finally, because the Skype program can update itself every time it runs, the security over the overall system can change without warning or even a change in appearance.

For a civil society organization relying on Skype for voice communications, the following security properties are of key importance:

Privacy Does the Skype system allow an outsider to eavesdrop on a conversation?

Authenticity If you initiate a Skype conversation with another user, are you sure that you are reaching the user whose username you specify?

Availability Does Skype always work if both participants are on the Internet, or can there be cases were you cannot see another Skype user, even if both are logged in? Can an in-progress conversation be interrupted?

Survivability If the network or Skype infrastructure is disrupted or otherwise damaged, can Skype users continue to communicate while the network is damaged?

Resilience If the network or Skype infrastructure is disrupted or otherwise damaged to the point that Skype does not function, can Skype users quickly reestablish communication with each other?

Integrity (Conversation) Does Skype loose bits of a conversation in progress? Are files that are transmitted delivered intact?

Integrity (System) How does the use of Skype affect other applications running on the user's computer and network? Other peer-to-peer programs come with spyware; does Skype?

In an attempt to answer these questions, I exchanged a series of email messages with Kat James, Skype's designated public relations contact for national media in the United States, Toivo Annus, a Skype developer, and Kelly Larabee, another Skype press officer. I also had a brief telephone call with Kelly Larabee. I also performed a preliminary analysis of the over-the-wire Skype protocol by capturing all of the packets sent to or from a computer running the Skype software before, during and after a Skype call was made.

Privacy

In line with the claims of its creators, Skype appears to encrypt or otherwise scramble information that is transmitted over the Internet. That is, in analyzing the packets of the communication, I was not able to easily view the unencrypted plaintext of my communications. But while I can confidently state that Skype is secure against casual snooping, I cannot say if Skype is secure against a sophisticated attacker.

The security of data sent over an encrypted or scrambled connection depends on many factors, including the specific encryption or scrambling algorithms used, how encryption keys are chosen or exchanged (known as *key management*), the implementation of the algorithms, the protocol that employs the algorithms, and the implementation of the algorithms and protocols in the software.

An analysis of the packets sent between Skype clients indicates that a combination of protocols are used for registering on the network, searching for other participants, and performing a voice telephone call. The program appears to use a version of the HTTP protocol to communicate with the Skype server "ui.skype.com" (apparently located in Amsterdam) to perform username/password authentication and register with the Skype directory server. A modified version of the HTTP protocol is used for communicating with other Skype clients. Finally, an encrypted, proprietary conversation is used for transmitting voice, instant messages, and files.

Using a Macintosh running Skype, I placed a call from Boston, Massachusetts, USA to Budapest, Hungary, over which several instant messages were sent and a file was transferred. All packets were captured. Analyzing the packets I learned that my Skype client in Boston first contacted a computer in the United Kingdom, apparently to check to see if it had the latest version of the Skype client, then to conduct a search of the Skype network for my desired respondent.

(The techniques that Skype uses for searching and directory management are similar to a system called PeerEnabler from Joltid, a company that "consist of the original management and development team behind KaZaA and the FastTrack peer-to-peer network."[5] Skype's media contacts insist that Skype does not actually use the PeerEnabler or FastTrack network, but instead uses a different program that accomplishes similar features.)

After the search completed, a series of packets were exchanged with the destination computer in Hungary for the duration of the call. All of these packets were indecipherable to me. This could be because they were encrypted, otherwise scrambled, or simply compressed with an undocumented compression system.

My conclusion from an analysis of the captured packets is that while the actual communications between Skype clients appears to be encrypted, searches conducted on behalf of Skype users --- including searches necessary to initiate Skype calls --- are observable by the Skype network. This means that it should be possible for even unprivileged participants of the network to perform traffic analysis and determine when one user calls another user. It is unknown if the design of the Skype network makes it possible for some nodes to monitor all searches and call set-up traffic, or if instead each node would only see a portion of the overall traffic.

What if Skype Really Does Use Encryption?

Skype claims that its system uses the RSA encryption algorithm for key exchange and 256-bit AES as its bulk encryption algorithm. However, Skype does not publish its key exchange algorithm or its over-the-wire protocol and, despite repeated requests, refused to explain the underlying design of its certificates, is authentication system, or its encryption implementation. Therefore it is impossible to validate the company's claims regarding encryption. It is entirely possible that the data is both encrypted and not secure.

Even if the Skype protocol does provide for encryption, it is possible that the Skype system could transmit the encryption keys with the voice channel (perhaps encrypted with another set of keys), or else archive the keys on the user’s hard disk. Access to these encryption keys would make it possible for a third-party to decode a recorded Skype conversation. Such key escrow capabilities could be built into Skype either for testing purposes or at the request of either police or intelligence services. Even if Skype does not currently have such monitoring features, they could be added to Skype at some future point in time and the modified client then distributed over the Skype network --- either to all users, or else to users that had been specifically chosen to meet some criteria.

Skype could use encryption, but use it poorly. Even though Skype really does use RSA, a poor implementation of the algorithm could provide no actual security. Because Skype has not published its protocol, it is not possible to say if the protocol that uses RSA is secure or not.

These concerns need to be taken in context. A conversation on Skype is vastly more private than a conversation using a traditional analog or ISDN telephone. Those conversations can be monitored by anyone who has physical access to the telephone line at any point between either party.

Skype's "Encryption" in Context

Skype is also more secure than today’s VoIP systems, since encryption is not part of most VoIP offerings. However, it is possible to protect a VoIP conversation by running the VoIP traffic over a Virtual Private Network. A system using VoIP over a VPN is probably more secure than Skype, assuming that the VPN was properly configured.

It is important to realize that the security of Skype can be subverted through the use of spyware or other kinds of monitoring programs running on the user’s computer. For example, programs like Netbus and Back Orifice can allow an outsider to turn on the microphone of a PC and transmit the audio to a remote location on the Internet. Such a program could spy not only on a Skype conversation, but on every other conversation taking place inside a room where a computer running the program was located.

There are other privacy concerns with Skype that users should be aware of:

- Although the Skype client does not appear to log or record voice conversations, it does have the ability to record IM conversations in a per-user “history” file. Skype enables history recording by default, meaning that all IM conversations are recorded unless users take other action. These files could be retrieved through the use of spyware, other remote-control applications, or by an adversary who gains physical possession of a computer system.

- Because all Skype users are logged into the same “cloud,” any Skype user can usually discover if any other Skype user is logged on at a given instant.

- It appears that Skype attempts to send packets directly over the Internet between participants in a conversation, but if a direct path is not directly possible it appears that Skype will instead send the packets through other computers running Skype. These intermediate computers are called “supernodes.”

It is not known if a supernode can monitor the voice traffic moving through it. Skype's representatives claim that such monitoring is not possible due to the use of encryption. It may be that such monitoring is in fact impossible. It may be that Skype's employees *think* that such monitoring is impossible, but that there is a flaw in their protocol or system design that makes monitoring possible. Many such flaws have been found in other cryptographic protocols after they have been deployed.

- The SkypeIn and Skype Out services may use encryption to the Skype gateways, but at that point the telephone calls are decrypted and sent over the standard public switch telephone network. At this point the calls are subject to both illegal and to court-ordered monitoring.

Finally, it must be remembered that the security of the Skype system also depends entirely on the good will of Skype's programmers and the organization running Skype's back-end servers. It is possible that there are back doors in the system allowing the Skype organization or others to eavesdrop or record Skype conversations. Skype's developers could even put a back-door in the system that could use the program to turn on a computer's microphone and either record the room's noise on the computer's hard drive or send the data over the Internet to another location. Such back-doors and trap-doors could be put in every Skype program or it the feature could be added to the Skype programs on the computers of specific users.

Authenticity

Every Skype user has a username and a password. Each username has a registered email address. In order to log into the Skype system the user must provide their username and password. If the password is lost, Skype will change the user's password and send the new password to the user's registered email address. This approach is called Email Based Identification and Authentication. [2] The Skype client also has the ability to "remember" a username and password and log in automatically.

An added complication with Skype is the Skype network. It appears that the network is used by Skype to perform username/password verification, but it isn't clear how this is done. For example, hosts on the Skype network could relay the encrypted username/password combination back to Skype's servers for approval. Alternatively, they could relay an unencrypted username/password combination. Alternatively, the Skype network may not be involved at all, and the communications between various Skype clients may serve another purpose. However, if the Skype network is involved, several attacks may be possible:

- It may be possible for a malicious Skype client to learn the username/ combination of registered Skype users.
- If a Skype user accesses the Skype network through a malicious Internet Service Provider, it may be possible for the ISP to direct that user's Skype communications to the malicious Skype node. Thus, it may be possible for a malicious ISP to learn any of their user's Skype passwords.
- Alternatively, it may be possible for a malicious node to fake a valid authentication, allowing a client to log in with a particular Skype username even though the password for that username is not known.

Because Skype is a voice communications system, its users can frequently identify a person that they are communicating with by the sound of the other voice. Voice is a biometric. This layer is absent, however, if Skype is used only for text messaging and exchanging files.

Under normal circumstances, it would appear that Skype's authentication system provides similar levels of authentication as other username/password systems --- such as AOL or HotMail. That is, most people have control of their accounts, but sometimes an adversary can learn a target's password by guessing, through social engineering, through the user of keystroke loggers, or by intercepting email used for password recovery. Likewise, administrators of the computer can leak passwords, reset passwords, and otherwise empower attackers to impersonate users. While there is a good chance that the person at the other end of a Skype username is in fact the person who has previously used that username, there is no assurance of this fact.

Availability

One of the great triumphs of 20th Century engineering was the astounding availability of the Public Switched Telephone Network. In many regions customers have come to expect downtimes of five minute per customer per year or less — the equivalent of 99.99905% availability.

Although the original design of the Internet was to allow the network to survive the loss of critical links (see "Survivability" below), availability has only recently become a goal of Internet equipment manufacturers and providers. Internet service is, in general, inferior to telephone service. Thus, it is likely that any Internet telephony service will offer inferior availability to the PSTN. (Some commentators have noted that PSTN availability seems to be decreasing with deregulation, and that availability of a single system is less important given the prevalence of multiple overlapping mobile phone networks.)

Additional factors may compromise Skype's potential availability. Since the Skype client depends on verifying username/passwords, it may be the case that the entire Skype network will cease to function if Skype's authentication servers fail or become otherwise unavailable. Existing VoIP systems do not have this problem, although systems that rely on a single gateway service will experience global failure if the gateway fails. (For example, all Vonage customers will lose their phone service if the Vonage gateway fails.)

Survivability

It is often said that the Internet was designed to withstand an atomic bomb. The truth is that packet switched networks were designed to make it possible for communications between nodes in a network to continue even if the direct connection between those two nodes were destroyed. The ability of a system to continue to operate after it has been degraded is known as *survivability*.

The Internet's design allows Internet providers to choose how survivable they wish to make their networks. If an organization connects its mail server to the Internet with a single DSL line and that DSL line fails, email service will not survive. On the other hand, if an organization procures two DSL lines, email service can survive any single DSL line's interruption. Survivable systems are generally more expensive than systems with a single point of failure. What's more, systems that are survivable rarely provide better day-to-day performance than systems that are not. As a result, most Internet users and many Internet service providers have not deployed systems that can withstand the arbitrary failure of one or more components.

It is not known if Skype's authentication servers can survive network disruptions or attacks.

Resilience

Packet switch networks are extraordinarily resilient. In many cases Internet connections can be restored more quickly than traditional telephone networks through the use of wireless networking products. An added benefit of Skype and other VoIP-based systems is that these systems were designed with mobile users in mind: They are highly tolerant of a user's IP address changing from day-to-day.

As a result, Skype and other VoIP-based systems are generally very resilient to local network disruption. If a building's network connection fails, just take your computer or VoIP telephone to another location and plug it in. As long as your computer can register with the Skype network, you will be able to receive calls at your new location.

On the other hand, Skype clients almost certainly could not operate if Skype's backend authentication network were to become unavailable. This could happen as the result of network destruction, some kind of hacker attack, a hostile insider, or even the failure of the parent corporation. In such a case the Skype network could become unavailable to some or all Skype users.

Integrity (Conversation)

Skype's integrity provisions are completely unknown. It's possible for speech spoken over the Skype system to be dropped or garbled before reaching the other end. Likewise, Skype makes no guarantees that Instant Messages or files will be delivered as they were transmitted.

In practice, however, Skype seems to do a good job faithfully transmitting voice, and messages and files appear to be delivered without corruption. One exception to this rule appears to be when Skype is used over an 802.11 wireless network. In this case, voice quality suffers considerably.

Integrity (System)

Network administrators are understandably concerned when users download and run software that might have wide-ranging implications. Many universities, for example, have complained that students running the KaZaA peer-to-peer file transfer system both consumer large amounts of bandwidth and potentially open up the school to lawsuits from aggrieved copyright holders. KaZaA users may also share the contents of their computers without their own knowledge. [3]

Because Skype conversations are limited to voice, the total load that a Skype "supernode" could put on a network would be equal to twice the number of conversations that a supernode would proxy at any given time times the bandwidth required for a single voice conversation. It's not known how high this limit is.

Skype could also be an infection vector for spyware. Although the program's creators promise that their program does not come with spyware or adware, it is possible that they are not being truthful or that their policy will change in the future. Skype could have security vulnerabilities that a third-party could exploit.

It should be noted that many of the risks posed by Skype are no different than the risks posed by email and other person-to-person communications medium. Indeed, Skype probably poses fewer risks to overall system integrity simply because the primary use of Skype is for voice communications. Care must be taken, however, when Skype is used to exchange files. Compared with KaZaA and other file trading programs, Skype poses less risk because the exchange is always with specific individuals, rather than files that are located through searching and downloaded from potentially anonymous sources. On the other hand, Skype poses more risk because programs like KaZaA have built-in anti-virus protection that scans programs as they are downloaded; Skype appears to have no such protection.

Recommendations

Overall, Skype appears to offer significantly more security than conventional analog or ISDN voice communications, but less security than VoIP systems running over virtual private networks (VPNs). It is likely that the Skype system could be compromised by an exceedingly capable engineer with experience in reverse engineering, or by a suitably-motivated insider.

When using Skype, the following recommendations may be helpful:

1. Make sure that any computer used for Skype is free of all spyware, adware, remote-control programs, worms, and computer viruses. All PCs running the Windows operating system should be equipped with up-to-date anti-virus and anti-spyware programs.

    a. A free anti-virus program is available from http://www.grisoft.com/
    b. A free anti-spyware program is available from http://www.lavasoftusa.com/
    c. Although there is probably little risk at using Skype to communicate with KaZaA 3.0 users, KaZaA 3.0 should not be used as a substitute for Skype given the potential liability

created by the exchange of copyrighted files without the permission fo the copyright holder.

2. The username/password combination used for Skype shouldn't be used for anything else.

3. The username used for Skype shouldn't be readily identifiable. It should have no relationship to the user's name, organization or occupation.

4. Both Skype usernames and passwords should be changed on a regular basis if the Skype network is used for any kind of sensitive discussions. Changing usernames makes it harder for an adversary to track the actions of the user. Changing passwords reduces the window during which a compromised password will be useful.

5. Skype users should assume the Skype system could become permanently unavailable at any moment. As a result, they should always have alternative techniques for contacting each other.

6. Do not assume that the person behind a Skype username today is the same person that it was yesterday. Somebody could be sitting down at your associates computer and using Skype without their permission, or their account may have been hijacked. Always independently verify the identiy of a person that you are communicating with if sensitive material is going to be exchanged.

7. Although Skype insists that it's voice system cannot transfer a virus, there is no evidence of this claim. In particular, a buffer-overflow in the voice decoder would enable another Skype user to execute commands on any system that the user was in contact with. Furthermore, Skype can be used to transfer files; these files can contain viruses or spyware.

8. Remember, just because Skype is apparently encrypted, the conversation is decrypted at the other end. There is no way to assure that the person you are communicating with is not, themselves, recording the conversation in which you are engaging. Using encrypted communications is no substitute for being careful about what you say.

References

[1] Charny, Ben, "Why VoIP is music to Kazaa's ear," September 11, 2003. http://news.com.com/Why+VoIP+is+music+to+Kazaa's+ear/2008-1082_3-5074558.html

[2] Garfinkel, Simson. "Email-Based Identification and Authentication: An Alternative to PKI?," IEEE Security and Privacy, November/December 2003.

[3] Good, Nathaniel S., Krekelberg, Aaron, Usability and privacy: a study of Kazaa P2P file-sharing. HP Labs: Tech Report: HPL-2002-163.

[4] James, Kat. "Re: Press query from Website: need press contact." October 17, 2004. Personal communication.

[5] Joltid, "Joltid / Company," Accessed October 26, 2004. http://www.joltid.com/index.php/company/

[6] Protocols.com, "Voice Over IP," http://www.protocols.com/pbook/VoIPFamily.htm

About the Author

Simson L. Garfinkel is a researcher in the field of computer security and award-winning commentator on information technology. Currently a doctorial candidate at MIT's Computer Science and Artificial Intelligence Laboratory, Garfinkel's research interests include computer security, the usability of secure systems, and information policy. He writes monthly columns Technology Review's Magazine and website and for CSO Magazine, for which he was awarded the 2004 Jesse H. Neal National Business Journalism Award for Best Regularly Featured Department or Column.