now ELECTRONIC!

Virtual Inc.

Volume 1 • Number 11 • February 1995

A NEWSLETTER FOR THE ONLINE BUSINESS COMMUNITY

How Encryption Can Protect Your E-mail Privacy

BY ARI M. WEINSTEIN

The need to communicate privately and securely is universal. We don't want others prying into our personal or business affairs, and possibly using the information they find against us. In the paper age, we relied on sealed envelopes, registered mail, and couriers to keep our messages private. In the information age, computers have made it easier than ever to intercept and read information intended for others. The best way to keep our electronic messages secure from such interception is to use encryption software.

Encryption is the process of taking information and rearranging it so that it cannot be readily interpreted. Simple codes that substitute one letter of the alphabet for another are a very basic form of encryption. Computers excel at rearranging information, and today's encryption software can perform very sophisticated operations that will render information extremely secure. The code produced by such software is very hard to crack, even with the help of another computer. A password or *key* is needed to decrypt the information.

Standard Encryption

Traditional encryption works this way: Information is encrypted and protected with a password key. The intended recipient is given the password, and can access the coded information by using the same software.

There is a problem with traditional encryption. How do you give your password to somebody who may be hundreds of miles away and with whom you are communicating electronically? Sending the password via e-mail defeats the purpose of using encryption in the first place. The same people from whom you are trying to conceal information can intercept your e-mail and obtain the password you are using to protect it. But how, you may wonder, can e-mail be intercepted?

At Work

E-mail Security

When you send e-mail to someone, via the Internet, a commercial online service, or even at the office, you are not communicating with them directly. Most e-mail systems use a *server* to store your message briefly before sending it on to the recipient. In the case of the Internet or an online service, there are *many* servers and host computers through which your mail is passed before reaching the recipient. The role of the servers is like that of a traffic cop: They regulate the ebb and flow of messages through the network, and relay messages from one point to another so that messages don't collide or get lost. The servers also see to it that your message is addressed correctly and can return your e-mail to you if it cannot be delivered.

Anyone with access to the servers and host computers can potentially intercept your e-mail. Sophisticated hackers can even gain access to the e-mail servers remotely, from their own homes.

Traditional encryption is therefore weak when used for electronic communication. Passwords cannot necessarily be exchanged securely. The telephone or a fax may offer a possible solution, but e-mail pen pals and contacts may be reluctant to exchange phone numbers until they hear more about you or your business. If you want to send that additional information securely, you have a problem.

continued on page 3

Virtual Inc. Is Now Electronic

BY *VIRTUAL INC.* STAFF WRITERS

Virtual Inc. has completely abandoned paper publishing as of this issue. The monthly newsletter, which has served the online business community since April 1994, is now published in Portable Document Format using Acrobat software from Adobe Systems Inc. PDF files can be viewed with Acrobat Reader 2.0, which is available for free from many online sources, in versions for Macintosh, Windows, and UNIX computers.

News

"Our audience is all online. Printing and mailing a paper newsletter just didn't make sense," said *Virtual Inc.'s* publisher, Michael Daconta. "The advantages of the electronic publication are too numerous to mention," he added. "Among them are full color, variable length,

continued on page 2

Inside:

Problems of a Virtual Man

Editor's Word

BY MICHAEL DACONTA

It is now 6 am on a Tuesday morning, and I am waiting to board a flight home from Washington National Airport in our capital, Washington DC. Being away from home always stresses the system. Each day away from my wife and family is a little more difficult. Things tend to annoy you more easily. So in that frame of mind, I present you with my list of top ten problems facing those of us who are "virtual trailblazers."

10. Hotel Rooms never accommodate laptops. Is it too much to ask to have two electrical outlets and a phone jack within 10 feet of each other? Every time I stay at a hotel, I have my modem strung up to one wall and the cords stretched across the room to my computer plugged in on the other side of the room. It always ends up like an obstacle course!

Will our virtual world ever have soft edges?

9. Too many electronic-mail boxes. I am wired to three online services (one with three account names to check) and two internet accounts. It has become impossible for me to check all of these on a nightly basis. Not to mention the requirement to be present when switching between services. Just getting mail has become a major event each night. (I expect an announcer to give the public a play-by-play commentary.)

8. Too much information to handle. We are definitely neck deep in content overload. The clutter and confusion factor has set in. Related to this problem is are the current horrible search methods. If I am asked to enter another boolean query, I may be sick.

7. No interoperability between service providers. How come CompuServe, Internet and America Online users cannot all participate in a single electronic group meeting? If the different online services cannot manage this amongst themselves, how about – at least – the online services and folks on the Internet? Will vendors ever begin to take interoperability seriously?

6. Toll roads on the info highway. The information highway charges you just as your telephone company does – not one big price, but lots of little ones. The vendors figure if they can nickel and dime you to death, maybe you won't notice being squeezed. CompuServe charges you every time you turn around. AOL is much simpler and straightforward. An Internet provider charges you a lot of small fees at startup time – like a connect fee – fees for extra services (like PPP or SLIP), and extra fees for other services like an IP address.

5. Point-and click is past its prime. The mouse interface has been a big success, but it is no longer efficient enough. In fact, most of the time I try to avoid it, because it takes my hands off of the keyboard. We need richer interfaces that will allow us to take advantage of multitasking. If you get the chance to look at a UNIX workstation with the FVWM (virtual window manager) environment, you will get an idea of what I am talking about. FVWM allows you to switch easily between multiple desktops. It is a great metaphor which reduces the cramping of a single desktop. If we can combine this new visual metaphor with a new interface like good voice recognition, we could increase productivity.

4. Buggy applications. The CompuServe navigator crashes and America Online kicks you off. There may not be any solution to this problem, except maybe a Vulcan mind meld to instill quality world wide.

3. Relying on my laptop too much. This laptop has become my sole connection to cyberspace when I am away from home. What a huge responsibility for such a light-weight appliance. A classic rule of military operations is always to have redundant communications. Oops! I don't have any. Is it worth the price of a PDA or palmtop just to be safe? Or even better, how about the rental car companies offering rental laptops!

2. Not enough time and too many virtual contacts. If my virtual mailboxes were like my tiny little home mailbox, the postperson would never be able to stuff it with all the mail I get. Maybe physical limitations are a good thing? Anyway, in cyberspace, there are no such limitations, and we have to cope with mountains of mail in our ever-expanding virtual web of relationships. The only current solution is to answer with brevity, but that short-changes the sender of the mail. Auto-filtering may make us more efficient in knowing which mail is the most important.

1. Away from home, the virtual world seems cold. When you are away from home, you only have a virtual world with which to interact. Flickering screens, a keyboard, and mouse leave much to be desired when you long for the warmth of a loved one. An animated screen cannot replace the hug of a small child. Will our vir-

continued on page 4

Virtual Inc. Is Now Electronic

continued

hypertext links, and searching capabilities."

Subscribers will be sent the Adobe Acrobat Reader software upon request. Refunds are being offered to subscribers who do not wish to switch to an electronic publication. At press time, however, no refund requests had been received.

"We have been working on the electronic version alongside the printed version for several months now," continued Daconta. "Readers who have received the electronic version were all impressed. They were seeing *Virtual Inc.* in color, they were able to zoom in and out for easy viewing, and they were even able to print copies identical to the paper version in every respect. We deemed the experiment a success, and abandoned traditional printing this month," he said.

Others on the Virtual Inc. staff were equally enthusiastic about the electronic newsletter. "We are no longer dependent on a third party for the final product," said Ari Weinstein, *Virtual Inc.'s* art director. "We can cut our production time by about a week, and deliver the newsletter earlier each month."

Readers who want a free sample of *Virtual Inc.* should contact vfusion@aol.com. All back issues of the newsletter are also available in Portable Document Format, and current issues are being distributed for free on the major online services for a limited time. ■

AOL to Browse Internet, Web

Originally reported by InfoWorld

America Online is encouraging software developers to ship their applications with an AOL Internet browser before the Microsoft Network connects to millions of desktops late next year.

In March, AOL will offer a standalone Internet browser that links directly to the company's home page on the World Wide Web. Soon after, the Internet browser will be integrated with the existing America Online network client.

AOL will announce in February their Internet service aimed at commercial information providers. It will offer a Web server that includes an object relational database, WAN transaction processing, firewall security, and data packet security over IP connections.

"Our system will interface to accounting systems, and our SQL-based server will include tracking, reporting, access control, logging, navigation, and connections to other WANs through our domain name server," said David Cole, Director of the America Online Internet Services Company.

By the end of 1995, AOL plans to offer complete network services to run on its high-speed network. ■

Encryption Can Protect Your E-mail Privacy *continued*

Public-Key Encryption

The solution for this problem is another form of encryption known as *public-key encryption.* In this type of encryption, two password keys are used. The keys are unique bits of code that complement each other and act in tandem: One key is entered to encrypt the data, and the other is entered to decrypt. Users who want to send data to each other each generate a pair of keys, and send one of the keys, known as a *public* key, to each other. The other key remains with the user who generated it, and is known as a *private* or *secret* key. The sender then encrypts a message with the recipient's public key. Once that is done, the message is sent, and only the recipient's private key can be used to decrypt it.

Since the keys can be used in tandem, public-key encryption can serve another security purpose: document authentication. If a user encrypts a message with his/her secret key, only the corresponding public key can be used to decrypt the message – proving it came from the sender. To achieve both security and authentication, a document can first be encrypted with the recipient's public key, and the resulting code then encrypted again with the sender's private key. The portion encrypted with the private key is attached to the message itself, acting as a digital *signature.* The signature is decrypted first using the sender's public key – proving the message's origin and authenticity. Once that is done, the recipient can decrypt the message itself with their private key.

The concept of public-key encryption is a bit tricky. However, since users each have their own pair of keys, it's easy to understand why this form of encryption is so secure.

This form of security does have an inconvenience factor, however. In order to send private e-mail to multiple recipients, you must obtain each of their public keys, and encrypt the message once for *each* recipient. Each recipient in turn, must have *your* public key to send you messages and verify your digital signature. How would you keep track of so many key codes, and how would you automate the process of encryption?

Pretty Good Privacy

Encryption, decryption, key management, and more can all be handled by a program called *PGP,* which stands for Pretty Good Privacy. PGP is available for PCs using DOS or Windows, Macintoshes, UNIX systems, and other types of computers. Released in 1991 by it's author, Philip Zimmermann, PGP and it's documentation are available for free on the Internet and from many bulletin boards and online services. PGP performs all of the operations outlined thus far: key generation, encryption and decryption, key management, and digital signing. PGP can encrypt any file – not just text messages – and it compresses, segments, and converts the data into pieces that can be safely handled by any e-mail system.

Several technologies are incorporated into PGP. Each is in the form of algorithms that manipulate data in different ways. In each case, the very best algorithms are used, so that files, messages, and keys processed by PGP are extremely secure.

Encryption for Everyone

PGP has been widely adopted by the online community as a de facto standard for data security. There are several reasons for its popularity: It's free; it's cross-platform, it's security algorithms have been very thoroughly tested, and Phil Zimmermann has done a remarkable job of providing all the necessary features for secure communication. Unfortunately, Phil has also attracted the unfriendly attention of the federal government. Encryption as secure at PGP's is viewed by some as a threat, because criminals could potentially use it for illegal activities with little chance of being detected. Until very recently, the government wanted to regulate the use of data encryption in a way that would have made it possible for federal law-enforcement agencies to obtain the keys to any message.

But while this debate continues, many companies are proceeding with plans to offer their services on the Internet, and they're relying on encryption to protect the privacy of their customers' transactions and credit card numbers. We all need to protect our electronic communications from prying eyes, so encryption – in various forms – is undoubtedly here to stay. ■

Pretty Good Reading about Pretty Good Privacy

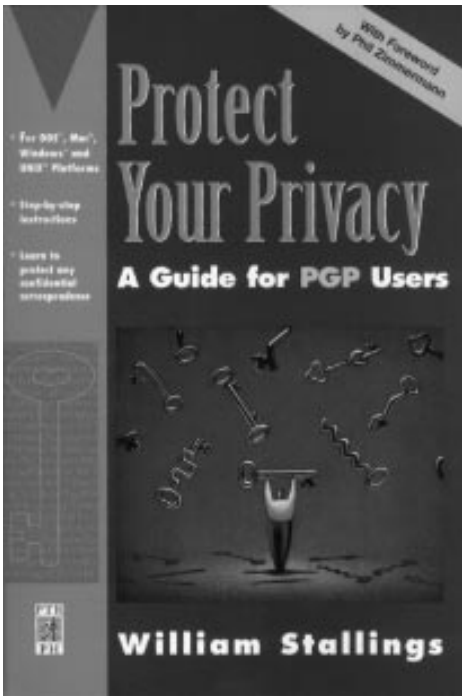
Protect Your Privacy: The PGP User's Guide *by William Stallings, (Prentice Hall PTR, NJ, 1995, 302 pages.)*

William Stallings has written an excellent guide to PGP which will serve beginners and advanced users equally well. Phil Zimmermann, the creator of Pretty Good Privacy, states in the forward that he will probably use Stalling's book himself as his preferred reference. This hearty endorsement is hardly surprising though, considering how thoroughly the practice and theory behind Pretty Good Privacy are covered in this book.

Stallings starts with 114 pages of detailed information about PGP: how it works, the concepts behind public-key encryption, and every single security feature that is incorporated into PGP. Since keys and their validity are of primary importance for the safe exchange of information with PGP, Stallings devotes two chapters to them. Ample diagrams and clear narrative help the reader understand the rather sticky subjects of public-key encryption and key management. The material is peppered with interesting factoids about encryption. I did not know, for example, that although encryption has been around since ancient times, public-key encryption was

continued on page 4

Good PGP Reading *continued*



introduced only about 20 years ago. Yet without it, secure exchange of data on the information highway would be highly inconvenient and fraught with obstacles.

Part 2 of the book discusses the various implementations of Pretty Good Privacy and their use on different platforms. There are separate chapters for DOS/UNIX, Macintosh, and Windows versions of PGP. Part 3 contains supplemental information, including a very good chapter on how to choose a secure password. That information would probably have been better placed before the user guides in Part 2 – it's a must-read.

I concentrated my reading of Part 2 on the user guide and reference chapters for Mac PGP, and found them very thorough. After completing the tutorial exercise Stallings provides, I was able to exchange secure data with a friend who read the DOS and Windows chapters. The reference chapters, one each for DOS/UNIX and Macintosh, cover every command found in PGP. There are only shell programs for Pretty Good Privacy on Windows – but they offer good graphical control of the underlying DOS application, and are well explained in Chapter 11 of the book.

Not liking math, I hesitated to read Chapter 12, The Building Blocks of PGP. But here too, I found the information fairly clear and interesting. Stallings does not get too academic, and instead recommends his book *Network and Internetwork Security* for in-depth understanding of security algorithms. The final two chapters of the book tell where to obtain PGP, and how to use a public-key server to obtain and store public keys. The former was written by a gentleman named Paul Michael Johnson, and is reprinted by Stallings with his permission. (Johnson maintains a list of PGP sources which is updated periodically.)

Overall, *Protect Your Privacy: The PGP User's Guide* recommends itself nicely to any reader who wants to learn the use of PGP without having to scroll through screen after screen of online documentation. And it provides excellent reading even when the computer is turned off. ■

Virtual Problems *continued*

tual world ever have soft edges? It needs them.

You may be saying to yourself, "I don't want to hear Mike's griping." But that's the wrong attitude. You need to retrain yourself to understand a key point of business success. Problems are money! If you want to make money, solve some problems. I've just given you my top ten to get started on. See any opportunities yet? ■

Virtual Inc.

A Newsletter for the Online Business Community

Editor In Chief
Michael C. Daconta

Managing Editor/
Art Director
Ari M. Weinstein

Associate Editors
Jeffrey Cohen
Marc I. Whinston

Contributing Editor
Jon X. Volquardsen

5160 Calle Bonita, Sierra Vista, AZ 85635
vfusion@aol.com
Phone: 800-269-8825
Fax: 602-458-1063

Virtual Inc. is published 12 times a year. Annual subscription rate: $30. Use any of the addresses or numbers above to request subscriptions. Letters to the Editor are accepted via electronic mail only. Letters submitted become property of *Virtual Inc.*, and cannot be returned.

Virtual Fusion™ Inc. is seeking programmers, artists, and engineers who want to work from home developing software for commercial distribution. E-mail vfusion@aol.com for further details.

Virtual Inc.

5160 Calle Bonita, Sierra Vista, Arizona 85635

Virtual Inc.

Published by Virtual Fusion Inc.
5160 Calle Bonita
Sierra Vista, AZ 85635
Phone: 1-800-269-8825
Fax: 602-458-1063
E-mail: vfusion@aol.com

✓ Yes! I'd love to subscribe. Here's the info you'll need:

Name .....

Address .....

City ..... State ..... Zip .....

Phone ..... E-mail Address .....

Computer type and configuration .....

✔ Please start my subscription to Virtual Inc. at the rate of $30.00 per year (12 issues). I have an e-mail account and Adobe Acrobat™ Reader 2.0.* I would like to subscribe for ..... years. Total enclosed .....

Please send your check or money order to Virtual Fusion Inc.
5160 Calle Bonita
Sierra Vista, AZ 85635

Payable to Virtual Fusion

Only $30 per year

12/94

* E-mail and the Acrobat™ Reader are needed to receive and read Virtual Inc. Acrobat is a registered trademark of Adobe Systems Incorporated