# FORUM ON RISKS

RISKS-LIST: RISKS-FORUM Digest Monday 1 July 1991 Volume 12 : Issue 01
FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

***Contents:***



The RISKS Forum is moderated. Contributions should be relevant, sound, in good taste, objective, coherent, concise, and nonrepetitious. Diversity is welcome. CONTRIBUTIONS to RISKS@CSL.SRI.COM, with relevant, substantive

## *The Risks of Undelete and the Law (Ron Dippold)*

"Subject:" line. Others ignored! REQUESTS to RISKS-Request@CSL.SRI.COM. For
vol i issue j, type "FTP CRVAX.SRI.COM<CR>login anonymous<CR>AnyNonNullPW<CR>
CD RISKS:<CR>GET RISKS-i.j<CR>" (where i=1 to 12, j always TWO digits). Vol i
summaries in j=00; "dir risks-*.*<CR>" gives directory; "bye<CR>" logs out.
The COLON in "CD RISKS:" is essential. "CRVAX.SRI.COM" = "128.18.10.1".
<CR>=CarriageReturn; FTPs may differ; UNIX prompts for username, password.
ALL CONTRIBUTIONS CONSIDERED AS PERSONAL COMMENTS; USUAL DISCLAIMERS APPLY.
Relevant contributions may appear in the RISKS section of regular issues of ACM SIGSOFT's SOFTWARE ENGINEERING NOTES, unless you state otherwise.
Date: Thu, 20 Jun 91 06:24:27 GMT
>From: rdippold@cancun.qualcomm.com (Ron Dippold)
Subject: The Risks of Undelete and the Law

Here's one about a class A dummy... You'd think he'd be a bit more careful on something like this.
Probably the most dramatic instance of recovery of "deleted" file information appears in a recent ruling of the Pennsylvania Supreme Court, Com. v.Copenhefer, 587 A.2d 1353. The defendant's death sentence was affirmed on "overwhelming" circumstantial evidence, including "incredibly comprehensive" evidence seized from the defendant's home pursuant to search warrants.
The computer evidence consisted of drafts of texts of phone calls, ransom and hidden notes, and a 22 point plan for the kidnapping scheme, which eventuated in murder of a bank manager's wife. (The defendant was a bookstore owner who had "unproductive transactions" with the bank).
The defendant argued that the computer evidence should have been suppressed because he had deleted the files, thereby creating an "expectation of privacy" under _Katz_ and its progeny. The court's opinion contains a readable explanation of how the deletion only affected the directory, and "subsequent usage never displaced the files in question and they remained in the memory of his computer."
The court soundly, and IMO correctly, rejected this claim, analogizing the retrieval of the deleted file data (by an FBI agent who was a computer expert)to deciphering a coded message in a diary, after the diary was obtained under a valid subpoena.
Somehow, I don't think Mr. Copenhefer will be doing any endorsements for PCTools or another defragmenter; "if only I had used Compress with the Clear option, I wouldn't be on death row now." Among other things, the old-fashioned physical evidence was quite overwhelming. But the case is a striking example of the law adjusting to

computer technology.
Sort of unbelievable, especially the part about an FBI computer expert (maybe they borrowed someone from the NSA?), but true! So remember, Norton WIPEDISK is your friend.
Ron Dippold

### *Patriot missile specifications (Robert I. Eachus)*

Date: Wed, 19 Jun 91 12:29:39 EDT
>From: eachus@d74sun.mitre.org (Robert I. Eachus)
Subject: Patriot missile specifications

There has been some tendancy here to treat the Patriot system "failure" to intercept the El Hussein missile in Dharan as a poor system specification or as badly designed software. This is totally wrong. If someone had gone to the Army before the Gulf War and asked, "In this hypothetical situation...how should the system respond?" The answer would have been to do as it did.
The "problems" in the software were bugs only AFTER it was known IN PRACTICE that 1) there were missiles in that speed range that could and should be attacked, 2) the Patriot systems' primary mission would NOT be defending against hostile aircraft, and 3) that "highly motivated" and experienced crews could successfully engage such missiles in "manual" mode using information from other sites. Given those circumstances updating the software and getting it to the field in a matter of days was a heroic effort, even if it arrived one day too late.
The real risk here is in assuming that the "fog of war" is a myth. You don't know how systems will be used in practice until you have actual combat experience. I have seen many "field mods" to hardware incorporated into later production models because the feature was needed to use the system to best effect in combat. This is NOT a failure of design or specification or production, it is often the result of someone trying something because he is dead anyway if it doesn't work. Such successful tactics quickly become the normal way the weapon is used.
A simple example is dive brakes, which were initially installed on P-38s after many crashed from incompressability problems. In combat, the only advantage that the P-38 had in some situations over its opponent was the ability to dive faster, so pilots took it to the limit and beyond. The dive brake was invented to "fix" a problem which only occurred when a pilot stayed in a steep dive at full power too long. (Actually, there was a "known fix" by the time the brakes were available—fly an outside loop!) If dive brakes had existed when the plane was designed the designers would have been told to leave them off. No reason to add weigth to the plane, and no sane pilot would do something like that anyway... Of course, after experence in combat, pilots would carry as much weight as possible, and try to use it to save their lives.

### *Lawsuit Pending over Patriot's Failure to Stop Dharan Scud (Sean Smith)*

Date: Wed, 19 Jun 91 12:26:33 EDT
>From: Sean.Smith@THEORY.CS.CMU.EDU
Subject: Lawsuit Pending over Patriot's Failure to Stop Dharan Scud

About half the US soldiers killed in the Dharan Scud attack belonged to a unit stationed outside of Pittsburgh. Recently, the local news has been reporting that a Pittsburgh area law firm is recruiting the families of the deceased to participate in a class action lawsuit against Raytheon, manufacturers of the
Patriot missile defense system. Considering that the system was being operated out of spec, to solve a different difficult problem (defense of a city) than the one it was designed for (point defense), this incident suggests that writing software may be RISKier than we thought...

### *Word Perfect file locking poor protection (John Gilmore and Helen Bergen via Peter Jones)*

Date: Tue, 25 Jun 91 19:52:19 EDT
>From: Peter Jones <MAINT%UQAM@pucc.PRINCETON.EDU>

Subject: Word Perfect file locking poor protection

A file on the SIMTEL20 archives, PD:<MSDOS.INFO>UNCRYPT.ZIP, gives information on how to break files that a WP user has "locked" with a password, in WP lingo. Here are some excerpts pertinent to RISKS.
>From: gnu@hoptoad.uucp (John Gilmore)
Newsgroups: comp.os.msdos.apps,sci.crypt
Subject: Word Perfect "locked document encryption" is trivial to break
Date: 27 Aug 90 22:58:27 GMT
Organization: Cygnus Support, Palo Alto

One thing that came up at Crypto '90 was a short paper from Ms. Helen Bergen at Queensland U. in Australia. She noticed the 'locked document' commands in WordPerfect, used by all the secretaries in her dept., and looked to see how strong it was. It turned out that the MSDOS DEBUG command and an envelope for scratch paper are enough for anyone to decode both a document AND the key used for it! Word Perfect Corp. didn't care about her results (letter reproduced below), but I thought that some Word Perfect losers, I mean users, here on the net might want to know.
You should consider WP locked documents like ROT13: fine to keep the text garbled until you type a command, useless for keeping things private.
John Gilmore
>From: <CSZBERGEN@qut.edu.au>
Date: Mon, 27 Aug 90 10:28 +1000
To: cygint!gnu

Dear John,
Here is the letter and a copy of the Latex source of my paper. It will be published in CRYPTOLOGIA in the near future. Thanks for your interest,
Regards,
Helen Bergen

**********

Quote from letter received from WordPerfect Pacific:
Thankyou for the copy of your paper entitled "File Security in WordPerfect 5.0". I sent a copy of the paper to WordPerfect Corporation in the USA and recently received a reply from them.
They confirmed that people have written programs to break the password. However, WordPerfect Corporation does not have such a program and therefore has no way of breaking it. They also pointed out that very few users would know how to write such a program.
It is possible that the manual may be amended in a future edition to clarify the protection that a password gives. They recommend that anyone concerned about security may want to take higher precautions than the password protection.
Thank you for your interest in WordPerfect.

**********

FILE SECURITY IN WORDPERFECT 5.0

H.A. Bergen School of Computing Science
W.J. Caelli Information Security Research Centre

Faculty of Information Technology
Queensland University of Technology
G.P.O. Box 2434, Brisbane, Q 4001, AUSTRALIA

ABSTRACT: Cryptanalysis of files encrypted with the 'locked document'option of the word processing package WordPerfect V5.0, is shown to be remarkably simple. The encryption key and the plaintext are easily recovered in a ciphertext only attack. File security is thus compromised and is not in accord with the claim by the manufacturer that: "If you forget the password, there is absolutely no way to retrieve the document".
KEYWORDS: Cryptanalysis, WordPerfect.

INTRODUCTION

WordPerfect is one of the most popular word processing packages in use today. It has a ‘locked document’ option which aims at protection of a WordPerfect file from unauthorised access. The manual states “You can protect or lock your documents with a password so that no one will be able to retrieve or print the file without knowing the password - not even you”. The manual also claims that “If you forget the password, there is absolutely no way to retrieve the document” [1].

[detailed explanation omitted]

In the 4.2 version, the only text encrypted was that contained in the actual document. This is unknown plaintext. In version 5.0, however, the printer information as well as the document text is encrypted. We have identified bytes 16 - 21, 24 - 27, 29 - 41, 43 - 45 as being constant for a particular system (as defined earlier, a particular licenced copy of WordPerfect on a particular PC and printer), and they do not change markedly from one system to another. So we have the ideal situation of known plaintext for a reasonable number of bytes. This can greatly simplify our attack as it makes it possible to recover the actual key. Then it is trivial to recover the plaintext by using WordPerfect to retrieve the file using the recovered key as the ‘’password’’. Alternatively, a program could be written to do this as the

encryption/decryption algorithm is known. We outline a strategy with the following example from one particular system:

[detailed explanation of finding the key omitted]

Retrieve the plaintext using WordPerfect with the key as the password. This is the easiest way to decrypt the document text. If no access to WordPerfect is available, then it is straightforward to recover the plaintext with a short C program which implements the decryption algorithm as described previously. This has been done successfully.

CONCLUSION

The encryption key is easily recovered in an apparent KNOWN CIPHERTEXT ONLY attack, as the system provides enough known plaintext in the printer information regardless of the document plaintext. The analysis, as shown, can literally be done on the back of a (large) envelope.

The analysis may be slightly more difficult where the physical system on which the files were prepared is completely unknown and vastly different to any system we have encountered, as this may reduce the amount of known plaintext. In these situations, statistical analysis based on the characteristic frequencies of characters in a language is used to decipher text files. This

is a standard method which is straightforward although a program may have to be written.

In summary, the cryptanalysis of files encrypted with the ‘locked document’ option in WordPerfect version 5.0 is remarkably simple. The inclusion of portions of known plaintext in the encrypted file is a fatal flaw in the system, since it provides a mechanism of attack in which the key can be recovered by hand, and document plaintext easily retrieved. All of the key can easily be recovered for keylengths of 1-13 and 15-17, far in excess of commonly used passwords of 8 characters. A high proportion of the key can be deduced for keylengths of 14 and 18-24. The cipher used is too weak, providing little or no protection.

If the attacker has knowledge of any other unencrypted file from the same system, the analysis is made even more simple. We stress that **both the key and the plaintext can be recovered**, independent of the content of the plaintext.

The worst problem is that it may give a false sense of security. For example, an attacker may decrypt a document, modify it and re-encrypt so that the originator is unaware of the alterations. We conclude that the file security is not consistent with claims made by the manufacturer and is not sufficent to protect sensitive documents from anything but the most naive attack.

References

1. WORDPERFECT CORPORATION (1989): WordPerfect for IBM Personal Computers.\\
2. BENNETT, J (1987): Analysis of the encryption algorithm used in the WordPerfect Word Processing Program,
Cryptologia, Vol XI. No 4. pp 206-210.\\
3. KONHEIM, A G (1981): {\em Cryptography, A Primer}, Wiley.\\
4. DENNING, D E (1981): {\em Cryptography and Data Security}, Addison Wesley.\\
5. CARROLL, J and Robbins, L E (1989): Computer Cryptanalysis of Product Ciphers, Cryptologia, Vol XIII. No 4. pp 303-326.\\

Biographical
Helen Bergen is a Lecturer in the School of Computing Science, Faculty of Information Technology, at the Queensland University of Technology. Her research interests within the Information Security Research Centre, Faculty of Information Technology, include cryptology and the application of supercomputers.
Bill Caelli is Director of the Information Security Research Centre within the Faculty of Information Technology at the Queensland University of Technology. He is also Technical Director and Founder of ERACOM Pty. Ltd., a manufacturer of cryptographic equipment. His research interests lie in the development and application of cryptographic systems to enhance security, control and management of computer and data network systems.—John Gilmore {sun,pacbell,uunet,pyramid}!hoptoad!gnu gnu@toad.com
The Gutenberg Bible is printed on hemp (marijuana) paper. So was the July 2,1776 draft of the Declaration of Independence. Why can't we grow it now?

Peter Jones (514)-987-3542
Internet:Peter Jones <MAINT%UQAM.bitnet@ugw.utcs.utoronto.ca>
UUCP: ...psuvax1!uqam.bitnet!maint

### *Statement in Support of Communications Privacy (John Gilmore)*

Date: Tue, 18 Jun 91 22:27:11 -0700
>From: gnu@toad.com
Subject: Statement in Support of Communications Privacy

The Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and RSA Data Security Inc. cosponsored a meeting of cryptographers, civil libertarians, business leaders, and people from all over the government who handle cryptography and privacy issues. The following statement was released at the meeting.
STATEMENT IN SUPPORT OF COMMUNICATIONS PRIVACY
Washington, DC
June 10, 1991

As representatives of leading computer and telecommunications companies, as members of national privacy and civil liberties organizations, as academics and researchers across the country, as computer users, as corporate users of computer networks, and as individuals interested in the protection of privacy and the promotion of liberty, we have joined together for the purpose of recommending that the United States government undertake a new approach to support communications privacy and to promote the availability of privacy-enhancing technologies. We believe that our effort will strengthen economic competitiveness, encourage technological innovation, and ensure that communications privacy will be carried forward into the next decade.
In the past several months we have become aware that the federal government has failed to take advantage of opportunities to promote communications privacy. In some areas, it has considered proposals that would actually be a step backward. The area of cryptography is a prime example.
Cryptography is the process of translating a communication into a code so that it can be understood only by the person who prepares the message and the person who is intended to receive the message. In the communications world, it is the technological equivalent of the seal on an envelope. In the security world, it is like a lock on a door. Cryptography also helps to ensure the authenticity of messages and promotes new forms of business in electronic environments. Cryptography makes possible the secure exchange of information through complex computer networks, and helps to prevent fraud and industrial espionage.
For many years, the United States has sought to restrict the use of encryption technology, expressing concern that such restrictions were necessary for national security purposes. For the most part, computer systems were used by large organizations and military contractors. Computer policy was largely determined by the Department of Defense. Companies that tried to develop new encryption products confronted export control licensing, funding restrictions, and classification review. Little attention was paid to the importance of communications privacy for the general public.
It is clear that our national needs are changing. Computers are ubiquitous. We also rely on communication

networks to exchange messages daily. The national telephone system is in fact a large computer network.

We have opportunities to reconsider and redirect our current policy on cryptography. Regrettably, our government has failed to move thus far in a direction that would make the benefits of cryptography available to a wider public. In late May, representatives of the State Department met in Europe with the leaders of the Committee for Multilateral Export Controls ("COCOM"). At the urging of the National Security Agency, our delegates blocked efforts to relax restrictions on cryptography and telecommunications technology, despite dramatic changes in Eastern Europe. Instead of focusing on specific national security needs, our delegates continued a blanket opposition to secure network communication technologies.

While the State Department opposed efforts to promote technology overseas, the Department of Justice sought to restrict its use in the United States. A proposal was put forward by the Justice Department that would require telecommunications providers and manufacturers to redesign their services and products with weakened security. In effect, the proposal would have made communications networks less well protected so that the government could obtain access to all telephone communications. A Senate Committee Task Force Report on Privacy and Technology established by Senator Patrick Leahy noted that this proposal could undermine communications privacy.

The public opposition to S. 266 was far-reaching. Many individuals wrote to Senator Biden and expressed their concern that cryptographic equipment and standards should not be designed to include a "trapdoor" to facilitate government eavesdropping. Designing in such trapdoors, they noted, is no more appropriate than giving the government the combination to every safe and a master key to every lock.

We are pleased that the provision in S. 266 regarding government surveillance was withdrawn. We look forward to Senator Leahy's hearing on cryptography and communications privacy later this year. At the same time, we are aware that proposals like S. 266 may reemerge and that we will need to continue to oppose such efforts. We also hope that the export control issue will be revisited and the State Department will take advantage of the recent changes in East-West relations and relax the restrictions on cryptography and network communications technology.

We believe that the government should promote communications privacy. We therefore recommend that the following steps be taken.

First, proposals regarding cryptography should be moved beyond the domain of the intelligence and national security community. Today, we are growing increasingly dependent on computer communications. Policies regarding the appropriate use of cryptography should be subject to public review and public debate.

Second, any proposal to facilitate government eavesdropping should be critically reviewed. Asking manufacturers and service providers to make their services less secure will ultimately undermine efforts to strengthen communications privacy across the country. While these proposals may be based on sound concerns, there are less invasive ways to pursue legitimate government goals.

Third, government agencies with appropriate expertise should work free of NSA influence to promote the availability of cryptography so as to ensure communications privacy for the general public. The National Academy of Science has recently completed two important studies on export controls and computer security. The Academy should now undertake a study specifically on the use of cryptography and communications privacy, and should also evaluate current obstacles to the widespread adoption of cryptographic protection.

Fourth, the export control restrictions for computer network technology and cryptography should be substantially relaxed. The cost of export control restrictions are enormous. Moreover, foreign companies are often able to obtain these products from other sources. And one result of export restrictions is that US manufacturers are less likely to develop privacy-protecting products for the domestic market.

As our country becomes increasingly dependent on computer communications for all forms of business and personal communication, the need to ensure the privacy and security of these messages that travel along the networks grows. Cryptography is the most important technological safeguard for ensuring privacy and security. We believe that the general public should be able to make use of this technology free of government restrictions.

There is a great opportunity today for the United States to play a leadership role in promoting communications privacy. We hope to begin this process by this call for a reevaluation of our national interest in cryptography and privacy.

Mitchell Kapor, Electronic Frontier Foundation
Marc Rotenberg, CPSR
John Gilmore, EFF
D. James Bidzos, RSA
Phil Karn, BellCore

Ron Rivest, MIT
Jerry Berman, ACLU
Whitfield Diffie, Northern Telecom
David Peyton, ADAPSO
Ronald Plesser, Information Industry Association
Dorothy Denning, Georgetown University
David Kahn, author *The Codebreakers*
Ray Ozzie, IRIS Associates
Evan D. Hendricks, US Privacy Council
Priscella M. Regan, George Mason University
Lance J. Hoffman, George Washington University
David Bellin, Pratt University
(affiliations are for identification purposes only)

### *NIST announces public-key digital signature standard (John Gilmore)*

Date: Thu, 27 Jun 91 11:39:59 -0700
>From: gnu@toad.com
Subject: NIST announces public-key digital signature standard

Statement of Raymond G. Kammer, Deputy Director
National Institute of Standards and Technology
Before the Subcommittee on Technology and Competitiveness
of the Committee on Science, Space, and Technology
On Computer Security Implementation
House of Representatives, June 27, 1991

Digital Signature Standard
I know that you are interested in our progress in developing a federal digital signature standard based upon the principles of public-key cryptography. I am pleased to tell you that we are working out the final arrangements on the planned standard, and hope to announce later this summer our selection of a digital signature standard based on a variant of the ElGamal signature
technique.
Our efforts in this area have been slow, difficult, and complex. We evaluated a number of alternative digital signature techniques, and considered a variety of factors in this review: the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S.,
the applicatility of patents and the level of efficiency in both the signature and verification functions that the technique performs.
In selecting digital signature technique method [sic], we followed the mandate contained in section 2 of the Computer Security Act of 1987 to develop standards and guidelines that ". . . assure the cost-effective security and privacy of sensisive information in Federal systems." We placed primary emphasis on selecting the technology that best assures the appropriate security of Federal information. We were also concerned with selecting the technique with the most desirable operating and use characteristics.
In terms of operating characteristics, the digital signature technique provides for a less computational-intensive signing function than verification function. This matches up well with anticipated Federal uses of the standard. The signing function is expected to be performed in a relatively computationally
modest environment such as with smart cards. The verification process, however, is expected to be implemented in a computationally rich environmnet such as on mainframe systems or super-minicomputers.
With respect to use characteristics, the digital signature technique is expected to be available on a royalty-free basis in the public interest world-wide. This should result in broader use by both government and the private sector, and bring economic benefits to both sectors.
A few details related to the selection of this technique remain to be worked out. The government is applying to the U.S. Patent Office for a patent, and will also seek foreign protection as appropriate. As I stated, we intend to make the technique available world-wide on a royalty-free basis in the public

interest.
A hashing function has not been specified by NIST for use with the digital signature standard. NIST has been reviewing various candidate hashing functions; however, we are not satisfied with any of the functions we have studied thus far. We will provide a hashing function that is complementary to the standard.
I want to speak to two issues that have been raised in the public debate over digital signature techniques. One is the allegation that a "trap door", a method for the surreptitious defeat of the security of this system, has been built into the technique that we are selecting. I state categorically that no trap door has been designed into this standard nor does the U.S. Government
know of any which is inherent in the ElGamal signature method that is the foundation of our technique.
Another issue raised is the lack of public key exchange capabilities. I believe that, to avoid capricious activity, Public Key Exchange under control of a certifying authority is required for government applications. The details of such a process will be developed for government/industry use.
NIST/NSA Technical Working Group
Aspects of digital signature standard were discussed by the NIST/NSA Technical Working Group, established under the NIST/NSA Memorandum of Understanding. The Working Group also discussed issues involving the applicability of the digital signature algorithm to the classified community, cryptographic key management techniques, and the hashing function to be used in conjunction with the digital signature standard. Progress on these items has taken place; however, as with the digital signature standard, non-technical issues such as patents and exportability require examination, and this can be a lengthy process. We have found that working with NSA is productive. The Technical Working Group provides an essential mechanism by which NIST and NSA can conduct the technical discussions and exchange contemplated by the Computer Security Act and also allows us to address important issues drawing upon NSA's expertise.

### *Re: Videotape of the pilot discussing the crash of UAL 232 (Robert Dorsett)*

Date: Sat, 29 Jun 91 00:28:11 CDT
>From: rdd@cactus.org (Robert Dorsett)
Subject: Re: Videotape of the pilot discussing the crash of UAL 232

>There's been a lot of discussion of the safety of fly-by-wire aircraft, so >here's the discussion of an accident that very possibly would have been >prevented were the DC-10 fly-by-wire rather than hydraulic.
As I'm sure Mary realizes, FBW does not alleviate the necessity for multiple-redundant hydraulics, and all the plumbing that comes with them. As currently implemented on most aircraft, it simply replaces the means by which the *hydraulic* actuators are operated. Instead of cables, there are electrical wires. These leads to one or more computers, which in turn process command
inputs from the pilot, leading to the possibility of unconventional control laws. Most of the controversy of FBW occurs at this stage. The severity of the failure involved would have happened whether the DC-10 were FBW or not.
Now, in rebuttal, I'm sure Mary'd point out that the FBW issue would only enter in the form of *control* issues subsequent to the accident, introducing unconventional control laws to effectively duplicate (or improve upon) the differential thrust technique Haynes used. And she has a point. But there's
always the question of whether the complexity and cost of such software will ever justify its usefulness in the "1:1e-9" catastrophic control failure case. In safety management, there is a point of negative return.
Perhaps a more salient observation would have been: this accident would not have happened if there was full manual reversion on the DC-10, ala the Boeing 707? :-)
Robert Dorsett Internet: rdd@cactus.org UUCP: ...cs.utexas.edu!cactus.org!rdd
End of RISKS-FORUM Digest 12.01
**********