

## FAX INTERCEPTION

This article is reprinted from Full Disclosure #23. Copyright (c) 1991 Full Disclosure. Permission granted by publisher to reprint when subscription information provided: Full Disclosure, Box 903-R, Libertyville, Illinois 60048, Phone: (708) 395-6200, Fax: (708) 395-6022, BBS: (708) 395-3244, Toll free: (800) 786-6184. Subscriptions: \$18 for 12 issues.

As with the introduction of all new communications technologies, there is a time lag between the availability of the technology and commercial development of interception devices. Accompanying the use of both are unanticipated risks and the potential for misuse and misunderstandings.

### False Sense of Security

With the widespread proliferation of fax machines came increased use. In general, a document transferred has been given the same sort of validity as one sent or received by U.S. Mail. In general, such communications were originally secure. Now that interception equipment is available, the sense of security has become false.

For all practical purposes, fax is a remote photocopying machine. The process begins with the sending unit converting the image on the page into a digitized image (numbers in an electronic format) and transmitting it as a noise sounding signal over a phone line. The receiving fax converts the signal into dots and prints it.

Since the image is transmitted over standard phone lines, the communication is subject to interception. However, rather than tapping the line with a tape recorder or simply listening to the oral communications, an interception device that makes sense of the specialized signal is necessary. Sometimes this is done by recording the transmission and later converting the recording of the modem signal to a computer image, sometimes it is done 'on the fly' as the signal is being intercepted.

### Simple Fax Intercepts

Why not just use a standard fax machine for interception? The signal sequences and handshaking at the time machines first connect complicates the possibility. During startup, the machines automatically select one of several built in protocols depending on line conditions. That is why on really noisy connections, the transmission of a page can take much longer. Directly connecting a 3rd fax machine to the line may confuse this process. Both the receiving unit and the intercepting machine would be sending signals about line conditions and protocol. However, if a 3rd fax machine did manage to get properly synchronized to the signal in use without interfering with the initial handshake, it would print an image identical to the one received by the intended recipient. We had mixed results when we tried this in our lab.

## FAXINT.TXT

Sometimes we managed to get all three machines synchronized. Using unmodified fax machines to attempt intercepts didn't provide sufficient reliability to be considered a viable approach. Indeed, continued attempts of this approach would likely put both sender and recipient(s) on notice that something was wrong as connections would be repeatedly lost.

This doesn't mean that it is really complicated to intercept faxes. The Philadelphia Inquirer reported in September 1990 that Japanese hackers have been stealing valuable information from corporations by using fax interception. The article claimed it could be done by anyone with a little knowledge of electronics. We agree, we have intercepted faxes in our lab. (See front cover for one such example.)

### Doing It Right

The latest commercially available fax interception devices generally use fax boards in IBM PC or compatible computers. The actual hardware used for fax interception is often the same as used by normal computer-fax systems. The software is more sophisticated. Rather than attempting to synchronize with the sending unit by sending protocol information, it adjusts to whatever protocol the two main players have established and stores the signal information.

After interception, the electronic information is stored in the computer and is available for review, to be printed, altered or discarded. Such equipment can be left unattended for long periods if necessary, or monitored for the instant use of information in cases where law enforcement is standing by waiting for some specific bit evidence.

### Cellular Fax Interception

Cellular phone based fax machines provide ripe opportunity for 'hacker' intercepts, since the signal is available via low cost police scanners. No physical connection to a common carrier network is necessary. There is absolutely no risk of being detected.

Commercial fax interception equipment gets more complicated, though. Since fax messages might be on the same phone lines as voice or other computer modem communications, some of the interception devices automatically route different types of communications to different interception devices. This provides the interceptor with a separate recordings of voice phone calls, faxes, and other computer communications.

Such fax interceptions are based upon the interceptor having a specific target. Distributing the sorts of information received for analysis isn't much different from an ordinary, now old fashioned, wiretap.

### Broadband Interception

## FAXINT.TXT

Presorting of signals and voice communications as described above makes broadband scanning for fax messages easy. The interception of satellite or microwave links has become possible. Cooperation by a common carrier with the government has happened in the past, and strikes a chord of dangerous reality today. But it really takes little by way of home fabricated equipment to monitor much of the satellite link traffic. Commercial equipment is also available. One commercial fax interception unit can decode up to 150 simultaneous fax transmissions from a 6,000 phone line satellite link.

Such broadband interception can also be done on oral calls, however, the task of listening to all the conversations for the important ones is much, much greater compared to scanning faxes. First, faxes are usually much more direct and to the point than normal phone conversations (not so much about Sunday's game). Additionally, optical character recognition (OCR) process can be used to convert much of the text to standard computer data and then be mechanistically selected for closer scrutiny by an automated search of keywords of interest. Encryption of a fax could also be noted, perhaps triggering further attention.

The risks resulting from broadband interceptions are heinous. Your fax could be intercepted not because you were a selected target of law enforcement, industrial spies or miscreant hackers, but because of the route your fax travelled through the common carrier networks. Broadband interceptions become a modern day version of general warrants. Satellite signals don't respect borders. Interception in nations with no privacy concerns for radio signals of what we, as users, understand to be Constitutionally protected communications has become a real threat. There are areas contained within our national frontiers where the United States Constitution does not apply. Foreign embassies present one such clearcut example. The status on Indian Reservations is not clearcut.

### Dangers of Fax

The February 13, 1990 issue of the American Bankers' Association publication ``Bankers Weekly'' reported that ``In one incident, a bank suffered a \$1.2 million loss through fraudulent funds transfer requests which were accomplished using nothing more than business letterhead, tape and scissors.'' A fax machine made such simple tools effective. Inordinate reliance on technology permitted the loss to actually happen.

The journal continues that there is a need for legislation (changes to the Uniform Commercial Code) to put a stop to the problem. Unfortunately, legislative efforts alone cannot correct the problem. The first step, is an understanding of the technology.

Once the technology is understood, administrative procedures can be implemented by users of fax machines to protect themselves. That protection

#### FAXINT.TXT

cannot be successful without understanding the limitations of the machinery. Taking any communications device for granted is a high risk path.

#### New Techniques For Fraud

The advent of fax technology has opened the door to new methods of fraud. Those intent on committing fraud have always devised methods of bypassing normal authentication systems in order to steal. As technology evolves, these methods also evolve. Protective measures must follow suit.

Faxes represent a multiple whammy. People who send faxes have some geographic distance between them. Because of past reliance on semi-automated communications, formal verification procedures are bypassed, substituting the mysterious nature of modern communications. There was a time, even recently, that tellers at banks asked for positive identification even in the case of small cash transactions inside a bank. Yet today we witness orders for large sums being processed simply because ``it came by fax.'' This is truly a conspiracy of laxness and misinformation.

A written purchase order from a company is likely to have a particular form, and include a signature. One attempting to issue a fraudulent purchase order would need to forge both the form and the signature. Additionally, envelopes and possibly a postage meter imprint from the issuing company would also be needed. Elsewhere in this issue we reprint a letter from the Federal Communications Commission. The letterhead was, for reasons we have been unable to determine, typed instead of printed. Some of the recipients we've talked to have placed calls to verify the authenticity of the letter. As it turns out, the letter was authentic and official.

A purchase order sent by fax on the other hand, can be created by cutting, pasting and xeroxing together parts of other orders from the company. When received by fax, the fake would appear legitimate.

#### PC's & Fax: The Miscreants Gun

The advent of PC based fax boards exaggerates these problem. A fax that originates, is received by, or intercepted by a personal computer (PC) fax board really opens the door for miscreants.

A fax, when stored on a PC is easily modified using ordinary commercial software intended for preparation of graphics. An image of the fax can be brought up on the screen and parts of it altered or cut and pasted electronically. For example, a purchase order could have a shipping address altered. A signature could be removed from one document and placed on another. All such operations can be done on a computer screen in moments. Document changes that could take a professional forger hours to accomplish could be done in minutes by an amateur, even an underage one.

#### FAXINT.TXT

Bogus faxes can be created to be sent to another fax, or incoming faxes could be altered by an employee and printed as authentic. Detection is difficult to impossible, depending on verification techniques used at audit.

The difficulty of intercepting standard U.S. Mail or voice phone calls and altering the content by a third party is enormous compared to fax messages. Before a fax message is printed, it is just a series of electrical signals. Any alternations result in changes without a trace of the alteration.

The receipt of a fax is <B>not<D> a confirmation of its content, unless other corroborative authentication validates the information.

Someone with access to a phone closet can route incoming fax line to a PC. The fax can then be connected to a different phone line. All incoming faxes would be first received by the PC and the operator could alter, erase, or forward without change those faxes to the standard fax machine. A pre-review and alteration if desired scheme can be effected. The same can not easily be accomplished with normal voice phone calls, or the U.S. Mail.

With the advent of the Caller-ID services, this information should soon be incorporated into fax machines, so the true number of the caller will be placed on the fax. This will still do nothing to prevent transmission of bogus faxes over that phone line.

#### Protect Yourself

The best rule for protecting one's interests when using faxes is to use them only with other confirmation or as confirmation of other communications. They should never be used for final copies of contracts, purchase orders or other important documents that could have a significant impact if altered, or entirely fabricated. Where would we be if our WW2 treaties terminating hostilities were faxed documents. Additionally, information that would not be given out over a standard phone conversation, subject to a wiretap, or other listeners (via a speakerphone, extension, etc), should not be sent by fax. There is no way to tell who may pick up a received fax and read it. In fact, it is more likely an unintended party will read a fax than pick up an extension phone and eavesdrop on a voice call (intentionally or not).

It should be kept in mind that any errant employees or others that could get access to the fax phone line(s) could intercept all faxes sent or received and make use of the fax images for whatever purpose they desired.

The intercepted faxes can be used to collect or create incriminating evidence, industrial espionage, or as the base of documents to be used in forgery. There's a whole new meaning to autograph collection.

#### Conclusion

#### FAXINT.TXT

Fax technology in its current form provides a useful service for business and others. However, the risks must be examined so the use doesn't go beyond that which is appropriate given its current functionality / risk ratio.

In conclusion, the convenience of a fax must be weighed against its risks and procedures implemented to authenticate incoming and outgoing faxes as well as what information is communicated by fax. As with all technologies, it must be understood so that it can be used for purposes that are appropriate for the needs of the technology and the user. A lack of understanding can leave the user exposed to unnecessary danger, liability and loss. When used with an understanding of the benefits as well as the pitfalls, a fax machine can greatly enhance productivity.

Downloaded From P-80 International Information Systems 304-744-2253