INTERNAL AUDITOR
JOURNAL OF THE INSTITUTE OF INTERNAL AUDITORS

April 1989 XLVI: 2

Perimeter Security for Telecommunication With External Entities

by Hanan Rubin and
Allan R. Paliotta

Perimeter Security for Telecommunication with External Entities

WE LIVE IN AN "Information Age." A new infrastructure, a pervasive network of electronic processing and telecommunication, is impinging on the millions of business, governmental, educational and personal enterprises in the world and the interactions among them.

When a culture experiences such fundamental change, both problems and benefits may occur. One immediate, practical problem confronting businesses and other organizations is how to deal with a new exposure that threatens them.

Background

The problem first presented itself some years ago when computer hackers discovered clever, often playful, ways to use and experiment with telecommunications. In many cases, the hackers invested much time in penetrating the computer environments of various entities.[1]

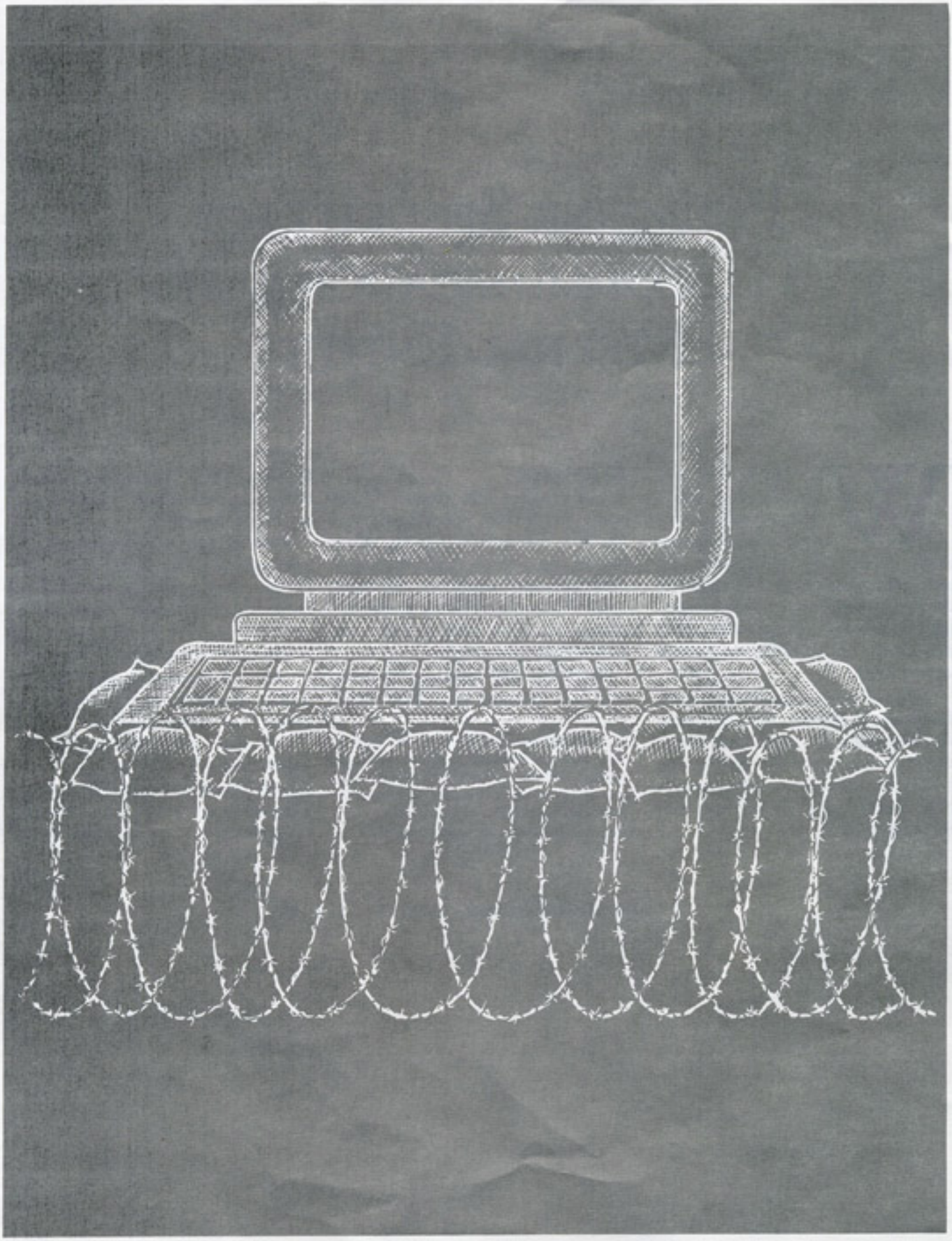
Typically, the hackers' motives were not personal gain, but "fun." However, their pranks jeopardized medical, governmental, educational and business records.

More recently, some highly talented computer experts have gone well beyond the bounds of the original hackers. At times, these experts (some of whom may be geniuses) seem to be driven by the ambition to damage—or toy with—the institutions of our society. Possibly, their real desire is to flex their mental muscles.

The much-publicized computer viruses are often the work of such experts. It is now common knowledge that these programs can destroy computer files at pre-set future times

[1] "Computer environment" in this context means the combination of all the computer facilities and the internal telecommunication network(s) of an enterprise, including the hardware and software of mainframe computers, as well as mini- and micro-computers.

by Hanan Rubin and Allan R. Paliotta



or when certain events occur. The programs can reproduce themselves and propagate within a computer environment. The potential devastation is alarming.

The risk of damage has been heightened by the trend toward "any-to-any connectivity" in modern computer environments. Even though such connectivity can improve performance, it may also help an outsider roam through the computer environment at will.

Perimeter security

To protect the computer environment from outside penetration and computer viruses, organizations need to adopt new approaches. In the past, for example, a particular company's telecommunication may have been confined to a "closed" internal network of leased lines. Outsiders had no means of access.

This same company may now have installed gateways, allowing outsiders to access certain business systems. Although this arrangement offers business advantages, it also introduces opportunities for outsiders to attempt unauthorized access and tampering.

For increased protection, computer operations should establish a perimeter security layer in addition to existing controls within the computer environment. This additional protection can be provided by what the authors propose to call an electronic "escort system."[2]

In basic terms, an escort system functions so that an outside entity (a person or a computer) reaching a gateway is first required to provide identifying information together with a password. The escort system immediately retrieves a menu of the business systems that are authorized for that entity. (The menu may or may not be presented to the outsider. In the latter case, the outsider would be required to know his menu options, thus adding further security.)

"The escort concept is still appropriate when a telecommunication connection is initiated by one's own company."

Upon selecting a menu option, the outsider is next given a computer facility or screen that is within the selected system. The outsider is thus "escorted" from the perimeter of the computer environment directly into the authorized business system.

A further password and/or other identifying information may then be required. In any case, the key point of an escort system is that *an outsider reaching a gateway will not obtain a general facility or entrance screen of the company's network or operating software; nor will he be given a capability for inputting commands to the network or the operating software. Thus, the outsider will not be "invited" to browse or to attempt unauthorized access.*

In general, such an escort service would be operated by an intelligent controller (that is, a computer device) protecting the gateways into the network, thereby providing security at the perimeter of the computer environment. Security systems of this general type are starting to be seen in a number of different industries, including banking, insurance, public data network services, and computer consulting and software.

Once an escorted entry has been made into a business system, further security measures are needed to protect against access elsewhere. Ideally, a system would escort the outsider back out of the computer environment upon normal or abnormal termination of a computer job.

In some instances, a business system may internally generate a sign-on to another business system. Such further access for an external entity (better yet, for any user) should be appropriately controlled.

The "clear screen" option may provide the opportunity to obtain further access and could lead to unauthorized roaming about the computer environment. This option should therefore not be available to outsiders unless adequate control over its use has been established.

The escort concept is still appropriate when a telecommunication connection is initiated by one's own company. In that case, protection is needed against potentially harmful content concealed in subsequent telecommunication from the outside.

Even though an escort system adds significant protection to that provided by controls at the data access level, it is only one part of the control structure needed to address external telecommunication. Two other important components, taken together, are called "message authentication."

As in the escort system, the first component requires positive confirmation of the outsider's identity. Confirmation may be obtained by one or more passwords, by the ability to provide private data when requested, by the ability to respond correctly to a variable challenge word, and so on.

In the case of an attempted dial-up connection, special procedures or devices are used for confirming identity. One method uses a commercially-available callback device. It requires the caller to disconnect and then to await an automatic callback at the external entity's telephone number of record.

Another method, even more effective, is to require the caller to use a

[2]Some readers may be familiar with the 7-layer model for "Open Systems Interconnection" established by the International Standards Organization. The security ideas in this paper are in line with that model. They apply to the same layers. Perimeter control via an escort system fits into layers 3 and 4; the controls that exist at the data access level fit into layer 5. A corresponding situation prevails, of course, for SNA layers.

hardware device known as a "token" when requesting the telephone connection. Tokens are essential if the caller (perhaps a sales representative) places calls from different telephone locations.

The second component of message authentication is the assurance of the integrity of transmitted messages—that is, the assurance that no message or part of a message is repeated, altered, or dropped. Contribution to such assurance may be made by the telecommunication ground rules known as "protocols," by various commercially available devices and software packages, and by the complex scrambling of messages via encryption.

Security within a computer environment

In addition to an escort system and message authentication, effective security requires key administrative and data access controls as well as program change management procedures. Umbrella security packages (such as RACF, ACF2 and Top Secret) should be installed to restrict access to electronic systems and files, data elements, and programmed user functions. (Protection is most effective when such security is installed so that access is denied whenever not specifically authorized. In the event security were ever lifted, processing should stop.)

Program change management procedures should be instituted to prevent the updating of production programs by other than authorized individuals. These procedures would also provide an audit trail of updates.

Long-term backup procedures should be developed to provide pre-infection copies of software for recovery purposes in the event of a virus attack. (Long-term backup is especially important for recovery from "time-bomb" delay viruses.)

Computer personnel should be instructed that, in the event of unusual computer performance or a strange processing problem, one of the possible causes may be a virus. Personnel with appropriate expertise should deal with the situation. *Backup programs and files should not be used until the matters are resolved.*

A security awareness program should be conducted on an ongoing basis to publicize precautionary measures. For example, downloading programs from public bulletin boards, using personally acquired software on corporate equipment, and executing programs from uncertain sources should all be outlawed. Employees should be required to sign a statement, preferably every year, acknowledging individual responsibility for compliance with corporate security policies and procedures.

Beyond the above controls and additional "environmental" controls (which need not be delineated here), there will be application controls specific to each business system. Even if the overall control structure for using a business system seems satisfactory, it may still be necessary to get an external entity to commit to it. A signed agreement with the external entity which requires compliance with the established controls and with other appropriate security measures may be needed.

Perimeter security in the future

An even stronger perimeter control over external telecommunication, an "intelligent messenger system," may become the perimeter security system of the future. This approach represents an improvement over the escort system; and, in a simpler form, it is already being used for some on-line inquiry systems.

Here is how the simpler version works: in an on-line inquiry system that permits external access, the outsider is served at the perimeter of the internal network (that is, at a gateway) by an "electronic messenger." The messenger carries inquiries to the business system and brings the requested information to the outsider. *The outsider does not enter the computer environment.* (A commercially available device for this specific purpose has been used as the controller that runs the intelligent messenger system.)

In the future, not only inquiries, but all transactions from external entities could conceivably be handled in a similar manner by an intelligent messenger system. Such a system might reformat all incoming transactions, generating the actual input to be applied and delivering it to the appropriate business system. Since the transactions would be executed from the reformatted input (which is internally generated), the intelligent messenger system would, in effect, block computer viruses and other surreptitious inserts by outsiders (if the design of the reformatting were clever enough). Specific virus-filtering techniques might also be introduced at this point in the processing logic.

An electronic messenger could deliver on-line output from the business system to the controller at the perimeter of the network for relaying to the outsider. *External entities could not enter the computer environment—not even for providing input or for receiving output.*

Reports indicate that plans for preliminary versions of intelligent messenger systems are already on some drawing boards. However, an appreciable development effort will be required before the concept is adaptable for general use. Specific development will be needed for each business system, particularly for the reformatting of the input, although some general-purpose routines may be developed to assist in that process.

The isolation of outsiders by intelligent messenger systems would go considerably beyond that provided by an escort system, and intelligent messenger systems could turn out to be one of the ultimate answers to external tampering and the virus problem. Until such a system is widely available, however, the controls within a computer environment should be supplemented by an escort system, thereby adding a needed layer of perimeter security. Of course, utilizing an escort system would not obviate the need for taking suitable

actions against the threat of internal tampering, errors, and fraud.

Conclusions

Companies using business systems which telecommunicate with the outside must utilize new approaches to protecting the computer environment. A control mechanism, an escort system, should be added now, thus providing a perimeter security layer. In the future, an even stronger control may be provided by intelligent messenger systems. Also, existing security awareness and controls must be maintained.

In essence, companies face these options in dealing with telecommunications security: (1) refraining from external telecommunication; (2) accepting the risks involved in present systems; or (3) establishing a higher level of security such as the escort system and the intelligent messenger system.

Hanan Rubin, PhD, CIA, CISA

is a vice president of the Metropolitan Life Insurance Company. He is in charge of the EDP Auditing Division, which he established, and two general/financial auditing units. He has held other technical and management positions in the computer field and has also been an Assistant Professor of Mathematics and research scientist at the Courant Institute of Mathematical Sciences of New York University. He is a member of The Institute of Internal Auditors Board of Research Advisors and a vice president of The Institute's New York Chapter.

Allan R. Paliotta, CISA

is manager of the EDP Auditing Division at the Metropolitan Life Insurance Company. He has spent 17 years in technical and management positions in data processing, two years in operational analysis, and six years in EDP auditing—all at Met Life. He is a member of the New York Chapter of The Institute of Internal Auditors and is a vice chairman of the IIA's 1991 International Conference, which will be hosted by the New York Chapter.