Chapter 8: Security and copyright

"We are at a crossroads. Are we going to have the tool of electronic surveillance, or are we going to let criminals use the national information infrastructure unfettered?' James K. Kallstrom, special agent in charge of the Federal Bureau of Investigation's New York office.'

"A lot of people here are very, very paranoid." Emmanuel Goldstein, publisher *2600: The Hacker Quarterly.*[2]

Internet security is an oxymoron. An *open system* by definition permits to some degree unfettered access. As recently as 1988, *security* meant disaster recovery. Now it has a richer, more varied and significantly more complex set of associations. Furthermore, many of these strike at the core of electronic information itself. "There is a trend to work in groups. And there is also a trend toward going after things that have some kind of financial value rather than curious folks just cruising the Internet" said Richard Petthia, CERT co-ordinator.[3]

Discussions of security oscillate between several different connotations of the term. First, there is the issue of access to the *system.* When referring to the Internet, a user may have different types of access, limited to one-way electronic mail services, or full *telnet* access. A wide range of software and hardware tools is available to manage system access. The responsibility for security falls upon the entity providing system-level access. This may be a local provider, or a university.

The second sense of the term 'security' is access to a particular server or certain files on that server. Most users are not aware of server-level security. The *secure information* is not displayed to the typical user. The information may be on the server, but hardware or software locks have been installed. A person logging into the University of California-Berkeley may find that certain files that were available

[I] Quoted in *The New York Times* by Edmund L. Andrews in 'US plans to push computer coding police can read,' 5 February 1994, page 29.

[2] Comment quoted in the *The New York Times,* 26 March, Business Section National Edition, page 1. The occasion was the 1994 Computers, Freedom and Privacy Conference in Chicago. 'Emmanuel Goldstein' is a *nom de plume* and is taken from a character in George Orwell's 1984. Subscriptions to 2600 are $21 for individuals, $50 for corporate subscriptions. Outside the US, individuals' subscriptions are $30 and corporate subscriptions are $65. Write P.O. Box 752, Middle Island, NY 11953.

[3] John Markoff, 'Keeping things safe and orderly in the neighbourhoods of Cyberspace,' *The New York Times,* 24 October 1993, page 7.

weeks or days earlier, no longer appear. Security is a server-level responsibility on a geographically-distributed system such as the Internet.

The third sense of the term is one that is often implicit in discussions of system security. The purpose of security is to restrict or control access to certain information. From the point of view of individuals or organisations who sell software, value-added information or provide transactional information, *security* translates into financial ownership and re-use considerations. A specific software program must be purchased. Unauthorised distribution of that program deprives the seller of income. Those with legal training speak of *security of trading,* and it is in this sense that hardware and software interact to allow the rightful customer access to information and the non-customer to be denied access.

In the Internet environment, managing security at the system and server level is demanding. The tasks fall upon organisations of many types and historically on a significant amount of volunteer labour. The third sense — the one which touches upon copyright, patents, trade secrets — remains after 30 years a troublesome problem and seems to be an issue that will be difficult to resolve in the electronic environment. Protecting intellectual property and confidential information in an open system environment raises difficult conceptual issues about the nature of electronic information, indeed about the nature of knowledge and knowing. Epistemology has ranked with watching paint dry as an adjunct to electronic publishing. More practically, setting up mechanisms that can manage and levy fees for *electronic information* in the Internet environment proves to be a daunting technical, conceptual and dazzlingly complex series of tasks.

Solutions will emerge over time. There are some suggestive developments in hardware and software that will permit different types of controls that will address system, server and information security issues. Regrettably, it is unlikely that these challenges will be successfully resolved in the next five to eight years. Electronic information available on the Internet and changing with what appears to be ever-increasing pace, is simply too new and too fluid.

1. A secure Internet?

In early 1994, seven sites suffered ‘sniffer’ attacks. Dain Gary, manager of the CERT Co-ordination Center, the oldest of the Internet intrusion tracking services, reported a 73 percent increase in incidents in 1993.’ But the 1994 activity was several orders of magnitude greater.

[1] CERT is located in Pittsburgh, Pennsylvania, near Carnegie Mellon University, one of America’s premier computer and software engineering institutions. Information about Internet security is available by sending electronic mail to *cert@cert.org*. Documentation about security can be obtained via *ftp* at the same address. The 24-hour telephone hotline number is 412-268-7090. CERT’s 1994 budget is $2.4 million. The request is to raise the budget to $5 million and doublc the staff from 14 to 30. There was a 39 percent increase in the number of sites affected by security incidents. See Elizabeth Silorovsky, ‘Explosion in growth, security issues drains CERT resources,’ *Federal Computer Week,* 28 March 1994, page 4.

Intruders exploited Internet system weaknesses to capture passwords and monitor network traffic. Internet providers NEARNet and BARRNet acknowledged security breaches. Other sites targeted by intruders were the University of Texas, and Rice University. CERT, the Computer Emergency Response Team, issued an advisory and urged users to change passwords. "We're seeing automated attacks involving thousands of hosts" said the manager of CERT.'

A *sniffer* program captures passwords and can give unauthorised users access to a node, a computer that acts as a gatekeeper to the Internet. The sniffer program intercepts and stores user passwords. The person who launched the sniffer retrieves the passwords and uses them to gain access to any files attached to these passwords. The importance of security attained international attention in 1988 when Robert Morris Jr. launched the Internet Worm. Mr Morris's program tested passwords that would grant access to privileged UNIX accounts. (A privileged account allows the user to take control of the UNIX system at a particular site.) When Mr Morris' program discovered a password, the program copied itself to another UNIX host. (The program replicated itself rapidly enough to impair system performance. Thousands of Internet sites had to take their servers offline and erase the errant program and its copies. Mr Morris was found guilty and sentenced to community service, not prison.)

The upswing in intrusions began several years ago. It coincides with the explosion of interest in the Internet and a simultaneous crack-down in the United States on pirate bulletin boards. The *hackers,* a term used in a pejorative sense to describe such unauthorised computer intruders, have become celebrities, of a sort.

These hacking incidents were publicised, but not by the Internet Society or any of the watchdog groups who monitor the Net. Information about the attacks came from Alexis Rosen in late 1993, president of Panix Public Access in New York City, an Internet access provider. Only after several months passed did CERT issue precautionary measures.[2] Mr Rosen has been critical of the amount of time taken by CERT to notify Internet users. "There's nothing worse than a watchdog that doesn't bark reliably" said Mr Rosen.[3]

The news of the attacks on the Internet comes at the same time more commercial organisations are using the public networks to conduct business, and when publishers are launching network publishing operations. It is unlikely that these attacks will slow the commercialisation of the Internet, but they do increase the priority of

[1] Ellen Messmer, 'Group warns of growing security woes on Internet,' *Network World,* 28 March 1994, page 9.

[2] Another security group is FIRST (Forum of Incident Response and Security Teams). The National Institute of Standards and Technology sponsors the secretariat for FIRST. It has no budget.

[3] Brian Livingston, 'The Mother of all networks, *PC Computing,* April 1994, pages 180 and following.

security issues, particularly for such information products and services as software and electronic distribution of for-fee information.

2. Security challenges

Several basic challenges to security exist. The principal one is inherent in UNIX itself: everything is a server. As the number of users grows, the likelihood that some users will attempt to breach security rises. With an appropriate protocol test device, a knowledgeable person can read unencrypted messages. (Local area networks can be more easily compromised by low cost protocol devices than wide area networks. Rapidly dropping prices and dramatic advances in technical functionality for network troubleshooting devices raises the spectre of more sophisticated intrusions aimed at high-value information.)

Equally basic to the Internet is the tenet that networks link to other networks. The thrust is for additional connectivity. A single local area network is manageable in most situations. When that network connects, security becomes a larger task. For many organisations, security may no longer be manageable.

Today's network environment is characterised by:

- Proliferation of Internet connections (public connections, not private connections for wide area networking).

- Rapidly increasing numbers of mobile computers (portable computers and wireless links).

- Geographically dispersed nodes in more than 50 countries, with 80 countries having electronic mail access.

- Cross platform computing (UNIX, Macintosh, IBM-compatible, Sun SPARCstations, among others linked in one environment) which is inherently more fragile than a homogeneous computing environment operating under strict controls in a single location.

- Continued reliance upon UNIX, which is garnering enhanced security features.

Furthermore, the reality is that high hurdles must be cleared before Internet-linked networks provide security of trading:

- Portable computers are one of the fastest growing segments in the computer hardware industry. They are easy to steal, not for the hardware which is becoming a mere commodity, but for the software, log-on scripts and access codes.' Wireless and traditional cable links can be tapped. Monitoring intrusions becomes more difficult for many organisations because tools to log and track break-ins are expensive and costly to maintain.

- Remote sites can be difficult to protect because of distance, the lack of an on-site trained staff, the difficulty of inspecting sites on a regular cycle.
- The weakest link in security is the behaviour of an *individual.* Users write down passwords. Systems that provide specific access to information and have the capability of billing the user are rudimentary, and, for most organisations, impractical because of the cost and complexity of the hardware and software systems needed to meter and control access.
- UNIX is, by definition, *open.* UNIX is a peer-to-peer operating system. It was not designed for security; easy connectivity was a design parameter.

An important question becomes, 'Can a public network such as the Internet be secure?' The answers range from 'Sometimes' to 'Not economically.'

It is important to recognise that security and copyright issues notwithstanding, the Internet juggernaut is not likely to be slowed in the next twelve to 36 months. As UNIX becomes more popular as the operating system for connecting to the Internet, security issues will remain an after-the-fact concern. The Internet will be used by entrepreneurs because it is cheap and readily available. Large organisations will push to introduce Internet-based services because of directors' fears that they will miss an opportunity.

3. US government activity

The US government believes that security on the information highway is a requirement for commercial success. To help ensure security, the Clinton administration introduced in 1993 a dramatic proposal to standardise computer and telecommunications encryption. (Encryption means that a voice or data message is scrambled using a key. The key may be a number or a string of letters. Without the key, the voice or data communication cannot be read. However, the wide access to public domain decrypting software routines and powerful computers means that a knowledgeable person can, using trial-and-error linked with mathematical techniques, break the code.)

According to Al Gore, "Encryption is a law-and-order issue, since it can be used by criminals to thwart wiretaps and avoid detection. Our policy is designed to

[1] Many portable computers are set up to allow users to access remote networks. The log-in process is stored in the portable's communications program. A stolen portable provides easy, immediate access to those systems. The password — that is, access to information — has *value* to the thief.

provide better encryption to individuals and businesses while ensuring that the needs of law enforcement and national security are met.”

The Capstone encryption policy is aimed at wiretapping, but its critics fear the technology can and will be extended to data communications.’ In practical terms, Capstone, incorrectly called the *Clipper Chip,* allows the government to have access to any message encrypted using the technology. For a government official with the ‘key’, no tedious hacking is necessary. To further assist the US crime bureaux, generic signatures in the Clipper Chip contain a Law Enforcement Access Field (LEAF), embedded in any transmission. Removing, tampering with, or altering the LEAF would be illegal and detecting such a message would trigger an investigation. The technology upon which Clipper is based is called *key escrow.* Messages are encrypted with private keys. However, any encrypted message built on Clipper could be decoded using the key to which the government has access. Supposedly, privacy would be assured under normal conditions. However, determined hackers can break most known codes. A flaw exists in the so-called Clipper Chip so that even before widespread deployment, its algorithms are no longer fully secure.

Despite the strong negative reaction from commercial vendors of encryption and other data protection products, the concept provides some insight into how governments are likely to react to the difficulties law enforcement officials face when they have to confront encrypted and, therefore, secret message streams in a global electronic Total Network environment. The Clipper Chip is an unpopular proposal by President Clinton’s administration to make computers and telephones “easier to bug.”[2] Surveillance is a *design* goal. Law-enforcement agencies would be able to gather evidence of illegal activities.[3]

The US government cannot require private manufacturers to incorporate the technology into their products. However, Federal agencies can mandate that US government suppliers include the Clipper technology in voice and data communications products. The buying power of the Federal government is significant, and opponents fear that many suppliers will include the technology in order to retain government contracts. The result may be Clipper’s becoming the *de facto* standard for data encryption. The Justice Department has ordered $8 million in equipment that incorporates the technology.[4] The US government would relax the export restrictions on Clipper technology but keep export controls in place for other encryption technologies. The counter argument is that law enforcement officials

[1] *Tessera* is the Capstone technology applied to data communications. *Clipper* refers to the technology embedded in telephones.

[2] Peter H. Lewis, ‘Collisions in Cyberspace on data encryption plan,’ New *York Times,* National Edition Business Section, pages 1, 26.

[3] The decryption algorithm *Skipjack* would remain classified. The National Security Agency has been developing the chip housed in a tamper-proof package, in a self-contained central processing unit containing the Skipjack algorithm.

[4] Ironically, a Bell Laboratories’ researcher cracked the Clipper algorithm in May 1994.

without an edge cannot do their job. Privacy effectively makes law enforcement officials' jobs more difficult, if not impossible. Clipper gives officials an advantage.

Critics of the Clipper proposal argue that the 1987 Computer Security Act is the cornerstone of US cryptography policy. It is unclear what organisation will hold the keys needed to unscramble voice and data communications. To dispel the surge of criticism for the proposed back door to encrypted private messages, the Administration proposed that the National Institute of Standards and Technology, and the Treasury Department's Automated Systems Division, would act as the escrow agents for the decryption key. Another approach is the recommendation for the Justice Department to designate a permanent key holder outside the executive branch of the US government. Another option is to entrust the decryption key to an office within the court system.

Critics say that Clipper will fuel an interest in encryption technology developed outside the US. Criminals would use technology that would make the enforcement officials' job harder and protect the secrecy of their communications. Another concern is that its security remains unproven. To make this standard effective, other means of encryption over telephone lines would have to be prohibited.

Other US governmental activity is receiving support as well. The National Security Agency, NSA, said that it would develop software that would prevent intruders from capturing the digital signatures used for authenticating user identities in the Defense Message System, the military's next-generation electronic mail system.

The National Institute of Standards and Technology (NIST) is planning a TCP/IP Firewalls Initiative. Information and guidance on Internet connection and security design will be provided.

3.1 Other security activity

Most versions of UNIX are open; that is, they do not provide system administrators with powerful tools to enforce the security of the particular system. UNIX, System 4.2 has received a National Security Agency B2 classification. Windows NT is a classification C2 network.'

The growth of open, distributed networks has generated a corresponding rise in security standards activity. US government security modes, outlined in the 'Orange Book' standards, are but one effort. Class C2 is the level most widely implemented.

Several other initiatives are under way. For example, the Joint Technical Committee of the International Organisation of Standardisation/International Electrotechnical

[1] A B2 level of security means that a user is sealed off from knowledge of any other user. A B1 level of security defines mandatory controls. A C2 level of security defines specific mandatory controls. The US NSA (National Security Agency) certifies products' levels of security. Informix Software Inc.'s OnLine/Secure relational database management system was given a B2 level of security.

Commission (ISO/IEC) has created an Open Systems Interconnection (OSI) security document (IS0 7498-2) for the OSI reference model. The OSI reference model, a standard for worldwide communications, defines a framework for implementing protocols in seven layers.

The IS0 document discusses complex issues related to open systems security. It deals with security frameworks that cover areas such as authentication, access control, confidentiality and key management. It also covers security in databases, directories and Structured Query Language (SQL) constructs.

Other subjects addressed in IS0 7498-2 include security in system management. This looks at areas in Common Management Information Services (CMIS) such as audit and alarms. In addition, OSI application security models are presented which focus on file transfer, transaction processing and terminal operations.

Despite the comprehensiveness of IS0 security, its problem is lack of acceptance. It is mostly unimplemented, and there is uncertainty as to how it relates to evolving vendor security mechanisms.

Three other security efforts of note are the Portable Operating System Interface for UNIX (POSIX), UNIX SVR4 ES and Kerberos (discussed below).

POSIX is a product of the Institute of Electrical and Electronic Engineers (IEEE), which proposes in its 1003.6 work group to "specify functional requirements and a system interface standard for security, auditability and control mechanisms in POSIX." Specifications are being developed for access control, partial Orange Book conformance, user privileges and audit trail definition.

A new POSIX security project is looking at the difficult issues associated with distributed security. In its early stages, the working group is trying to identify necessary services, the nature of security application programming interfaces (APIs), as well as the group's relationship to other standards efforts.

Novell's UNIX System Laboratories (USL), Summit, N.J., manages the fortunes of UNIX System V. Its Enhanced Security version (SVR4 ES) includes a comprehensive array of protection features that encompass the B2-level of security. It also offers some B3-level features and closes some UNIX security holes.'

In response to the recent surge in reported intrusions, the Internet Engineering Task Force has stepped up its efforts to set more stringent security standards. The IETF, the standards-setting body for the Internet, has established a working group to study the reports of Internet security problems.* Its other actions were to call attention to

[1] Jerry Cashin, 'Open, distributed users tightening UNIX security,' *Software Magazine,* January 1994, pages 8 1 and following.

[2] Terry Tam, 'Standardising security: the IETF distributed security model would allow central management and interoperability', PC *Week,* 24 January 1994, page N3.

vendors who install systems that are not secure, and network mangers who have not made security a priority.

The Internet Engineering Task Force (IETF) has proposed a generic security model by which remote-access products would be able to inter-operate with third-party or standards-based security systems currently on the market. The IETF proposal calls for a generic distributed security authentication model. It theoretically allows the built-in security features included with each remote-access product to interact with third-party or standards-based security systems.

The IETF security standard would help relieve some of the burden placed upon technology developers and hardware manufacturers of making proprietary security systems compatible with other vendors' products. If adopted, the standard could evolve into a public domain collection of security interfaces compatible with most authentication and authorisation servers.

However, committee and volunteer processes on which the Internet depends to a large degree, move slowly. Standards emerge; they are not mandated. Organisations must deal with Internet security by selecting from the various hardware, software and procedural options available.

4. Routine challenges: passwords and electronic mail

The best security is not to have confidential or vital information on any computer that is connected to the Internet. But for many organisations, particularly publishers, the Internet represents a quantum leap in marketing and distribution to ignore.

4.1 Passwords

Security experts know that password-only systems provide little or no protection against intruders. Hackers can intercept or gain access to passwords. Password-only systems can be breached by a number of methods, including trial-and-error.

Most systems do not implement password protection beyond that provided in the standard UNIX tool set. Furthermore, most systems do not require that the user create a new password on a regular cycle, for example, every 30 days.

Because the Internet is a collection of different systems, the security procedures across the thousands of servers vary widely. Some installations are secure; others are not. Most minicomputer and mainframe installations have built-in security for remote log-ins to their terminal servers. Some overworked system administrators implement minimal security levels; others find security procedures to be cumbersome. Often the administrator does not have the time and resources to implement more effective security.

A security truism is: 'Network security is more difficult than mainframe security. The more distributed the environment, the more complex. The more open the network environment, the more difficult security becomes.' In the Internet environment, the burden shifts from centralised controls to network controls. Then, further down the line, individual devices carry the burden for security.

4.2 Electronic mail

Consider access to electronic mail. On the Internet, mail can be stored in several host computers before it is forwarded to the addressee. In most Internet environments, there is no guarantee that private mail is not being intercepted and read by others. Although not generally known, anyone with technical expertise and the ability to use a back door to a system, exploit the UNIX architecture or access to a router, can intercept messages.

A more sophisticated threat is compromising the physical lines themselves. Coaxial cable, twisted pairs and fibre optic cable can be tapped physically. A network equipped with devices that measure reflectance characteristics can detect such intrusion; most organisations do not have this hardware.

The large commercial electronic mail systems build safeguards into their systems. A hacker examining SprintMail messages would be able to examine the 'wrapper' for the message but not the message itself. Employees of the large commercial mail services are aware of the trail that unauthorised access would leave. However, most Internet sites do not have the resources to implement stringent security measures.

Experts say that most violations of the privacy of electronic mail are a result of a user's lapses. Passwords are shared, or they are written on a slip of paper and taped to the computer monitor. Many users find they have several electronic mail accounts to manage. For convenience, a single password is used for all the systems. Hackers know that popular passwords are names of children, names of pets, even the user's own name or telephone number.' Furthermore, downsizing has led to more security exposures.

Other users leave the area while their workstation remains logged on to the network. Although system administrators initiate an automatic log-off after a period of inactivity, some power users implement a program that mimics keyboard input to avoid logging on and off the system.

5. Physical security techniques

One category of security techniques involves hardware or software 'devices' designed to screen out unwelcome users.

5. I Call backs

One common type of protection is the call-back or dial-back system. Under such a system, the computer keeps a list of authorised telephone numbers from which a legitimate call can be accepted. The user dials the remote computer and identification is made through passwords or account numbers. The remote computer then disconnects the caller and looks up that caller's telephone number in its internal tables. It then initiates a remote session with the caller's computer by calling back

[1] Judy Helm, 'Communications,' *PC World,* March 1994, page 240.

the approved site. Other security measures then take effect for logon and system-access privileges. UNIX solutions cost significantly more and require additional staff resources to install and maintain.

5.2 Challenge-response systems

A challenge-response system requires that the user provide a unique code generated by an electronic device. Password generators can cost anywhere from $50 to thousands of dollars. Security Dynamics (Cambridge, Massachusetts) manufactures a popular device called a use hand-held authenticator, where a user needs a different password each time to use it. A software solution called 'S/Key' that runs on a PC is available from Bell Communications Research. The Secur ID devices cost about $60 apiece.'

5.3 Kevlar smart card

A hardware-only family of security boards is manufactured by Isolation Systems (Ottawa, Ontario). A separate add-in board implements security independent of the host's central processing unit (CPU). All security parameters are stored in the board's permanent random access memory and are inaccessible to the user through the host CPU. Even after successful logon, the board controls ail disk accesses and provides security mediation and encryption. Some models also have the capability to accept smart-card readers.

The size of a credit card, the smart card contains an integrated silicon chip capable of intelligent interaction with the host computer system. Unlike an actual credit card which holds only a small amount of information (password, ID, account number) on a magnetic strip, the smart card can contain large amounts of information and can be programmed to give lengthy responses to computer interrogation. The combination of add-in boards and smart-card hardware may be suitable for applications where usage is metered; for example, the sale of documents. Selling and distributing cards becomes a distribution problem.

5.4 SmartDisk

New to the hardware security scene is the SmartDisk, a variant of the smart card, from SafeBoot. SmartDisk is a 3.5-inch floppy disk package that integrates smart-card technology. SmartDisk is inserted into the floppy drive as if it were a real diskette, but the read/write heads connect to the SmartDisk's circuitry, making them a kind of universal interface. Once inserted, the SmartDisk is used to encrypt the hard drive and protect it with a password.

The password and encryption keys are then stored in permanent memory on the SmartDisk. The disk then can be ejected and normal operations resumed. On the next boot up, the SmartDisk is inserted, logging the user on to the computer transparently. Without the SmartDisk, the computer is just so much metal and

[1] *Newsbytes,* 17 March 1994

plastic. The product is especially aimed at portable-computer users who are guaranteed that a stolen computer is rendered inert.'

NIST, the US standards setting agency, is working with the National Security Agency on integrating PC Cards into network access control processes. NSA's developers include Litronic Information Systems of Alexandria, Virginia. About 100 passwords can be pre-loaded on each card under this scheme. However, the cards have to be updated periodically. Internet hosts would run special software synchronised with the cards. Each card user who called a host would use the next available password. Hackers could not steal passwords by eavesdropping on the connections because each password would work only once.

Data transmitted during an Internet session would remain unprotected unless they were encrypted, but the data probably would be worthless unless the hacker knew what applications were involved. Future tests also might involve PC Card data encryption based on NSA proposals.*

5.5 Fire walls

The Internet link can be accomplished with a high degree of security. If a site wishes to provide *telnet* or *ftp* functionality, security can be strengthened by erecting a *firewall* between the internal (organisational) network and the Internet. In effect, Internet transactions are limited to one 'machine' at arm's length from the rest of the system.

The firewall is a highly secure computer that acts as a liaison between the Internet and the other computers within an organisation. This computer is often placed in a physically secure room. A firewall is a dedicated machine equipped with safeguards that acts as a single, easily defended Internet connection.

There is risk in linking a corporate network to the public world of the Internet. These so-called firewalls vet incoming messages and make sure that an outsider authorised to access a certain computer in the company does not roam anywhere else or leave software that records confidential information, such as people's passwords. At IBM, travelling employees are issued smart cards that identify them to the firewall. IBM tests the security system annually, challenging its own programmers to ferret out problems.[3]

However, firewalls .work in two directions. Outside access is limited. Access to such external services as the Internet are restricted as well. Further more, effective firewalls are costly. Anyone gaining access to the system must pass through up-front protection. Some network routers can be set up to pass only packets to

[1] Horace Labadie, 'Digital crime watch,' *Computer Shopper,* March 1994, page 594

[2] Shawn P. McCarthy, 'Feds eye PC cards as Internet security option,' *Government Computer* News, April 1994, page 1.

[3] Rick Tetzeli, 'The Internet and your business.' (Information Technology: Quarterly Report), *Fortune,* 7 March 1994, pages 86 and following.

designated TCP/IP servers. Similarly, only packets from specific networks will be passed to the server. The most effective firewalls use comprehensive user and service authentication. But the resources required to maintain such s&vices are not justifiable for many organisations.

6. Encryption

Encryption — a secret coding scheme — is one way to send information over a public network and protect the security of the message. Encryption is one of the more effective forms of messaging security. Intelligible data (sometimes referred to as *cleartext* or *plaintext)* appear in an unintelligible form (described as *ciphertext*). A random sequence of digital bits (the key) interacts with chunks of the original message or communication stream. The result is a message that cannot easily be decrypted.

Encryption depends upon a key; that is, a string of characters used to create the jumbled file. Encryption can be used to provide secure messages. Alternatively, customers can access encrypted information that can only be read with the digital key that unlocks or de-scrambles the information. Hardware encryption devices are also available. These are usually referred to as *dongles* and are commonly used to protect certain engineering and technical software from unauthorised use.

The more digits in the digital key, the longer the encryption process takes and the more secure it becomes. More iterations of the algorithm are completed. To recover the original message, the digital key is required. The processes of bit shifting and Boolean substitution are reversed.

There are several trends in the use of encryption to increase network security, one of which is encryption of the log-in scripts. These encryption routines are run locally on the user's machine; their purpose is to prevent an unauthorised person from copying the log-in scripts. Public and private key schemes are becoming increasingly important in a wide range of applications, and many electronic mail programs automatically encrypt their messages.

6. I Data encryption standards

The most widely used private key process is known as DES, Data Encryption Standard. The broad acceptance of DES is one of the reasons critics of the Clipper proposal believe that the encryption technology will diffuse rapidly through the computer and telecommunications industries. The process was developed by the US National Bureau of Standards, now the National Institute for Science and Technology (NIST)

The same string is used to encrypt and decrypt the password or message. The problem becomes providing the decryption key to the recipient of the message. Once the intruder knows the encryption key, all messages can be decrypted.

DES uses a 64-bit key with eight bits used for error correction. The remaining 56-bit key is used for the encryption and decryption, which yields 70 quadrillion keys. Because of advances in computing capability, there is concern that DES may have become less secure. Skipjack, the technology of the Clipper chip, is an 80-bit, dual-key algorithm developed by the National Security Agency (NSA).

Among the advantages of DES are:

- Quick processing on the sender's machine.
- Wide availability.
- Can be used to keep data on a network secure.

6.2 Public key encryption

In this approach, the sender of a message uses one key to encrypt the message; the recipient of the message uses a public key to decrypt the message. Knowing the encryption key will not allow the intruder to unlock the message. Public-key cryptography first became popular in the mid-1970s when Whitfield Diffie and Martin Hellman introduced a scheme that uses a published key to encrypt and a private key to decrypt a message. Anyone who knows a person's public key can send a message; only the person receiving the message can decrypt the message.

The public key approach relies upon providing the key to the recipient of the message. Thus, the security of the encrypted message is only as good as the method of transferring the key. Anyone with the key can decrypt the message.

Public key encryption is slow. The algorithm requires computing capability and extracts an overhead penalty from the server. Large numbers of short messages, or a few very long messages, place additional burdens on the system.

In 1977, Massachusetts Institute of Technology scientists (Rivest, Shamir and Adleman) proposea RSA. Their approachbffers several advantages over DES, notably breaking the limit for a 64-bit key. RSA keys can be any size. The pioneers of public key encryption are RSA Data Security Inc. (Redwood City, California). This firm provides its encryption products as shareware. The company also produces digital signature products.[1] Microsoft's server version of Windows will feature RSA database protection.

The RSA algorithms currently can also be found in an Internet-published program called PGP (Pretty Good Privacy). Philip Zimmermann, a Colorado-based software consultant, developed this public domain encryption program for electronic mail, using encryption techniques that are difficult to crack. PGP encoded fields are decoded with the same key that encrypts them.

[1] Digital signatures allow the sender to publish the public key. When a person wants to send a message that can only come from one sender, the sender encrypts the message with the public key. The recipient can read the message with the public key the user has provided. The message which includes the sender's name, a time and date stamp, could only have come from the particular sender. Using RSA's technology, nodes have a unique key that can be registered.

In 1991, PGP was made available as freeware. The software was copied by users to Internet sites throughout the world. Cryptographic software, however, is subject to export restrictions. Mr Zimmerman is the subject of a Federal grand jury investigation, the issue being that PGP code is a member of class of products that are not exported from the US to other countries. However, one of the questions in this suit will be, 'When software is downloaded by a user, is it 'exported'?'

It is possible to blend the public and private key encryption. For example, a message is first encrypted by public key encryption using DES, which is faster. The DES key is random, and can be enclosed with the encrypted message. The receiver must decrypt the DES key using the other half of the public key. The DES key is used to decrypt the document.'

Another public-encryption scheme is Privacy Enhanced Mail (PEM), a version of the public key encryption approach. PEM will encrypt a portion of the message using a public key and the majority of the message using a private key. The private key is a variation of DES. The Internet is exploring the use of node registration in order to provide valid digital signatures for encrypted messages. AT&T, Computer Associates International, and Novell have said they will support PEM.[2]

A shareware PEM product is TIS/PEM, published by Trusted Information Systems, (Glenwood, Maryland). The company also sells a commercial product, Trusted Mail.

6.3 Kerberos

An important development for UNIX systems is the Kerberos server. An independent, protected node grants specific rights to specific users for specific network resources. Kerberos moves messages between itself, the users and the server nodes in encrypted packets called *cookies.*

The Kerberos system eliminates the requirement for unencrypted, flat ASCII tex: passwords to be sent over the network. In this process, the secret key is never sent over the network. A version of the program is available without charge on the Internet or directly from Cygnus Support (Mountain View, California).

6.4 Application to electronic mail

The three major PC-based electronic mail systems — cc:Mail, Microsoft Mail and DaVinci e-mail — have encryption integrated into the software. The DaVinci product includes in-transit encryption as well as mail box encryption.

[1] This procedure makes sense to users who are familiar with the computer procedures required to handle these steps. For most users, the effort is not worth the trouble. When a single opening exists, security is effectively breached.

[2] Paul Strauss, 'Secure E-mail cheaply with software encryption,' *Datamation*, 1 December 1993, pages 48, 50.

Password protection of mailboxes on public mail services can be breached by repetitive dialling software scripts. In essence, the communication software calls the network, tries a number, and is rejected. A software routine increments the number, calls the network, and repeats the process until access is gained.

If encryption is passed from local area network to local area network directly, a third-party encryption product is required. The major providers of popular PC-based electronic mail programs do not give their software the functionality to read a competitor's encrypted files.

However, private encrypted electronic mail can be retained when passed over AT&T's EasyLink, MCI Communications' MCI Mail, and Sprint's SprintMail. But sender and receiver must use the same encryption technique. None of these services has integrated encryption into its services.

7. Copyright

Copyright can also be considered a *security* issue.In essence, business professionals will not engage in transactions unless [I] they can be certain they will be paid, [2] the information product and service does not fall into the hands of those who did not pay for that access, and [3] owners can control unauthorised re-use of the information. The traditional protection afforded publishers of information products has been copyright law. Much of the law dates from the late 19th century and traditionally lags behind practices and technology.

In the past, copyright provided a measure of protection for different uses of the same information, usually in different media. Today, copyright is struggling with digitisation and dissemination on a global scale in fractions of a second. The information — represented by 1s and 0s — can be sliced and diced into different products, configurations and media.

There is, within the exploding world of electronic information and the Internet environment, no agreed upon mechanism for protecting intellectual property. The environment is diverse, changing rapidly, and becoming increasingly fractious. What 'meaning' copyright has is inherent in the law itself. But law is particular, and the Internet is general and not bound by time, space or central authority.

Although almost a truism, it is important to recognise that electronic information poses a number of quite difficult issues to those who make and sell information. Most organisations know that they are not allowed to make multiple photocopies of newsletters, magazine and journal articles and sections of books. The increased use of optical character recognition and imaging tools raises the threat of distribution of copyrighted information in electronic form. But what about copies of articles attached to an electronic mail message and sent to hundreds of people on a LISTSERV?

Even though the technology is different, the copyright laws remain in effect. Phillips Business Information Inc. (Potomac, Maryland) brought suit against Atlas Telecom (Portland, Oregon). The software company paid a $100,006 settlement.'

The Wall Street Journal reports, "For a business, entering a newsletter into electronic mail or a database saves labour, time, money and paper. But for publishers, it's a disturbingly hard-to-track method of copyright infringement. Companies that want to make limitless copies may do so legally only by buying a licence, which usually costs thousands of dollars."

The information superhighway is envisioned as an open platform. In the words of Mitchell Kapor (Chairman, Electronic Frontier Foundation) and Jerry Berman (Executive Director, Electronic Frontier Foundation): "Every person would have access to the entire superhighway, so programmers could distribute information directly to consumers. Open platform services will spur diversity in the electronic media, just as low production and distribution costs make possible a wide variety of newspapers and magazines."*

As more individuals and organisations connect, more information will be generated. The misunderstandings and misuse of intellectual property will increase.

A fine line divides fair use and online theft in an electronic environment. The law of intellectual property is not simple, nor is there consensus on how to manage intellectual property in an Internet-like environment.

7. *I A test case*

A person or organisation may assume that information is property when it is not. In the 1991 case of US v. *Riggs,* two individuals were prosecuted for wire fraud, interstate transportation of stolen property and computer fraud.[3]

Only the computer fraud statute (18 United States Civil Code 1030) addressed computer issues. The case pivoted around Robert Riggs, a computer enthusiast who gained access to a computer system operated by Bell South, a Regional Bell Operating Company. No password was required. Mr Riggs copied a file about emergency telephone procedures and deleted a statement from the document and forwarded it to Craig Neidorf, a college student best known for the electronic publication ***Phrack***.[4] Charges were dropped. The *Internet World* article says:

[1] Junda Woo, 'Electronic copying may bring lawsuits,' The *Wall Street Journal,* 6 October 1993, page B4.

[2] Mitchell Kapor and Jerry Berman, 'A superhighway through the wasteland?' The New York *Times,* 24 November 1993, page A15.

[3] A more detailed discussion of this case appears in Mike Godwin's 'When copying isn't theft: how the government stumbled in a 'hacker' case,' *Internet World,* January-February 1994, pages 80 and following.

[4] This publication contains information about hacking into computer systems. It is widely available on bulletin boards.

"Under the First Amendment, the presumption is that information is free, and that it can readily be published and re-published. For this reason, information 'becomes property' only if it passes certain legal tests. This means that law enforcement cannot simply assume that whenever information has been copied from a private computer system, a theft has taken place."' In this case, the prosecutor could not establish that the information in the document met legal tests to be established as a property interest.

Information can be property interest under patent law and copyright law. Patent law did not apply in this case. Copyrights qualify as property interests in certain situations. A copyright cannot be willed to a survivor as personal property. In the US, interstate transportation of stolen property statues does not extend to copyrighted material.*

In short, copying of computerised information can be theft only if information can be demonstrated to be property or if it meets some other view of information as property, such as trade secret law or breach of confidence.

Neither of these approaches applied in the *Riggs* case. The emergency information was not a trade secret because there are no competitors in a monopoly situation. In the case of emergency information, if competitors did exist, they would know the emergency information. Bell South argued that the information in the document was worth $80,000; Mr Neidorf's attorney pointed out that the information was available from another Regional Bell Operating Company and from Bell Communications Research (the research and marketing arm of the seven RBOCs).

The Riggs case illustrates that it is not easy to establish "elements of a theft crime when the 'property' in question is information."[3]

7.2 Alternatives for publishers

An increasing number of publishers are starting up their own online systems and dealing directly with paying customers. Ziff Communications and Engineering Information are two examples of trying to protect copyright by becoming gatekeepers. Other ways in which publishers address copyright are:

- *Contracts.* The confidentiality of contracts can pose problems. They may be difficult to apply in the Internet environment. In America, the National Writers' Union has supported two members' suit against the New York Times, Mead Data Central and UMI for reproducing the writers' work in electronic form without the permission of and additional payments to the authors. The authors claim they granted just one-time print rights.

[1] *Internet World,* January-February 1994, page 82.

[2] See 47 US 207 Dowling v. United States (1985). The case involves transportation of pirated recordings of Elvis Presley. Copies do not meet the tests of physical identity.

[3] *Internet World,* January-February 1994, page 85.

- *Licences*. A collective licence allows an industry or group to make an unlimited number of copies for a fee; permissions licensing grants an individual or organisation specific permission to make a specific number of copies.

The problem is that it is difficult to police unauthorised copying or sharing of digitised information. When the violator is a customer, the delicate task of managing the relationship looms.

Trade secrets are difficult to enforce in a public arena such as the Internet unless someone who can be identified posts information that can be shown to be a trade secret.

8. Software piracy

Software suppliers are losing millions of dollars through a new method of piracy which uses major computer sites to store and distribute illegally-copied packages. 'The Internet effectively allows pirates to send out illegal software without fear of detection by exploiting anonymous access to the worldwide network. Now suppliers are calling for the monitoring of software which is sent across international networks such as Internet.

David Worlock, President of the Brussels-based European Information Industry Association which represents 130 service suppliers, claimed recently that trials are taking place in Europe on tagging and identifying documents sent on international networks.

"Within the Internet we are appalled by instances of people taking a piece of software, illegally hiding it in the file architecture of a computer system attached to the Internet, and then advertising the ability to go into the innocent computer and extract the pirated material" said Mr Worlock.

Sites known to have been attacked by pirates are in academia, but increasingly corporate users of the Internet are also targets. The aim is to gain access to commercial software and make it available to others on the network without charge. One of the rallying cries of certain Internet users is, 'Information wants to be free."

Most sites targeted by intruders have no idea their systems are being used to store and distribute pirated software. The prestigious Massachusetts Institute of Technology discovered that its Internet server held thousands of dollars worth of commercial software free for the taking. Worldwide losses are put at $11.8 billion per year. The Software Publishers Association claims that American business software piracy cost publishers about $1.6 billion in 1993.[2]

[1] Tony Collins, 'Software pirates exploit Internet's slack security'. *Computer Weekly,* 13 January 1994, page 1.

[2] Peter H. Lewis, 'Student accused of running network for pirated software', *The New York Times, 9* April 1994, pages 1 and 9.

In the past, pirates have used bulletin boards to exchange pirated software. But bulletin board operators have clamped down on piracy by restricting access to registered users only. Criminals are now switching their attention to the Internet which remains an open, worldwide network for research, academic and corporate users. By exploiting the anonymous File Transfer Protocol (*ftp*) in the Internet, pirates seek to avoid detection. Certain servers strip identification text making it difficult to know the identity of the person taking software.

9. A snapshot of Internet hacker tricks

There are a great many techniques that determined hackers can use to obtain access and information from Internet sites. The most obvious approach is to use the Internet server itself as a clearing house for pirated information, most often commercial software. However, as Internet use grows, a similar technique can be used to provide unauthorised users with commercial information of value, not just popular programs.

David LaMacchia, a student at the Massachusetts Institute of Technology, created a partition on the MIT Internet server, asked friends to place commercial software programs on the server, and then limited access to the hidden partition by providing details of the log-on procedure to selected individuals. To protect the identity of the users of the hidden partition, Mr LaMacchia and others routed their use of the partition through Internet sites that strip user identification details as part of the normal message storing and forwarding process. In effect, anonymous users were able to access the partition, copy commercial programs such as WordPerfect and Excel, and log off without revealing their identities or usable audit trails in the MIT usage logs.

Within the Internet environment, security becomes the responsibility of each node. Despite the range of technology available to network managers, security boils down to granting or withholding access privileges to users on each of the connected nodes.

In a basic open UNIX system, the file containing account names and passwords can be read by any logged in user. The passwords are encrypted, but once an intruder has a copy of the file, passwords can be discovered.

UNIX file security is rudimentary in nature, though. It offers conventional read, write and execute access permissions which are stored, along with other parameters, in a data structure called an Information Node. Manipulate the latter and information integrity can be comprised. System administrators must carefully analyse all changes to the Information Node.’

[1] Jerry Cashin, ‘Open, distributed users tightening UNIX security,’ *Software Magazine,* January 1994, page 8 1 and following.

There are a number of common Internet hacker tricks. The simplest is to log on to a node and test passwords such as the word *password* and common names such as *fred* or *john.*

A more skilled hacker will place sniffer programs within a server and locate or capture passwords. These programs can be difficult to locate. The sniffer programs are often used in conjunction with hidden files which contain the sniffer programs. The files often have non-standard names; for example ..___ (dot dot space space space) or ..^G (dot dot control G). Intruders often name a sniffer file with an innocuous or common UNIX command. Key files such as *ftp* and *telnet* have been used to host Trojan horses.’ One way to check for these programs is to make sure that search paths do not specify unusual sub-directories. The offending sub-directory is often inserted at the beginning of the path.

Intruders with knowledge of UNIX often assign themselves system privileges. In effect, they become a system administrator for the site. Privileged accounts can be located via the UNIX *find* command to search the root partition for any file that sets *XXXuid* to the root user. Intruders use the *chron* and *at* files to insert their own programs into a system. Files referenced in these two files should not be word-writeable. Intruders can gain access to the system even after they have been discovered and blocked from it; evidence of intrusion in the.form of unusual entries sometimes appears in accounting, syslog and security logs, but the more accomplished hackers will delete entries that leave evidence of their use of the system. Standard security measures include routine checking of *the/etc./password* file that allows the administrator to verify that account changes are authorised, since accounts without passwords are often an indication of an intruder.

9.1 Basic precautions

UNIX system administrators can disable the /dev/nit, but all operators are best advised to avoid using reusable passwords that are transmitted in plain text. It is also important for non-technical staff to recognise that passwords are virtually useless when used alone since they can easily be stolen, discovered or merely guessed. If plain text passwords are used, they should be compound; for example, *happy-people.*

To help circumvent password discovery, the password’s active life should be limited. Passwords should be changed frequently, but not so frequently that users become confused. On networks, Access Control Lists should be used based on one password instead of adding passwords to increase user access. Too many passwords increase, not reduce, the risk of intrusion.

Audit trails can be useful unless the hacker makes use of the anonymous forwarding sites which strip user identifications. Audits should show all attempts to log on to

[1] These are programs that look like one type of program but have other functions

the system, whether they were successful or not, and, if possible, what files were used or changed.

Gateway activity logging should be enabled, since these logs should be able to keep track of all inbound and outbound traffic. To preserve the privacy of the messages, the logs should contain information on whom the message was sent to and from, information about any attachments and the time/date of the transmission.

Programs or devices which use regularised prompts or error messages can alert the knowledgeable hacker. Off-the-shelf products as they are installed out of the box should therefore never be run, but default passwords and network messages should be altered immediately whenever possible.

Prompts that indicate the form of the expected reply — for example, *User Name* or *User Account* — make the hacker's job much easier. The inclusion of company names and other predictable data in messages, prompts or menus can provide hackers with specific data on which to base their searches for more compromising information, such as company address, so they can search through your dustbin for discarded printouts.

One may wish to verify that backdoors and loopholes have been closed. A ***backdoor*** is an entry point into a program put there for debugging or other development purposes. The door can be opened usually by an unusual keystroke series (one unlikely to occur during normal operation) or a small, innocuous-looking program. Such entry points permit invasion with all protections disabled. In general, backdoor ports are sealed once the programming job is completed. Check for known backdoors in network products destined for an Internet application.

Determine if a person with a copy of the security software can gain access to a system by setting up as a new SuperUser or system administrator from a dial-up connection. If reinstallation of the Administration program is permitted, a new SuperUser account should not be retroactive. Files protected by prior users must remain protected.

A little-known precaution is to keep security inconspicuous. The more visible the security procedures, the more likely the system will come under attack. High-profile security measures such as those the telephone companies maintain, attract hackers who view them as a challenge. The more visible the security, the stronger the signal about the value of the information in the protected system.

Despite every technical precaution, users need information about the issues surrounding gateway access. Seeking their guidance in establishing any policies about the unauthorised use of electronic mail and other Internet services can be useful. However, no security system is impervious or totally secure.' Certain information

[1] Paul Merenbloom, 'The E-mail dilemma: managing your gateways to the world,' *InfoWorld, 28* February 1994, page 54.

systems and network managers often will not make the changes necessary to provide their workers with secure systems.

10. Outlook 2000

Regrettably, there does not appear to be a short-term solution to many of the difficult security issues associated with the Internet. A combination of tiered information services may be one practical solution: free or low-cost information would be available at Internet sites, acting as magnets, with interested Internet users being able to examine the free and low-cost information. Higher-value information would be available directly from the information suppliers, presumably via facsimile or some other secure means of transmission. Payment can be arranged by credit card or some mechanism acceptable to both parties using a financial utility service such as CommerceNet.