A Review of Information Security Principles

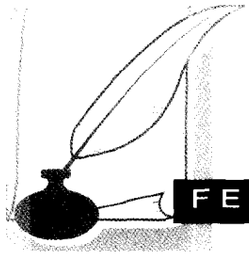
Ms Sharman Lichtenstein

Information security principles underpin the achievement of quality in information security for an organization. Security analysts will be in a better position to develop or evaluate information security by consulting a complete, cohesive and integrated set of all existing information security principles. This article presents and describes seventy-three information security principles, highlighting their evolution from the domains of physical security, accounting, operating system security and computer security.

Introduction

Information security principles guide the selection, design and evaluation of information security controls. These principles evolved from physical security principles, accounting principles, operating system security principles and computer security principles. For example, Gaines and Shapiro (1978) first suggested that physical security principles such as barriers and guards were also applicable to information security. Two well-known sets of information security principles are those of Parker (1984) and Wood (1990). These sets share a number of principles (for example, the principle of least privilege, which evolved from the 'need to know' concept originally developed for military establishments). However, there are principles in Wood's and Parker's sets that are not shared. This problem is frequently experienced in other sets - the sets contain only limited selections of existing principles. Furthermore, principles are often listed under different principle names or vary in definition, between sets. For example, Saltzer and Schroeder (1975) described the principle of work factor corresponding to only one perspective of the cost-effectiveness principle of Wood (1990). This can be confusing for security analysts consulting sets of principles for guidance in controls selection, design or evaluation, and confusing for researchers studying information security principles. Hence, a single, comprehensive and integrated set of information security principles is required for effective information security practice as well as for the consolidation of the theory of information security principles.

Principles may be interrelated - for example, controls which are cost-effective



often satisfy the simplicity principle. Principles may appear to conflict - for example, the principles of human involvement and minimum reliance on real time human intervention. Such relationships are potentially useful in information security development or evaluation, however it is a complex task at present to define these relationships while there exist so many disparate and unintegrated sets of principles - to enable these perceptions, it is first necessary to integrate all existing sets of principles, then study the integrated set.

It has been suggested that information security requirements for modern, adaptive organizations differ from those for traditional organizations (Baskerville 1992). For example, flexible, interpretable and human-reliant information security is required, rather than rigid, technological controls which inhibit spontaneity and flexibility. Baskerville was concerned that traditionally selected controls for such organizations may be inappropriate. Lichtenstein (1996) continued this line of thought, proposing a new set of information security principles in order to satisfy the information security needs of adaptive organizations, based on an evaluation of Wood's (1990) twenty-three information security principles. Rather than an evaluation of merely Wood's principles, it would be preferable to evaluate an integrated, complete set of existing principles.

The above discussion has introduced five rationale for compiling and reviewing an integrated and complete set of existing information security principles:

- an understanding of the evolution of each principle is required for validation of the use of the principle in the information security domain;
- for use by researchers in information security when compiling new sets of principles;
- for use by practitioners in the selection, design and evaluation of controls;
- as a basis for developing a model of the relationships between information security principles;
- in order to determine appropriate information security principles for adaptive organizations.

This article presents and reviews seventy-three information security principles, and describes their evolution.

Information Security Principles

The determination of all previously proposed information security principles is a sizeable and complex undertaking. Furthermore, the evolutionary path for each information security principle is often lengthy, complicated and tricky to uncover. Reasons for these difficulties include the following: Some principles were merely alluded to rather than directly specified as principles. Other principles appear under the nom de plumes of concepts, practices, notions, issues, aspects, policies, or definitions. Some authors have labelled control types as principles, for example Cole (1978) believed authentication to be a principle, however technically, it should be labelled a control type.

There can also be confusion in assessing whether a particular principle was intended by the author for the domain of information security, computer security, or operating system security. One source of this confusion is that the term 'information security' is often used interchangeably with 'computer security'. Baskerville (1988) defines 'computer security' as purely the protection of electronic computer and communication systems, i.e. a concern with the security of technology. He defines 'information security' as a broader range of issues, including computer security, systems analysis and design methods, manual information systems, managerial information security issues (for example security policies) and societal and ethical issues. This particular definition for information security is adopted in this paper.

Definitions of several terms which assist readibility follow:

- Subjects are people or information resources constrained by controls.
- Objects are information resources being protected.
- Controllers are people who cause controls to operate effectively.
- Perpetrators (violators) are people who deliberately attempt to compromise controls.

The principles are presented in groups of related principles which facilitate reader comprehension.

Multidisciplinary

Information security measures must account for a variety of perspectives, including technical, administrative, organisational, operational, commercial, educational and legal (OECD, 1995). Lichtenstein (1998) and others support this "holistic" approach to information security.

Proportionality

The OECD (1995) consider that information security measures should be mounted in accordance with the possible risks (see risk reduction).

Integration

Information security measures should be co-ordinated and integrated in order to create a coherent overall security system (OECD, 1995).

Timeliness

Relevant parties should act in a timely and co-ordinated fashion to information security threats and breaches (OECD, 1995).

Reassessment

Information security must be reassessed periodically to cater for changing information security requirements (OECD, 1995).

Democracy

Information security must permit the legitimate use and flow of data as befits a democratic society (OECD, 1995).

Barrier (Access Control)

Gaines and Shapiro (1978) discussed the concept of a barrier between a subject and an object. A barrier is a facility or hurdle which must be overcome in order for a subject to gain access to an object, and is thus the forerunner of the access control principle (Caelli et al. 1989). Controls based on the barrier principle can be physical (for example, badges) or logical (for example, passwords), and possess two properties: they attempt to prevent direct compromises, and are passive. Gigliotti (1984) noted that barriers have been employed by humans throughout history for physical security, and argued that barriers may be used for retentive purposes as well as exclusion purposes, for example physical barriers may prevent easy extraction of computing equipment by thieves. Cole (1978) discussed the corresponding principle, controlled access, with respect to network resources. Wood (1990) believed that a strong approach to access controls could be achieved via the principle of complete mediation (Saltzer 1974, Saltzer and Schroeder 1975, Berman 1983), which involves checking each access request from a subject to an object, for current authority (called authorization (Fisher 1984)).

Permission-Based

Saltzer and Schroeder (1975) and Pfleeger (1989) recommended permission-based access control, where a requested access should only be granted after checking that it has been specifically permitted (rather than the access being granted unless it has been explicitly denied).

Controlled Usage

Cole (1978) supported the concept of controlling the usage of network resources, in order to prevent possible disasters.

Continuous Protection

Cole (1978) and Pfleeger (1989) indicated the need for controlled access to the use

and modification of the controls themselves.

Guard

A human guard represents a mechanism for detection, apprehension, surveillance, instrumentation, and counterforce (Gaines and Shapiro 1978). The surveillance employed by the guard is active, rather than passive, observation.

Detection

A violator may be detected in his/her activities (Gaines and Shapiro 1978), via surveillance, alarms, accounting procedures or auditing mechanisms. The consequences of detection must be significant, for example apprehension of the violator.

Identification of Violator

Gaines and Shapiro (1978) signalled the need for controls which identify a violator in the event of detection.

Apprehension

Gaines and Shapiro (1978) considered apprehension of a violator as a possible consequence of detection.

Counterforce

Gaines and Shapiro (1978) described the use of counterforce by a guard, in order to 'actively resist a violator'.

Cost-Effectiveness

Saltzer and Schroeder (1975) and Gaines and Shapiro (1978) described the principle of work factor (the quantitative cost of compromising a control, considered from the perpetrator's point of view). Parker (1976) proposed the principle of cost and degradation of performance. Wood's (1990) principle of cost-effectiveness is based on these two principles.

Both Wood (1990) and Gigliotti (1984) described the owner-of-the-information view of cost-effectiveness : the reduction in expected asset loss value should be greater than a control's cost. However, expected asset loss value is not always able to be established precisely. Thus, as a constraint on control selection, the cost of a control to be selected should be less than the value of the asset being protected. For example, one should not spend $15000 per year to protect a database with a value of only $3000 in the free market. Parker (1976) believed that quantitative risk analysis should be used to determine the likely financial loss due to threats. The total cost of a planned control (including cost of selection, acquisition, development and implementation of control, environment modification, reduced productivity of work and replacement of work) then needs to be calculated. The focus is on the control reducing, rather than covering, asset-loss costs. Cost-effectiveness of the control is measured in long-term benefits, as performance may be increased and subsequently productivity, in turn leading to reduced error-rates. Increased productivity and reduced error-rates contribute to reduced costs.

Wood (1990), Gaines and Shapiro (1978), Saltzer and Schroeder (1975) and Gigliotti (1984) described the cost-to-the-perpetrator view of cost-effectiveness: the worth of a compromise to the perpetrator (for example, the value of the information gained, if sold) should be less than the cost of the compromise (for example, the risk of getting caught) to the perpetrator. However, Wood argued that perpetrators often act irrationally, and therefore this view should only be used as a check on the owner-of-the-information view. He further suggested that the cost-to-the-perpetrator view may unfortunately take the focus off the owner-of-the-information view (which he believed was the correct perspective).

Simplicity

This principle was originally proposed as economy of mechanism by Saltzer (1974),

for controlling the sharing of information in the Multics operating system. Saltzer and Schroeder (1975) extended this to cover hardware and software protection mechanisms. Farr et al. (1974), Lane (1985), Pfleeger (1989), Berman (1983) and Parker (1976, 1981, 1984) all recommended simple controls, incorporating the notions of smallness, and straightforwardness. Wood (1990) explained that less effort would be required to design, implement and operate simple controls, with a side-benefit being that the controls would probably also be cost- effective. Simple controls are easily understood and easily tested. Thus errors created in design and implementation are more likely to be detected and corrected. Simple controls are also less likely to depend on people for their proper functioning, and because they are well-understood by users, tend to gain user support and are thus unlikely to be avoided. This principle also supports the concept of a simple human interface, so that users may easily and automatically apply controls. An example of a simple control is the password.

Override

Farr et al. (1974) first proposed the principle of fail-safe, incorporating the override principle. Parker (1981, 1984) proposed the principle of override and failsafe default, incorporating the override principle. Wood (1990) discussed override on its own. Others to discuss this principle were Hamilton (1972) and Martin (1973). A control should provide the capability for persons with due authority to stop or interfere with its operation in the event of the control's failure, or in other circumstances which would necessitate control shutdown or interference. Controls should only be subject to override under such special circumstances. For example, in the event of a fire, access controls must be able to be overridden for safety reasons, as well as to enable rebuilding of the system. Without override, a control may be perceived as inflexible.

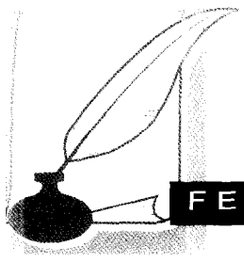
Overt Design and Operation

The principle of open design was proposed by Saltzer (1974), Saltzer and Schroeder (1974), and Pfleeger (1989), and discussed as non-secret design by Lane (1985), as absence of reliance on design secrecy by Parker (1976), absence of design secrecy by Parker (1981, 1984), and as overt design and operation by Wood (1990). The principle states that controls should be open, evident and public rather than concealed. Secrecy should reside in only a few key items which vary, for example in the passwords listed in a password table. Farr et al. (1974) stated that 'security should not rely on secret techniques'.

Parker (1984) suggested that controls should be designed with the assumption that potential attackers know as much about them as the controls' designer, although he emphasised that this does not imply that controls should be exposed without reason. Wood (1990) reinforced this by recommending against overreliance on a control's design and operation for security strength. He suggested that the concealment of controls may result in incompetence, laziness and illegality, as it may provide opportunities for authorised persons to engage in illegal yet undetectable activities.

Parker further added that secrecy may not be a strong approach to securing systems, as the strength of a control relies primarily on its design and suitable operation, in particular its complexity, plus the effort required to compromise it, and to a lesser extent on its concealment.

Baran (1964), Peters (1967), Weissman (1969), Cole (1978) and Gigliotti (1984) all recommended overt design and operation of controls. One example of the principle in practice is the publication of the data encryption standard DES, prior to its usage. This gave the public greater confidence in the DES algorithm as a control mechanism. They realised that the security associated with its use did not depend on the resistance of the algorithm to possible



cracking attempts, as the algorithm had been published.

Parameterization

Baran (1964) stated that since the existence and nature of many controls is public knowledge (through overt design and operation), security resides with a control's keys or parameters rather than with its secrecy. Wood (1990) also believed that variable, rather than constant, controls should be designed, for two purposes. The first purpose is to enable greater control effectiveness through the crime discouragement value associated with the uncertainty in a potential attacker's mind as to parameter values. For example, if the lower limit amount above which credit card purchases need to be authorised, constantly changes, criminals who may consider using a stolen credit card may be discouraged by the uncertainty as to the lower limit value, although they may be well aware that a lower limit exists, and well aware of the credit card authorization procedures. If they knew the value of a fixed lower limit, however, they would ensure that they only ever purchase goods to a value lower than this when using the card. The second purpose of variable controls is the usefulness of parameterization in today's changing business environment, where reconfiguration of controls to cope with changes is often required.

Entrapment

The entrapment principle derives from traditional criminal detection techniques, for example law-enforcers enticing a criminal into a preset trap in order to gain evidence for a crime. Entrapment in information security entails a perpetrator walking into a preset trap (Parker 1981, 1984, Wood 1990) and is useful to obtain information about unknown penetrators who have already gained access to an organization's system, and to collect evidence for prosecution. The principle is based on making designated vulnerabilities in the system attractive to the suspected attacker, who would therefore be more likely to attack those vulnerabilities and could then more easily be detected and stopped.

Parker (1984) drew attention to the deficiencies of entrapment. Firstly, there is the assumption that perpetrators act rationally and have considered many of the vulnerabilities they may attack, and that they have the skills and knowledge to do so. Secondly, entrapment may be an irresponsible security strategy, since it provides individuals with a tempting opportunity to engage in illegal activities. Wood (1990) further warned of the legal and ethical issues to be considered, as such controls may in some cases violate either the law, company regulations or ethical standards, and may even expose management to civil suits.

Independence of Control and Subject

This principle states that the people constrained by a control (the subjects) should be independent of the developers of the control (the controllers), so that the people constrained are not responsible for assuring the effectiveness of the control (Gaines and Shapiro 1978, Parker 1981, 1984, Wood 1990). Subjects should be monitored via other controls. For example, a programmer who is to be solely controlled by an access control program should not have been involved in the design, coding or testing of that program. Wood referred to this principle as a variation on separation of duties, with the focus on whom is being controlled by which security measures. Fisher (1984) referred to the accounting principle individual cannot both originate and approve transactions. Brock et al. (1986) also referred to its origins in accounting security, stating that the people who are responsible for information should not be the same as the people who record it. The difficulty in achieving the separation required for independence of control and subject has been noted by many authors.

Separation of Privilege

Saltzer and Schroeder (1975) and Lane (1985) specified that access to information should depend on more than one condition or control. They believed that protection mechanisms which consist of more than one control are more flexible. If this principle is applied (Pfleeger 1989), the compromise of any single control would be insufficient to gain access, an example being the use of authentication plus a cryptographic key to gain access to information. This principle is strongly related to defensive depth.

Split Knowlege

Farr et al. (1974) discussed the principle of split knowledge, a principle originating in accountancy. Two or more people possess literal or metaphorical keys, which gain access to high security functions in combination only.

Avoid Single Control

This principle is a well-known accounting principle (Brock et al. 1986). At least two people are required to control high security operations (Farr et al. 1974). Jackson and Hruska (1992) referred to a similar principle, dual control, which states that high security functions should be performed by two controls or individuals: one for checking that the function itself is carried out, and the other to make sure that no mistakes or illicit acts are carried out.

Division of Knowledge

This principle states that no single person should possess sole complete knowledge of a system. Instead, knowledge about a system should be divided amongst a group of people (Lane 1985). Martin (1973) pointed out that a greater degree of planning and conspiracy is then necessary to compromise the system, thereby increasing the risk of detection in the process. Fisher (1984) adds that a piece of information on its own may be useless unless combined with other information.

Minimise Personnel Interaction

Jobs should be organised to avoid contact between people in different jobs, in order to minimise opportunities for unauthorised access to information. For example, programmers should ideally not enter the computer room. This principle helps to enforce the access control principle.

Minimise What People See

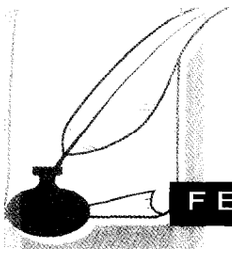
Farr et al. (1974) suggested that waste, input, output, labels, and other tempting information should not be left lying about, exposed, for unauthorised people to peruse. This principle can be combined with that of least privilege.

Segregation of Duties

Lane (1985) described division of duties and responsibilities, which originates from accounting principles (Brock et al. 1984). Parker (1984), Fisher (1984) and Baran (1964) defined segregation of duties as the distribution of the duties or activities which are required for a process amongst several people. Segregation of duties is an extension of the avoid single control principle. Errors in processing are reduced, and further, a person would not be able to compromise a control without collaboration (and the associated increased likelihood of detection).

Rotation of Duties

Lane (1985) called this job rotation. Jackson and Hruska (1992) also discussed rotation of duties, suggesting that in order for over-familiarity, laziness or conspiracy against the organization not to set in, resulting in accidental or deliberate breaches, employees should be shifted



from one duty to another at random intervals.

Universal Application

A strong control is applicable across all environments, people, equipment and applications (Parker 1981, 1984, Wood 1990). Parker confirmed that if rules are not followed, the result is often failure of the control. If exceptions are absolutely necessary, they should be minimised and clearly defined. An example of universal application is the use of badges in an organization. If senior management are not obliged to wear badges when entering the computer room, then a person may gain access simply by removing their badge. On the other hand, if everyone in the company must display a colour-coded badge, it would not be as simple for an unauthorised person to gain access.

Hostile Environment

Controls should be designed for a non-trusting environment by assuming the worst user intentions (Parker 1976, Caelli 1987, Wood 1990). Lane (1985) argued that even though in most cases employees within a company are reliable and trustworthy, an organization should take steps to protect its assets and information against employees with ill intent. Wood (1990) cautioned that a designer should not rely on the ethics of the user to compensate for the lack of a control.

Minimum Reliance in Real-Time Human Intervention

Manual or human intervention weakens the functioning of a control, and a control that requires no human intervention for its operation is considered to be superior and should be chosen in preference (Parker 1981, 1984). Manual functions are considered to be the weakest in a control's operation, and they must be examined not only during a control's operation, but also when controls are violated or attacked and need to be repaired. For example, rather than have a security guard posted at a door, an automated door employing an algorithm is preferred. This principle contradicts Wood's (1990) principle of human involvement.

Reaction and Recovery

Controls can be reviewed in relation to the way that they behave when activated (Parker 1984). When the deliberate compromise of a control occurs, the consequences may be instant evidence of the violation, identification of the perpetrator, or cause the start of a search for the perpetrator (Gaines and Shapiro 1978). Parker (1984) was concerned that controls may be designed to destroy the asset being protected and also deny the attacker access to it, which may result in recovery being complex and prolonged. Jackson and Hruska (1992) discussed recoverability, which requires the system to recover with acceptable speed to an acceptable state, and which required security to be restored to an acceptable state, after an attack. The duration and appropriateness of a control's response should be assessed, as by giving inappropriate responses a control could reveal valuable information that could be of use to the violator. For example, where a user identifier plus a password are required to authenticate a user, if an incorrect user identifier is entered, the password should still be accepted and tested, to avoid disclosing the fact that the user identifier was invalid (Parker 1984).

Residuals and Reset

Parker (1981, 1984) believed that the residual conditions after a control has been activated, as well as the overall situation and requirements for resetting the control, should be assessed. This principle has overlap with the principle of reaction and recovery. The desired result is that the asset being protected will be as secure

after the control has performed its function as it was beforehand. For example, where a control has caused irregular halting of a report print, residuals of the partially-printed reports may be discovered and collected by unauthorised people. Fisher (1984) also discussed residuals.

Manufacturer, Supplier and Servicer Trustworthiness

Parker (1981, 1984) argued that in order to determine whether a control is trustworthy, it is necessary to prove its reliability, integrity, sustainability and adherence to specifications. Often, the determination of these is infeasible, in which case trust must be placed in the manufacturer, supplier, and maintenance service organizations and personnel. For example, if a computer package is acquired, trust must be placed in the software manufacturer of the software, the suppliers (for a reliable delivery), and possibly also in the supplier's maintenance support staff. It is usually difficult to assess the trustworthiness of external organizations and their personnel. Parker (1984) considered that the period of time that a particular management has been in charge is a better guideline than the length of time that a company has been in operation whilst maintaining a good reputation. However, he recognised that the most important factor remains the trustworthiness of the relevant individuals within the external organizations.

Least Privilege (Need to Know)

This principle was originally devised for the military as 'need to know' (Pfleeger 1989, Saltzer 1974, Saltzer and Schroeder 1975, Weissman 1969), and has been widely followed for many years (Parker 1984). It involves providing the least amount of information necessary to a person, which would allow that person to perform their tasks effectively. The principle has been discussed by many other authors including Cole (1978), Fisher (1984), Parker (1976, 1981, 1984), Baran (1964), Caelli et al. (1989, 1991), Hamilton (1972), Jackson and Hruska (1992), Lane (1985), Wood (1990). Farr et al. (1974) referred to the principle of minimise personnel knowledge.

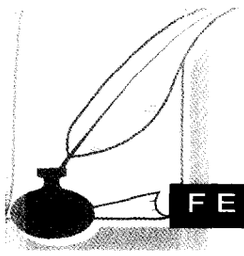
The purpose of least privilege is to reduce the number of unauthorised functions, accesses and resultant errors (Saltzer 1974). Jackson and Hruska (1992) argued that the position or status of a person within an organization should not in any way influence their access privileges. If an individual does not prove their need for access, they must not be granted it due to job title. The principle must be enforced in accordance with the sensitivity and value of the information.

Assurance

Cole (1978) and Pfleeger (1989) described the concepts of adequacy of security, and confidence in integrity, of controls. Assurance incorporates the notions of auditability, reliability, accreditation and self-checking. Jackson and Hruska (1992) and Caelli et al. (1991) also discussed assurance.

Auditability

This principle requires the generation of evidence by controls in order to assure that they are operating as expected (Fisher 1984, Parker 1976, 1981, 1984, Pfleeger 1989, Wood 1990). Controls must be examinable by an auditor in order to guarantee that it is functioning correctly and according to specification. Wood (1990) suggested evidence such as logs, audit trails, reports, and flashing lights. Gigliotti (1984) pointed out that the auditability features of a control may actually protect assets. For example, if warning lights are activated when a control is attacked, the violator will probably cease the attack, in order to avoid apprehension.



Instrumentation

Wood (1990), Parker (1976, 1981, 1984), Caelli et al. (1989), Gaines and Shapiro (1978), Fisher (1984), Berman (1983) and Martin (1973), discussed instrumentation, which is the provision of feedback by a control at the moment it fails or is being attacked, in such a way as to alert the people responsible for the control immediately, thereby enabling prompt action to be taken. A control should be monitored for proper operation, and an analysis carried out of its failures and attempted attacks on it. It is dangerous to possess a control which is presumed to be operating correctly, but in reality may be under attack, malfunctioning, or disabled. Feedback provided by a control must be presented efficiently, in order to ensure that it can be examined and clearly understood. Alarms can be used for immediate alerting. Parker (1976) referred to instrumentation and threat monitoring. Jackson and Hruska (1992) referred to monitoring.

Surveillance

Gaines and Shapiro (1978), Fisher (1984) and Martin (1973) discussed the use of surveillance (observation) for detection purposes. Fisher (1984) described the monitoring of journals for variance, and the monitoring of personnel.

Sustainability

Controls should be robust, i.e. they should function effectively throughout their operating life (Parker 1976, 1981). Wood (1990) believed that controls should be able to withstand attacks over time, and in hostile circumstances. Sustainability is more likely if the controls are automated, rather than dependent on people, whose motives and attitudes are questionable. The more flexible and adaptable the controls, the more sustainable they are likely to be. Also, the ability to handle intentional and unintentional attacks promotes the sustainability of controls.

Accountability

Wood (1990) believed accountability to be a fundamental principle for information security. This involves designating a specific person responsible for the security of an asset (Hamilton 1972) or answerable for a specific operation of a control (Caelli et al. 1989). Parker (1981, 1984) argued that an individual should not be responsible for too many controls, as this may lead to the violation of the least privilege and sustainability principles. An example of accountability is the use of user identifiers and passwords for authentication, as this gives the user the responsibility for protecting this information. Pfleeger's (1989) view of accountability was that a system should provide a comprehensive, secure history of security-related actions, for example by recording denied accesses. Caelli et al. (1991) suggested that audit information should be safely stored, and used to trace actions back to specific users. The OECD (1995) referred to the responsibilities of owners, providers and users of systems being made explicit.

Acceptance of Control Subjects

This principle was discussed as personnel acceptance and tolerance by Parker (1976, 1981, 1984), and as awareness of problem, easy to use, likelihood of use (Pfleeger 1989), acceptability (Lane 1985), and psychological acceptability (Saltzer 1974, Saltzer and Schroeder 1974). User acceptance is essential in order for users to routinely, willingly, effectively, appropriately and automatically apply controls (Berman 1983, Schweitzer 1982). For a control to be effective, users should understand its role in maintaining security, and should accept associated constraints. Users who do not accept controls will circumvent them (Wood 1990, Schweitzer 1982, Caelli et al. 1989, Berman 1983). User acceptance may be achieved via training and other forms of encouragement. For example, users would be encouraged by

management adherence to controls. An example of a generally well-accepted control is the password.

Awareness

The OECD (1995) advise that owners, providers and users of systems should be able to readily gain information about existing information security measures, and further, should be made actively aware of such measures (provided that information security measures are not compromised as a result).

Defensive Depth

Defensive depth refers to a series of consecutive controls that need to be encountered separately by a penetrator in order to reach their target (Cole 1978, Pfleeger 1989, Graham 1968, Caelli et al. 1989, 1991, Gigliotti 1984, Gaines and Shapiro 1978, Parker 1981, 1984, Wood 1990). Controls should be layered for added security, either via multiple control points (Fisher 1984), or repeated use, of the same control. Wood (1990) suggested that controls are stronger when applied in parallel rather than in series, and recommended the use of redundant controls. Farr et al. (1974) also espoused redundant controls in operating system modules, as an extra defence against the inevitability of bugs in large, complex systems. Layered controls can, however, frustrate legitimate users who require frequent access. For example, with computer networks, several passwords may be required for access to a specific resource. Caelli's (1989) ring model of controls, displaying various layers of controls to be penetrated, illustrates the principle of defensive depth. Pfleeger (1989) discussed overlapping controls.

Isolation and Compartmentalization

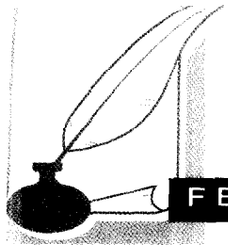
The principle of isolation and compartmentalization is based on the old adage "don't put all your eggs in one basket" (Wood 1990). The principle states that logical and physical assets should be distributed and divided into separate groups to minimise loss of assets in the event of a control being compromised (Graham 1968, Parker 1976, 1981, 1984, Pfleeger 1989, Saltzer and Schroeder 1975, Wood 1990). Pfleeger (1989) discussed physical, temporal, cryptographic and logical separation. For example, multiple backups of valuable software should be stored at different sites, so that in the event of a fire, a copy will still be secure. Controls should also be minimally dependent on other controls in order to minimise failure overall.

Least Common Mechanism

Cole (1978), Saltzer and Schroeder (1975), Parker (1981, 1984), Pfleeger (1989) and Wood (1990) discussed the concept of minimising controls common to a number of users. Wood (1990) stated that this principle implies that 'the effectiveness of controls should not, to the extent possible, depend on the proper operation of other controls'. For example, local area networks (LANs) in a star configuration depend on the central node for proper operation; if that node fails, the network would be unavailable. However, if the network were to employ a ring configuration, the failure of one node would not cause unavailability, as traffic could still be sent the opposite way around the ring (Wood 1990). Least common mechanism also suggests that the proficiency of any single control should not be dependent on the correct operation of other controls.

Control the Periphery

Wood (1990) argued that systems should aim to detect and prevent a breach at the point of entry to the system, rather than when the attacker has already gained entry. This principle was first referred to by Cole (1978) as object versus path protection, recommending protecting the



path to an object as well as the object itself. An example is a virus detection package which informs a user in the event of an inserted infected floppy disk, before the users can run the software on the infected disk, in order to protect software already in the computer (Wood 1990). Saltzer and Schroeder (1975) believed that this principle, when properly applied, underpinned the security of a system.

Completeness and Consistency

Controls should meet specifications and be completely tested before they are implemented and operated (Parker 1976, 1981, 1984, Wood 1990). Wood (1990) described 'provably secure systems' in the US Department of Defence, incorporating comprehensive specification and testing of controls. Controls also require consistent specifications, and regular, monitored operation (property of consistency). Irregular application of controls may draw attention to a vulnerability. Cole (1978) referred to self-checking, where controls are checked for correct operation by various means, for example via diagnostic tools. All possible compromise attempts may not be able to be identified in adaptive organizations (Baskerville 1992), and thus the aim of completeness may not be achievable.

Default to Denial

This principle (Wood 1990) has been referred to as failsafe default (Parker 1981, 1984, Saltzer 1974, Saltzer and Schroeder 1975). This principle proposes that when a control fails, access must be denied so that security will not be compromised accidentally. For example, if there is a power failure, an electronic door must remain in a locked state. It is important to ensure human safety when implementing this principle, for example there must be an alternative escape mechanism in the event of a fire, in the locked door situation above.

Total reliance should not be placed on the ability of computers to provide correct security, as they lack human commonsense, and are thus unable to analyse and deal with all possible circumstances. Technology needs to develop significantly before it can be adjudged self-sufficient for security purposes. Humans should be involved in the enforcement and development of security design and decisions. Wood (1990) believed that a human being must always double check on important decisions made by the system. This principle appears to conflict with Parker's (1981, 1984) principle of minimum reliance on real-time human intervention.

Secure Image

According to Gigliotti (1984) and Wood (1990), the public should be confronted by a secure system image, whether the system is secure or not. Since security is a psychological state of mind, a secure image lessens the chances of attack and, accordingly, to appear vulnerable may provoke exploitation, abuse and attack. This is one reason why organizations whose systems have been breached often do not draw the breach to the attention of the public by reporting it to the media.

Low Profile

Valuable assets should be kept out of view, in order to reduce the likelihood of attack (Gigliotti 1984, Schweitzer 1982, Gaines and Shapiro 1978, Wood 1990). An example is the placement of expensive computer equipment in a windowless room. The principle also suggests that the existence of, and details about, controls, should not be disclosed to the subjects of the controls (see principle of concealment). Potential violators may be aware that they do not know enough about a control in order to compromise it, unapprehended.

Risk Reduction

Parker (1976) recommended evaluating each proposed control to determine its

ability to reduce the risk of threats to the assets which are to be protected. Risk reduction is typically achieved via risk assessment techniques.

Legal and Ethical Considerations

Parker (1976) stated that controls should comply with the law, and further, should not impose unethical pressures on people. Parker (1976), Fisher (1984) and Lane (1985) believed that employees should not be placed in a position where they could easily gain access to unauthorised information or use company assets to their advantage. It is the employer's responsibility to determine the employees' limit of temptation and place trust in them accordingly. Fisher (1984) referred to prohibit conversion and concealment. The OECD (1995) advised that the rights and legitimate interests of all people are resected by information security provisions.

Reference Monitor

This principle was proposed by Cole (1978), and involves designing access controls so that they are:

- always invoked
- isolated from unauthorised alteration, and
- accredited as being trustworthy.

Identification

Every subject must be uniquely linked to an identifier, in order to enable checking of an access request (Cole 1978, Schweitzer 1982, Fisher 1984, Pfleeger 1989).

Marking

This principle requires every object to be linked to a label showing the security level of the object, thereby 'marking' the object (Pfleeger 1989). Whenever there is an access request for that object, the label may be checked for permission-granting or denial. Jackson and Hruska (1992) discussed file labelling , in which the security level of a file is classified internally, via magnetic coding, or externally, via visible exterior marking, or via both means.

Multiple Functions

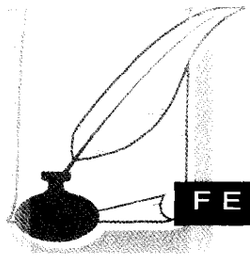
Controls are usually selected to serve one security function: either deterrence, prevention, detection or recovery (Parker 1981, 1984). Each control chosen may, however, have a secondary function as well. Most controls have some degree of deterrence. For example, a uniformed security guard at a door has more deterrent value than an electronically locked door. A control that serves more than one security function at a time is a stronger control. Parker (1981, 1984) provides a qualitative method for multiple function evaluation.

Concealment

Gaines and Shapiro (1978) discussed the principle of concealment which applies to both physical and abstract controls, and the valuable information itself. All knowledge required to mount a successful attack should be hidden from possible perpetrators. Encryption of data is an example of concealment of valuable information. This principle conflicts with overt design and operation.

Compromise Recording

Saltzer and Schroeder (1975) suggested that controls which responsibly record an attempted breach may be preferred to a complex control which would entirely prevent a breach. They argued that it may be more useful to be made aware of the breach in order to take appropriate corrective action by designing an improved control. For example, a padlock on a filing



cabinet, when damaged, shows the user who next uses the cabinet that a compromise has occurred. An improvement on the padlock control could then be designed.

Discretionary Privilege

Users will be given the least access privileges necessary, however users may be able to pass these privileges on to other users, at their discretion, in order to provide all users with minimal restrictivity (Lichtenstein 1996). This is a variation of the least privilege principle, aimed at the information security needs of adaptive organizations.

Control the Core

When organizational boundaries are fuzzy and flexible, as in adaptive organizations (Lichtenstein 1996), controls should concentrate on protecting the actual asset rather than the point of attempted break-in.

Default to Human Involvement

In the case of control failure, humans should be given the authority to decide whether access should be granted or denied (Lichtenstein 1996), whilst the control is being restored. This conflicts with default to denial, and was suggested for adaptive organizations, where adaptive security is a key requirement.

Semi-hostile Environment

In an adaptive organization, controls should be designed for an environment in which it is important to trust the users, and to anticipate that the users may also be novices (Lichtenstein 1996). The system's lifespan may be short, and users may not be able to become familiar enough with the system to abuse it.

Changing Image and Profile

A changing image can be presented to the public, as this may discourage attack due to the difficulty involved in becoming familiar with a system under constant change (Lichtenstein 1996).

Flexibility

Controls should be designed to be versatile and interpretable so that they can be used in different situations in a number of ways (Lichtenstein 1996). Cole (1978) referred to this as extendability, stating that controls must be able to handle new and changing requirements, as otherwise users may circumvent the controls. Berman (1983) suggested that controls needed to be interpretable in different situations. For example, if a user has obviously misspelled his or her name whilst logging in, it would be unreasonable to disable access privileges. However, if a user has repeatedly attempted an unauthorised access to a file, it is reasonable to disable their access privileges temporarily.

Maintainability

Maintainability of controls is important (Fisher 1984), particularly in adaptive organizations, as controls are likely to need changes within only a short system lifespan, and therefore any required changes must be able to be made promptly and easily (Lichtenstein 1996).

Logicality

Logical controls are preferable to physical controls, as they are more flexible (Lichtenstein 1996, Baskerville 1992). Controls can be designed to possess a logical component, which may be extracted and reused as required.

Reusability

Controls should be designed to be reusable, so they can be used for different

situations and systems (Lichtenstein 1996, Baskerville 1992).

Disposability

Throw-away security needs to be considered in the design and selection of controls, so that when certain controls are no longer required for an application, they can be easily dismantled or disposed of (Lichtenstein 1996, Baskerville 1992).

Interpretability

Controls should not have limited usefulness through being highly technical (Lichtenstein 1996, Baskerville 1992). Controls should be open to human interpretation, so that they are used in the most appropriate way for a specific situation.

CONCLUSION

The review of the seventy-three principles described in this article constitutes a resource for information security practice and research, as suggested in the introduction. In a related paper (Lichtenstein 1998), a taxonomy of the principles is defined which groups the principles described above into classes. Planned future work includes continuing the search for additional principles, and evaluating the applicability of the principles to modern systems and organizations.

Contact: Ms Sharman Lichtenstein
Department of Information Systems,
Monash University, Melbourne, Australia
Email: sharman.lichtenstein@is.monash.edu.au

REFERENCES

Baran, P. (1964) Security, Secrecy and Tamper-free Considerations, On Distributed Comms 9, Rand Corp Techn Rep.

Baskerville, R. (1988) Designing Information Systems Security, John Wiley.

Baskerville, R. (1992) Information Systems Security : Technology and Management, Copenhagen Business School, Copenhagen.

Berman, A. (1983) Evaluating On-line Computer Security, Data Communications (DCM), 12 (7), July.

Brock, R.H., Palmer, E.C. and Cunningham, M.B. (1986) Accounting : Principles and Applications, McGraw-Hill Book Company.

Caelli, W.J. (1987) Guidelines for Privacy and Security in Computer Systems, Australian Computer Journal, 19(4).

Caelli, W.J., Longley, D. and Shain, M. (1989) Information Security for Managers, Macmillan Publishers Ltd.

Caelli, W.J., Longley, D. and Shain, M. (1991) Information Security Handbook, Macmillan Publishers Ltd.

Cole, G.D. (1978) Computer Science and Technology: Design Alternatives for Computer Networks Security, National Bureau of Standards, Special Publications US Government Printing Office Washington.

Farr, M.A.L., Chadwick, B. and Wong, K.K. (1974) Security for Computer Systems, NCC Publications.

Fisher. R. (1984) Information Systems Security, Englewood Cliffs: Prentice-Hall.

Gaines, S. and Shapiro, N.Z. (1978) Some Security Principles and their Application to Computer Security, Operating Systems Review, 12.

Gigliotti, R.J. (1984) Security Design for Maximum Protection, Butterworths Publishers.

Graham, R.M. (1968) Protection in an Information Processing Utility, Communications of the ACM, 11 (5).

Hamilton, P. (1972) Computer Security, Cassell / Associated Business Programmes Ltd.

Jackson, K.M. and Hruska, J. (1992) Computer Security Reference Book, Butterworth- Heinemann Ltd, Oxford.

Lane, V.P. (1985) Security of Computer Based Information Systems, Macmillan Education Ltd.

Lichtenstein, S. (1996) Information Security Design Principles for Adaptive Organizations, Computer Audit Update Journal, June, Elsevier Advanced Technology, UK.

Lichtenstein, S. (1998) Information Security Principles: a Holistic View,Computers & Security (forthcoming).

Martin, J. (1973) Security, Accuracy and Privacy in Computer Systems, Prentice-Hall Inc. Englewood Cliffs, N.J.
OECD (1995) Guidelines for the Security of Information Systems, OECD.
Parker, D.B. (1976) Crime by Computer, NY: Charles Scribner's Sons.
Parker, D.B. (1981) Computer Security Management, Reston : Reston.
Parker, D.B. (1984) Safeguard Selection Principles, SRI International, Menlo Park, California, USA.
Peters, B. (1967) Security Considerations in a Multi-program Computer System, Proceedings AFPS, 30 AFIPS Press.
Pfleeger, C.P. (1989) Security in Computing, Prentice-Hall International, Inc.
Saltzer, J.H. (1974) Protection and the Control of Information Sharing in Multics, Communica-tions of the ACM, 17(7), July.
Saltzer, J.H. and Schroeder, M.D. (1975) Protection of Information in Computer Systems, Compcon Conference Proceedings, IEEE.
Schweitzer, J.A. (1982) Managing Information Security: A Program for the Electronic Information Age, Butterworth Publishers.
Smith, A. (1776) An Inquiry into the Nature and Causes of the Wealth of Nations, London: Methuen.
Weissman, C. (1969) Security Controls in the ADEPT-50 Time-sharing System, AFIPS Conference Proceedings, 35.
Wood, C.C. (1990) Principles of Secure Information Systems Design, Computers and Security, 9.