South African
Computer
Journal
Number 17
September 1996

Suid-Afrikaanse
Rekenaar-
tydskrif
Nommer 17
September 1996

Computer Science
and
Information Systems

Special Edition: Computer Security

Rekenaarwetenskap
en
Inligtingstelsels

IBM

The South African Computer Journal
An official publication of the Computer Society of South Africa and the South African Institute of Computer Scientists

Die Suid-Afrikaanse Rekenaartydskrif
'n Amptelike publikasie van die Rekenaarverenging van Suid-Afrika en die Suid-Afrikaanse Instituut vir Rekenaarwetenskaplikes

Editor
Professor Derrick G Kourie
Department of Computer Science
University of Pretoria
Hatfield 0083
Email: dkourie@dos-lan.cs.up.ac.za

Subeditor: Information Systems
Prof Lucas Introna
Department of Informatics
University of Pretoria
Hatfield 0083
Email: lintrona@econ.up.ac.za

Production Editor
Dr Riël Smit
Mosaic Software (Pty) Ltd
P.O.Box 23906
Claremont 7735
Email: gds@mosaic.co.za

World-Wide Web: http://www.mosaic.co.za/sacj/

Subscriptions

	Annual	Single copy
Southern Africa:	R50,00	R25,00
Elsewhere:	$30,00	$15,00

An additional $15 per year is charged for airmail outside Southern Africa

to be sent to:
Computer Society of South Africa
Box 1714 Halfway House 1685

Phone: +27 (11) 315-1319 Fax: +27 (11) 315-2276

Information Security – The Family Member Who Came Home

Basie von Solms
Rand Afrikaans University, Johannesburg, South Africa
basie@rkw.rau.ac.za

The claim that the information society is upon us and that the information superhighway is about to affect us all, is such a cliche that it hardly bears repeating - practically everyone is talking and writing about it. Although the assertion that information *security* is an essential and integral part of the information society might also seem cliched to some, it nevertheless does not get as much attention and exposure as it should. Information security has always been seen in the same light as taxes: nobody really wants it, but everybody (reluctantly) admits that we need it. Following an alternative analogy, it is like an unwanted family member: we realise that he is part of the family, but we really do not want to be bothered by him. In the last few years, the growth of the Internet and the explosive appearance of the World Wide Web (WWW) has brought information security into corporate boardrooms and private lounges. Suddenly everyone wants to get to know this unwanted family member a little better!

This issue of SACJ is dedicated to the unwanted family member and if, by reading this issue, all of us in the IT family are able to learn just a little more about this sibling, then producing the issue would have been worthwhile. In fact, we should welcome him back home as soon as possible.

A little background about this issue is in order. The International Federation for Information Processing (IFIP) is a consortium of about 60 member countries. It provides an umbrella for many international IT activities. Countries are represented by their national IT society, South Africa being represented by the Computer Society of South Africa (CSSA). IFIP has a total of 13 Technical Committees (TCs), each concentrating on a different aspect of IT. TC 11 deals with all aspects of information security. It organises an annual international conference – the so-called IFIP/Sec series, which is widely regarded as one of the major information security conferences.

IFIP/Sec 95, the 11th International Conference on Information Security, took place in Cape Town in May 1995 and IFIP/Sec 96, the 12th International Conference on Information Security, took place on the Greek island of Samos in May 1996. Complete proceedings of the two conferences, together containing more than 80 articles, have been published by the official IFIP publishers, Chapman and Hall. This issue of SACJ consists of a selection of four articles from the IFIP/Sec 95 Proceedings and two from the IFIP/Sec 96 Proceedings. It is intended not only to disseminate relevant information, but also to bring the information security interests of SAICSIT, CSSA, IFIP and TC 11 to the attention of readers. If, after reading this issue, you are interested in the remaining 74 articles, or in the activities of any of these bodies, please feel free to contact the guest editor directly.

The selected articles cover a diverse range of information security issues. Parker extends its theoretical and conceptual understanding, Hoffman addresses several of its non-technical but crucial aspects, Muftic concentrates on its role in open distributed systems, de Ru and Eloff link into the use of biometrics in information security, von Solms investigates the security protocols for the Internet and WWW, and Pangalos and Khair remind us that information security requirements extend even into the medical field.

The first four articles are from the IFIP/Sec 95 Proceedings. The first, by Donn Parker, suggests a framework for information security in order to avoid information anarchy. He argues that the traditional view of the role of information security – to protect the three elements of confidentiality, integrity and availability of information – is dangerously oversimplified. He includes three more elements of information into the equation: authenticity, utility and possession. The article provides a good platform for gaining a better understanding of what information security really ought to be about.

In the second article, Lance Hoffman addresses the important issues of escrow encryption and export controls – specifically, as he clearly points out, from a US standpoint. The article highlights the very important fact that cryptology is not merely a technical issue, but that the political overtones, civil liberties and administrative implications are also extremely relevant. Ignoring these non-technical issues, as many information security specialists tend to do, will have a negative impact on the field becoming a discipline in its own right. Since its first publication, some of the issues raised by the Hoffman article have been receiving attention. For example, the idea of international cryptology policies is being addressed by the European Organisation for Economic Cooperation and Development (OECD). Relevant recent articles on the escrow aspect can be found in [1].

In the next article, Sead Muftic concentrates on aspects of security in open distributed environments. He identifies a number of elements suitable for a secure system in such an environment. These are: smart cards, secure user workstations, integrated security clients, security servers and a global certification system for international networks. This last aspect is becoming more and more important as basically all secure protocols use public key encryption in some form or the other. Using these elements, he also describes a number of security enhanced applications – secure Internet e-mail and secure EDI. Muftic stresses the fact that all these elements are operational, implemented, and already in use.

de Ru and Eloff then discuss the reinforcement of password authentication using typing biometrics. Biometric methods are probably the best means of authentication, but many of these methods are technology-intensive and expensive. Their article tries to use typing characteristics as a cheap and user-transparent way to augment the traditional password.

The last two articles are from the IFIP/Sec 96 Proceedings. von Solm's article gives an overview of two non-payment related and one payment related secure protocol for the Internet and the WWW. The non-payment related protocols are Secure Sockets Layer (SSL) and Secure Hypertext Transport Protocol (SHTTP). SSL is usable in any TCP/IP environment, while SHTTP is specifically for the WWW. Both make use of public key encryption. The payment related protocol, Secure Payment Protocol (SEPP) was superseded by the Secure Transaction Protocol (SET) early in 1996, but only after the article had already been submitted to IFIP/Sec 96. The presentation at the conference however, covered SET and not SEPP. An appendix is attached to this article, giving a brief overview of SET, as SEPP is no longer relevant. SET also uses public key encryption.

The last article by Pangalos and Khair introduces a methodology to improve the security of medical databases in relation to authentication. Though the methodology of the authors is in itself important and interesting, the article was selected for this issue to underline the importance and relevance of information security in medical IT applications – an area where security introduces new problems quite distinct from those traditionally encountered in the financial and other fields. Becuase of the differences, information security in medical applications still requires much research.

It is hoped that readers will find this issue of SACJ useful, and also that they will get involved with the activities of the bodies mentioned above.

References

1. *Communications of the ACM*, **39**(3):33–53, (March 1996).
2. http://www.visa.com.

Appendix A

Secure Electronic Protocol (SET) [2] is the secure payment protocol announced by MasterCard and Visa in February 1996. The two previous protocols, SEPP and STT, announced independantly by these two companies, were replaced by SET.

This Appendix gives a brief and oversimplified overview of the SET message flow between the customer and the merchant when a payment is made.

Only the most basic parts of messages are discussed, and many details are left out for the sake of simplicity.

The electronic purchasing process can basically be divided into two phases. Phase 1 is a browsing and negotiation phase in which the customer will decide what to buy. Goods and price will be negotiated and agreed upon between the customer and merchant. The phase will probably end with a completed order form, specifying the goods,with the associated price, the customer is about to buy.

At this point the customer decides to start Phase 2, the payment phase. It is at this point that the SET payment protocol is initiated.

Step 1:

A message is sent from the customer to the merchant, requesting, amongst other things, the public key certificates of the merchant and the merchant's acquirer.

Step 2:

The merchant sends these certificates back to the customer.

Step 3:

- The customer validates the certificates received from the merchant.
- The customer constructs the Order Information (OI).

  OI contains info about the goods and negotiated price.
- The customer generates a DES key K1 and encrypts OI under K1, giving K1(OI).
- The customer encrypts K1 using the public key of the merchant, giving MP(K1).
- The customer constructs the hash of the OI, giving H(OI).
- The customer constructs the Payment Information (PI). The PI contains info about the credit card nr, expiry date etc.
- The customer generates a DES key K2 and encrypts PI under K2, giving K2(PI).
- The customer encrypts K2 using the public key of the acquirer, giving AP(K2).
- The customer constructs the hash of the PI, giving H(PI).
- The customer constructs the hash of OI, the hash of PI and concatenates them, giving H(OI)||H(PI).
- The customer digitally signs this concatenation giving S(H(OI)||H(PI)). The customer performs

this operation to uniquely associate the specific OI with the specific PI.

Step 4:

The customer sends the message M1= [K1(OI), MP(K1), H(OI), K2(PI), AP(K2), H(PI), S(H(OI)||H(PI))] to the merchant.

Step 5:

The merchant receives M1= [K1(OI), MP(K1), H(OI), K2(PI), AP(K2), H(PI), S(H(OI)||H(PI))]

- The merchant retrieves K1 and then OI.

  Note that the merchant cannot retrieve PI in any way. The customer intended it this way, because he/she does not want the merchant to see his credit card info.

- The merchant creates H(OI), concatenates it with H(PI) received in M1, and compares it with the H(OI)||H(PI) received in M1.

  Note that the merchant can retrieve H(OI)||H(PI) from S(H(OI)||H(PI)) by using the customer's public key.

  If they are equal, then the merchant knows that the OI he/she has retrieved from M1 is the 'correct' OI intended by the customer to accompany the PI provided by the customer.

  Note that this process allows the merchant to associate a specific OI with a specific PI without knowing precisely what PI is.

Step 6:

The merchant now requests an authorisation from his acquirer, by sending the following message M2 to the acquirer: [H(OI), K2(PI), AP(K2), H(PI), S(H(OI)||H(PI))]

- The acquirer goes vica versa through the same procedure as the merchant, allowing the acquirer to associate the specific PI with the specific OI without knowing precisely what OI is.

  The customer does not want the acquirer to see what he/she is buying, but wants the acquirer to link the OI to the PI.

Step 7:

If necessary, the acquirer gets authorisation from the issuer, and send a digitally signed authorisation back to the merchant.

Step 8:

The merchant informs the customer that the transaction is authorised.

SACJ is produced with kind support from
Mosaic Software (Pty) Ltd.

A New Framework for Information Security to Avoid Information Anarchy

Donn B Parker
SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025

Abstract

It is reasoned that to preserve the three traditional elements of information security, confidentiality, integrity and availability, it is not sufficient to fully protect information. Three new elements are introduced: authenticity, utility and possession of information. Different scenarios are used to demonstrate that all six these elements are needed for comprehensive information protection.

Keywords: *Information Security, Confidentiality, Integrity, Availability*
Computing Review Categories: *D.4.6, K.4.2*

1 Introduction

The purpose of information security that most infosec specialists identify is to preserve the three elements of confidentiality, integrity, and availability of information. The 1991 paper, *Restating the Foundation of Information Security* [1], argues that this is a dangerously oversimplified definition of infosec. The preservation of these three elements does not include many kinds of information losses that infosec should prevent. My intent is to demonstrate in more rigorous fashion that the preservation of these elements must be expanded for infosec to be sufficiently comprehensive to protect information appropriately in all of its security aspects.

Accordingly, I have added authenticity, utility, and possession of information as other elements that must be included. I discovered the last element, possession of information, in dealing with the theft of small computers, wherein the loss of the exclusive possession of the information content of thc stolen computers is often greater in value than the loss of the computers. Yet the thieves may not even be aware of the information and therefore do not violate either the possible confidentiality or availability of it when the victim still possesses a backup copy. The victims have lost exclusive possession of the information in these cases but not its confidentiality, availability, utility, integrity, or authenticity. The victims might suffer a loss from extortion, for example, in which none of these other elements are violated.

My intent here is to rigorously demonstrate the need for all six of the above elements of information security preservation. The stated pairing and order of these six required elements-and the resultant deeper understanding of infosec-also have some logic and practical value, as will be seen. First, I will demonstrate the need for these elements through scenarios of infosec loss in which each loss is explicitly covered by one and only one of the elements. Therefore, if a loss scenario is accepted as a subject for infosec attention, then the element covering the loss in that scenario must be attributed as an element of infosec. In addition, I suggest some controls that are needed specifically to protect the information from each loss. Some of these controls might be overlooked if any one of the six elements has not been explicitly included.

The possibility exists that more elements of information security than the six presented here may be needed to cover additional types of losses. This could happen as information technology advances, criminals become more innovative, or the concept of infosec changes is extended.

I claim that if the elements of infosec are not rigorously, comprehensively, and logically stated and addressed, using the correct English language meaning of each word, infosec will remain the incomplete and flawed folk art it is today. (Integrity has been abused in this regard by defining it incorrectly to include the meaning of authenticity-see the appendix for the dictionary definitions of the elements.) With such inexactitude, infosec and its practitioners will ultimately lose the confidence of society, and the perpetrators of information loss will continue to successfully take advantage of infosec shortcomings both in practice and under the law.

For example, all infosec specialists should understand that protecting the possession of information as intellectual property is an obvious requirement under common, copyright, trade secret, and patent law. Yet possession cannot be included within the meaning of the original three elements of preserving confidentiality, integrity, and availability. To illustrate, possession but not confidentiality can be lost if the victim encrypted the information before it was stolen. In addition, by definition, integrity cannot be lost or changed in this example because it is an intrinsic property of information content and is not associated with the extrinsic property of possession that does not affect the content. Finally, possession but not availability can be lost if, for example, the new possessor makes the stolen information available for sale to the owner, such as in a case of extortion. Exclusive possession can also be lost but availability preserved if only a copy of the information is stolen. In contrast to the theft of tangible objects when the objects are copies, not authentic originals, loss of exclusive possession is unique to information. Infosec must recognize that two or more people can possess the very same, authentic information simultaneously.

Possession is an extrinsic property of information similar to confidentiality. The information may or may not be possessed, but this has no effect on the information itself. Examination of the information does not necessarily identify who possesses the information or if anyone possesses it. In addition, the information may contain the ownership identity but not the identity of the current possessor. For infosec purposes, ownership should be considered to be a form of possession. Under law, one party may possess information but another may own it. Stealing information may be different than stealing the ownership of information.

I believe that possession has not been fully considered as a unique element of infosec because government – which considers possession and confidentiality as synonymous – has dominated the development of infosec. Treating possession and confidentiality separately reveals a profound underlying difference in the security needs of business and democratic government and makes clear why democratic government security does not apply identically to business. In a democratic government, information is owned by all the people governed; it is public information, and the only constraint is whether it should be kept confidential. Otherwise, at least in the United States, the Freedom of Information Act requires that the information be shared with the public. A democratic government holds no exclusive copyright, patent, or trade secret right to it. Government does not buy, sell, barter, or trade information, except in some cases to cover costs of publication or to offset costs of other services.

In business, information is a commodity or facilitates a service that is bought, sold, bartered, and traded to make a profit, and the primary purpose of infosec is to protect such business information as an asset or property. When government information is stolen, the fear is only for loss of confidentiality; when business information is stolen, possession or exclusive possession is lost. Loss of confidentiality is only a consequence in some cases after loss of possession. For example, the huge problem of software piracy is the loss of possession-including control over software use-and confidentiality is rarely an issue. Business does have a small amount of high-value information for which loss of confidentiality rather than loss of exclusive possession is the greatest concern, and the consequential loss of confidentiality is most often profits. A similar loss in government would result in very different consequences, primarily loss of military or diplomatic advantage.

We must conclude that business and government infosec have some of the same confidentiality concerns, but business infosec has the additional possession element that government does not have. Taking most kinds of information from the government is not stealing and no loss is incurred. Taking most kinds of information from a business is stealing and loss of possession or at least exclusive possession is extremely serious. Espionage against government and business that causes a loss of confidentiality of some information is most serious.

These differences make clear why employee clearances, the principle of need-to-know, mandatory access control, classification of information, and cryptography are typically most important government controls, whereas the owner, custodian, user accountability principle of need-to-withhold; discretionary access control; copyright and patent; and digital signatures are typically most important business controls.

Now consider the value of the expanded and more comprehensive elements of infosec for the purpose of identifying threats. If the security elements are separated into the more distinct six parts, more actions that adversaries may take can be conceived of in a threat analysis than the typically stated modification, destruction, disclosure, and use. For example, I am led to derive a far more "comprehensive threat list for information security." The following list- derived by considering all six elements as well as from collecting and studying more than 3,500 computer abuse cases since 1958-is a far more complete list of abusive actions against information:

- Threats to availability and usefulness
  - Destroy, damage, or contaminate
  - Deny, prolong, or delay use or access
- Threats to integrity and authenticity
  - Enter, use, or produce false data
  - Modify, replace, or reorder
  - Misrepresent
  - Repudiate (reject as untrue)
  - Misuse or fail to use as required
- Threats to confidentiality and possession
  - Access
  - Disclose
  - Observe or monitor
  - Copy
  - Steal
- Exposure to threats
  - Endanger by exposure to any of the above threats.

The last item, exposure to threats, was added as a separate category to deal with the human failing, and sometimes crime, of negligence on the part of managers, owners, custodians, users, and infosec specialists. The best solution to this problem is meeting a standard of due diligence by using infosec controls that are easily available or known and that are used by others under similar circumstances. Holding people accountable for their duties and responsibilities, as well as motivation and awareness programs for employees and managers, are also very important.

2 Formal Demonstration

I claim that the following six scenarios of information losses derived from real cases are well within the range of above-listed threats that information security should protect against. Following each scenario is an analysis of why each of the six proposed elements does or does not address the loss scenario. Because one and only one element of information security covers each scenario, that element must be included as a stated part of information security.

Loss Scenario I: Availability

Scenario I discusses the significance of the element of availability in a computer file theft. In an act of sabotage, the name of a data file is removed from the file directories in a computer possessed by the victim. Users of the computer and the data file no longer have the file available to them because the computer operating system recognizes the existence of information for users only if it is named in the file directories. The other information security elements do not address this loss because the utility, integrity, authenticity, confidentiality, and possession of the unavailable information have not been changed in the scenario as stated. Therefore, since availability is prevented as a result of this loss, preservation of availability must be accepted as a purpose of infosec.

Several controls are used to preserve or restore availability of data files in computers. These controls include having a backup directory with erased file names and pointers until the files are purged by overwriting with new files, good backup practices, good access controls to computers and specific data files, use of more than one name to identify and find a file, availability of utility programs to search for files by their content, and shadow or mirror file storage.

The severity of availability loss can vary considerably. For instance, all copies of a data file can be totally destroyed with no means of recovery; a data file can be partly usable with delayed recovery at moderate cost; or the user may have inconvenient access to the file with timely full recovery.

Loss Scenario II: Utility

In this scenario, an error occurred when the only copy of valuable information was routinely encrypted in a computer and the encryption key was accidentally erased or changed. The usefulness of the information was therefore lost and in this case could only be restored if cryptanalysis could be successfully accomplished.

Although this scenario could be described as a loss of availability or authenticity of the key that was lost or changed, the loss focuses on the usefulness of the information, not on the key. The only purpose of the key was to facilitate the encryption but not to provide the usefulness of the information that was encrypted. The loss concerned the information and its loss of utility. The loss of the key would be a loss of a different information asset.

The information in this scenario is available but in a form that is not useful. The integrity, authenticity, and possession are unaffected. Confidentiality is greatly improved if changed at all.

To preserve utility of information, four controls are suggested. These include internal application controls such as verification of data before and after transactions, security walk-throughs during application development to limit unresponsive forms of information at times and places of use, minimization of adverse effects of security on information use, and control of access that may allow unauthorized persons to reduce the usefulness of information.

The loss of utility can vary in severity. The most severe case would be the total loss of usefulness of the information with no recovery. Less severe cases could range from somewhat useful with full usefulness of data restored at moderate cost to less-than-perfect usefulness with timely full recovery.

Loss Scenario III: Integrity

A software company under pressure to meet a delivery date provided an accounts payable application program to a client without including an important control. The master copy held by the software company contained the control that functioned according to specifications. The omission was not discovered because no known violations of the control occurred. An accountant in the client company, however, discovered that the control was missing and that the program had failed to check for duplicate payments. The accountant took advantage of the omission and engaged in a large accounts-payable embezzlement. The client company sued the software supplier for negligence.

The software application performed as intended except that the duplicate billing control was missing. Because the program was incomplete, however, the product lacked integrity. The meaning of "integrity" is limited to "a state of completeness, wholeness, soundness, and adherence to a code of conduct."

Availability and utility were not violated in that the program was in use and was useful for its intended purpose so far as it went. Having come from the correct supplier, the program was authentic and performed correctly as far as it went. Its failure to perform the duplicate billing control meant that the program performed incorrectly under some circumstances, not because the control was incorrectly programmed but because it was missing. If the control were present but failed to conform to specifications, the program would lack authenticity; however, conforming to specifications was not relevant since the control was missing. The software company's failure was omitting the control in the program delivered, not the failure of the program (to the extent that it could perform) to conform to specifications. It was also a genuine program from the software company. Thus, the program lacked integrity, not authenticity. Confidentiality and possession are not affected and not at issue in the scenario.

Several controls can be used to prevent loss of integrity of information. These controls include using and checking sequence numbers and check sums or hash totals for series of ordered items that would ensure completeness and wholeness; doing reasonableness checks on types of information in designated fields; performing manual and automatic text checks on presence of records, subprograms, paragraphs, or titles; checking for unexecutable code and mismatched conditional transfers in computer programs; and promoting adherence to codes of ethics (to achieve integrity of people).

The severity of integrity loss can vary. Significant parts of the information can be contaminated or misordered but be short of total unavailability, with no recovery possible. Or, with delay, a few parts of the data in that condition can be restored at moderate cost. Alternatively, small amounts of contaminated information can be recovered in a more timely way at low cost.

Loss Scenario IV: Authenticity

A book distributor obtained the text of a book on a disk from an obscure publisher. The distributor changed the name of the publisher on the disk to a well-known one, had the book printed, and-unknown to either publisher-distributed it successfully in a foreign country.

The book was misrepresented as published by a well-known publisher. Therefore, it did not conform to reality and was not an authentic book from that publisher.

Availability and utility are not at issue in this case. The book also had integrity because it was complete and sound. The publisher lacked integrity since it didn't conform to ethical practice, but that is not the subject of the scenario. The correct owner also possessed the book even though it was deceptively represented as having come from the popular publisher. Although the distributor would have attempted to keep its actions secret from the popular publisher (and probably the obscure publisher), confidentiality of the content of the book was not at issue.

A number of controls can be applied to ensure authenticity of information. These include confirming account balances, transactions, correct names, deliveries, and addresses; checking on genuineness of products; segregating duties or dual performance of activities; using double entry bookkeeping; checking for out-of-range values; and using passwords, digital signatures, and tokens to authenticate users at workstations and LAN servers.

The severity of authenticity loss can take several forms, including no conformance to genuineness or to fact or reality with no recovery possible. Authenticity loss can also be moderately false or deceptive with delayed recovery at moderate cost, or information can be mostly factual.

Loss Scenario V: Confidentiality

An individual inserted a radio transmitter into an ATM that received signals from the touch-screen CRT used for inputting customers' PINs and conveying account balances. The device then broadcast the information to a receiver that recorded the PINs and account balances on a VCR for retrieval.

The secrecy of the customers' PINs and account balances were violated. Hence, their privacy was invaded.

Availability, utility, integrity, and authenticity are unaffected in the confidentiality violation. The customers' and the bank's exclusive possession of the account balances information was lost but not possession per se because they still held and owned the information.

Controls to maintain confidentiality include using cryptography, training employees to resist deceptive social engineering attacks designed to obtain their technical knowledge, physically controlling location and movement of mobile computers and disks, and controlling access to computers and networks. Security also requires ensuring that resources for protection should not exceed the value of what may be lost, especially with low incidence. For example, protection against radio frequency emanations in ATMs (such as in the scenario described above) is probably not advisable considering the cost of shielding and access control, the paucity of such high-tech attacks, and the limited monetary losses possible.

The severity of loss of confidentiality could vary. The loss in the worst circumstance would be disclosure of information to the most harmful party with permanent effect. Information could also be known to several moderately harmful parties with a moderate-term effect or be known to one harmless, unauthorized party with short-term effect.

Loss Scenario VI: Possession

A gang of burglars aided by the disgruntled and recently fired operations supervisor break into a computer center and steal all copies of a company's master files on tapes and disks. They also raid the backup facility and steal all backup copies of the files. They hold the materials for ransom in an extortion attempt.

The burglary resulted in temporary lost possession of all copies but not loss of legal ownership of the master files and media on which they were stored. Loss of ownership and permanent loss of possession would be accomplished if the materials were never returned and the victims were to stop trying to recover them.

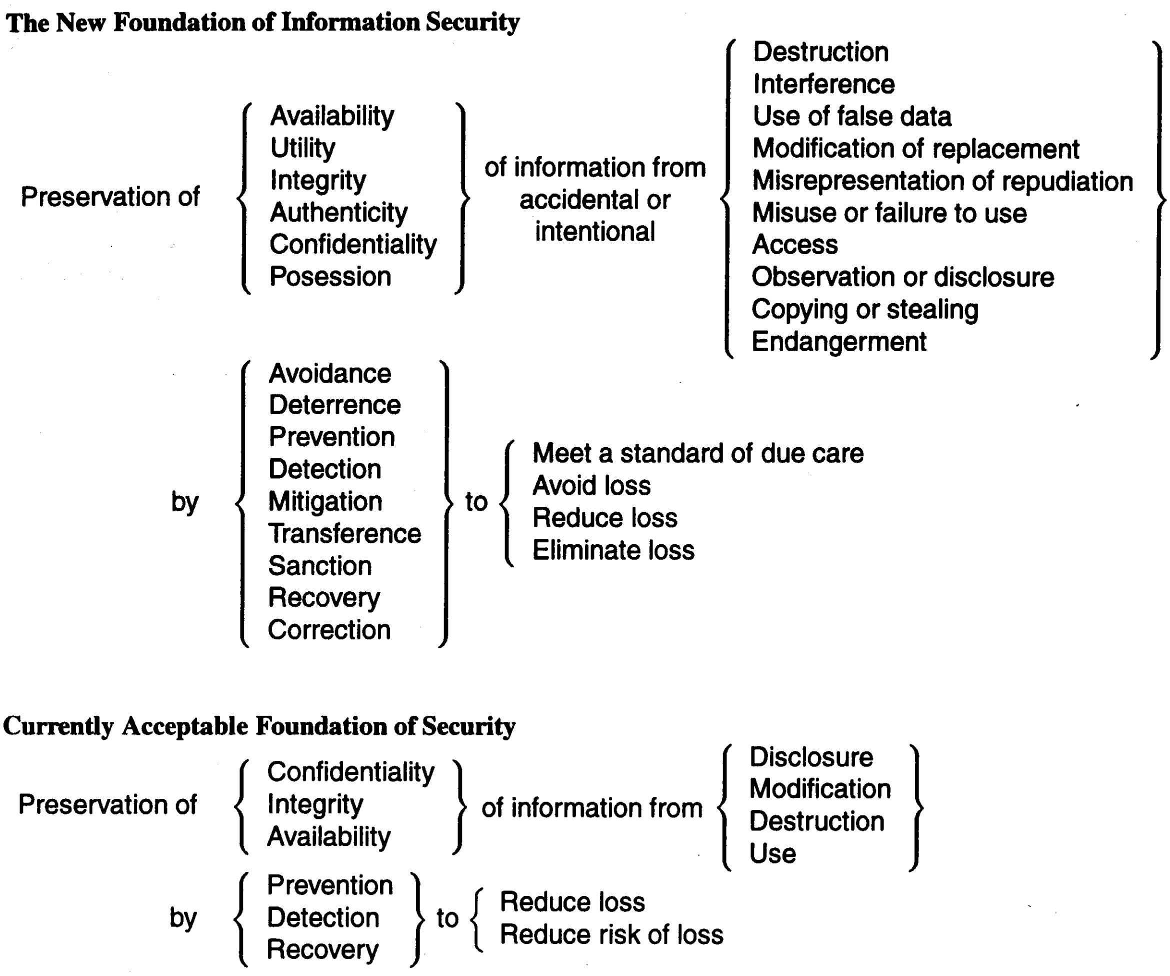
Availability is delayed in this scenario but could be accomplished by paying the ransom or using legal force to recover the materials. Utility, integrity, and authenticity are not an issue. Confidentiality would not be violated unless the files were read or disclosed.

Several controls should be used to protect the possession of information. These include using copyright, patent, and trade secret laws; implementing physical and logical access limitation methods; preserving and examining computer audit logs for evidence of stealing; using file labels; inventorying tangible and intangible assets; etching identification on computer equipment; using distinctive colors and labels on disk jackets; and assigning ownership to organizational information assets.

The severity of loss of possession varies with the nature of the offense. In a worst-case scenario, the most harmful party would take the information along with any and all copies with no recovery possible. Or a moderately harmful party could take it for a moderate period of time before it would be recovered at moderate cost. In the least harmful case, a harmless party would possess one copy of the information with timely recovery possible.

3 Conclusion

Some scenarios of losses that infosec should address require the use of all six elements of preservation to specify the se-



The New Foundation of Information Security

Preservation of {Availability, Utility, Integrity, Authenticity, Confidentiality, Posession} of information from accidental or intentional {Destruction, Interference, Use of false data, Modification of replacement, Misrepresentation of repudiation, Misuse or failure to use, Access, Observation or disclosure, Copying or stealing, Endangerment}

by {Avoidance, Deterrence, Prevention, Detection, Mitigation, Transference, Sanction, Recovery, Correction} to {Meet a standard of due care, Avoid loss, Reduce loss, Eliminate loss}

Currently Acceptable Foundation of Security

Preservation of {Confidentiality, Integrity, Availability} of information from {Disclosure, Modification, Destruction, Use}

by {Prevention, Detection, Recovery} to {Reduce loss, Reduce risk of loss}

Figure 1. Information security framework

curity to be applied. The six elements are independent of one another by having unique definitions, with one exception. The only possible definition of an element included within the definition of another is when loss of confidentiality results when loss of possession occurs, because a violation of confidentiality always results in at least a violation of loss of exclusive possession. Loss of exclusive or nonexclusive possession, however, does not necessarily result in loss of confidentiality, as seen in the above scenario of stealing information without examining it or when the information stolen is not confidential.

All six elements of infosec presented here must be used. This is essential if infosec is to be complete and accurately described. Moreover, to adequately reduce or eliminate vulnerabilities and threats, the use of all six elements is critical to ensure that nothing is overlooked in applying appropriate controls, such as those identified above. These elements also aid in identifying abusive actions that adversaries could take before the actions are realized. As technology advances, adversaries become more sophisticated, and as the concept and scope of infosec changes, more changes or additions to the six elements may be required.

All six elements can be paired into three double elements for simplification and ease of reference, and the order of presentation should have some meaning as well. Availability and utility fit together as the first element. Controls common to them include secure location, appropriate form for secure use, and accessibility of backup copies. Integrity and authenticity fit together-one concerned with internal structure and the other with value conformance with external facts or reality. Controls for both include double entry, reasonableness checks, use of sequence numbers and check sums or hash totals, and comparison testing. Control of change applies to both. Finally, confidentiality and possession go together since they are only partially independent, as previously stated. Commonly applied controls include copyright protection, cryptography, digital signatures, escrow, and secure storage. The order used here is logical since integrity and authenticity generally have value only if the information is available and useful, and confidentiality and possession have material meaning if the value of the information is sufficient because it has integrity and authenticity.

A summary of the complete framework of infosec is provided in Figure1. It includes the six elements of purpose, an abbreviated list of abusive acts, nine functions, and four goals.

References

1. D Parker. 'Restating the foundation of information security'. In *Proceedings of the 14th National Computer Security Conference*, (1991).

Appendix A

The following definitions are the relevant abstractions taken from *Webster's Third New International Dictionary*.

Security: Freedom from danger, fear, anxiety, care, uncertainty, doubt; basis for confidence; measures taken to ensure against surprise attack, espionage, observation, sabotage; protection against economic vicissitudes (old age guarantees); penal custody; resistance of a cryptogram to cryptanalysis usually measured by the time and effort needed to solve it.

Availability: Capable of use for the accomplishment of a purpose, immediately utilizable, accessible, may be obtained.

Utility: Useful, fitness for some purpose, capacity to satisfy human wants or desires.

Integrity: Unimpaired or unmarred condition; soundness; adherence to a code of moral, artistic or other values; the quality or state of being complete or undivided; material wholeness.

Authenticity: Quality of being authoritative, valid, true, real, genuine, worthy of acceptance or belief by reason of conformity to fact and reality.

Confidentiality: Quality or state of being private or secret; known only to a limited few.

Possession : Act or condition of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled.

Notes for Contributors

The prime purpose of the journal is to publish original research papers in the fields of Computer Science and Information Systems, as well as shorter technical research notes. However, non-refereed review and exploratory articles of interest to the journal's readers will be considered for publication under sections marked as Communications or Viewpoints. While English is the preferred language of the journal, papers in Afrikaans will also be accepted. Typed manuscripts for review should be submitted in triplicate to the editor.

Form of Manuscript

Manuscripts for *review* should be prepared according to the following guidelines.

- Use wide margins and $1\frac{1}{2}$ or double spacing.
- The first page should include:
  - title (as brief as possible);
  - author's initials and surname;
  - author's affiliation and address;
  - an abstract of less than 200 words;
  - an appropriate keyword list;
  - a list of relevant Computing Review Categories.
- Tables and figures should be numbered and titled.
- References should be listed at the end of the text in alphabetic order of the (first) author's surname, and should be cited in the text in square brackets [1–3]. References should take the form shown at the end of these notes.

Manuscripts accepted for publication should comply with the above guidelines (except for the spacing requirements), and may be provided in one of the following formats (listed in order of preference):

1. As (a) LaTeX file(s), either on a diskette, or via e-mail/ftp – a LaTeX style file is available from the production editor;
2. As an ASCII file accompanied by a hard-copy showing formatting intentions:
   - Tables and figures should be original line drawings/printouts, (not photocopies) on separate sheets of paper, clearly numbered on the back and ready for cutting and pasting. Figure titles should appear in the text where the figures are to be placed.
   - Mathematical and other symbols may be either handwritten or typed. Greek letters and unusual symbols should be identified in the margin, if they are not clear in the text.

   Contact the production editor for markup instructions.
3. In exceptional cases camera-ready format may be accepted – a detailed page specification is available from the production editor;

Authors of accepted papers will be required to sign a copyright transfer form.

Charges

Charges per final page will be levied on papers accepted for publication. They will be scaled to reflect typesetting, reproduction and other costs. Currently, the minimum rate is R30-00 per final page for LaTeX or camera-ready contributions that require no further attention. The maximum is R120-00 per page (charges include VAT).

These charges may be waived upon request of the author and at the discretion of the editor.

Proofs

Proofs of accepted papers in category 2 above may be sent to the author to ensure that typesetting is correct, and not for addition of new material or major amendments to the text. Corrected proofs should be returned to the production editor within three days.

Note that, in the case of camera-ready submissions, it is the author's responsibility to ensure that such submissions are error-free. Camera-ready submissions will only be accepted if they are in strict accordance with the detailed guidelines.

Letters and Communications

Letters to the editor are welcomed. They should be signed, and should be limited to less than about 500 words.

Announcements and communications of interest to the readership will be considered for publication in a separate section of the journal. Communications may also reflect minor research contributions. However, such communications will not be refereed and will not be deemed as fully-fledged publications for state subsidy purposes.

Book reviews

Contributions in this regard will be welcomed. Views and opinions expressed in such reviews should, however, be regarded as those of the reviewer alone.

Advertisement

Placement of advertisements at R1000-00 per full page per issue and R500-00 per half page per issue will be considered. These charges exclude specialized production costs which will be borne by the advertiser. Enquiries should be directed to the editor.

References

1. E Ashcroft and Z Manna. 'The translation of 'goto' programs to 'while' programs'. In *Proceedings of IFIP Congress 71*, pp. 250–255, Amsterdam, (1972). North-Holland.
2. C Bohm and G Jacopini. 'Flow diagrams, turing machines and languages with only two formation rules'. *Communications of the ACM*, **9**:366–371, (1966).
3. S Ginsburg. *Mathematical theory of context free languages*. McGraw Hill, New York, 1966.

South African
Computer
Journal

Number 17, September 1996
ISSN 1015-7999

Suid-Afrikaanse
Rekenaar-
tydskrif

Nommer 17, September 1996
ISSN 1015-7999

Contents

GUEST EDITORIAL

SPECIAL EDITION: COMPUTER SECURITY

Drukkers
Printers