December 1997

Layered Protection of Availability

Jussipekka Leiwo
Monash University

Yuliang Zheng
Monash University

Layered Protection of Availability

Jussipekka Leiwo and Yuliang Zheng
Peninsula School of Computing and Information Technology
Monash University, McMahons Road, Frankston, Vic 3199, AUSTRALIA
Tel. +61-(0)3-9904 4287, Fax +61-(0)3-9904 4124
E-mail: {skylark,yuliang}@fcit.monash.edu.au

Executive summary
Availability is far less understood than other two general objectives of information security, confidentiality and integrity. To bridge this cap, a layered protection framework for availability shall be established. Protection measures are classified into three layers, and characteristics of threats and countermeasures shall be studied in detail at each layer. The rough classification of layers is into technical measures, administrative measures, and external measures. This classification shall be also used to establish the scope of protection. Restriction of the scope of availability is essential, since even though availability depends on several types of protection measures like physical security, not all of them should be considered as actual information security measures.

As the cost-effectiveness is the major concern of adequate information security management, a method to estimate the cost of availability shall be established. Violation of availability shall be considered as realisation of any intentional or accidental threat that causes an unacceptable long delay to an authorised access to information or service. Availability requirements shall be seen as specification of acceptable response times in normal circumstances, under a minor violation, and when a major violation has occurred. A notation shall be given to the acceptable response time policy, where availability requirements are formally specified. These requirements shall be aligned with results of risk analysis to support specification of protection measures.

The major goal of this paper is to clarify the research on availability and to identify components that influence the protection from service provision, security management, and technical point of view. Once the layered protection is established, future research may be carried on at several areas, either on layer specific topics or to establish links for protection between layers. For comprehensive understanding of the problem of availability, measures are required at each layer, and integration of measures at different layers emerges. Being less understood than confidentiality or integrity does not mean being valuable. Cases can be identified where availability becomes the major requirement of systems. To provide protection in such cases, a comprehensive approach becomes essential.

1 Introduction

Availability has typically been considered as protection against denial of service attacks, where an authorised entity is illegally prevented from accessing information or processing service. From a wider point of view, availability can be considered as protection of information and processing services against different threats to satisfy each authorised request without delay. Due to the nature and number of threats against availability, wide scope causes problems. Since it is not possible to identify all threats against availability, question has been raised of availability being an adequate objective of information security (Bailey 1995). The problem has been approached by studying sub concepts of availability, like utility (Parker 1992) and operability (Keus and Ullman 1994), separately or by restricting the concept into prevention of illegal allocation of resources (Millen 1992). A wide point of view shall be taken in this paper, and a comprehensive framework for the protection of availability at several layers shall be established. The framework consists of identification of threats and their countermeasures, specification of an acceptable response time policy, and justification of the cost of protection.

Other general objectives of information security are better understood than availability, and several formal models exist to protect confidentiality (Bell and LaPadula 1974; Bell 1988; Brewer and Nash 1989; Denning 1976; Harrison, Ruzzo and Ullman 1976) and integrity (Biba 1977; Clark and Wilson 1987). Availability is an important objective, since cases can be identified where major threat is denial of service. For example, integrity and confidentiality within the burglar alarm system are minor

requirements, whereas availability of service is the critical factor (Needham 1994). As analysed by Reed (Reed 1992), even short interrupts in information processing services cause serious problems for most organisations. Recent examples of commonly known violations of availability are TCP SYN Flooding (CERT CA-96.21) and TCP/IP ping attacks (CERT CA-96.26). From the dependable computing point of view, availability becomes even more important. Dependability can be seen as protection of four attributes of systems: availability, reliability, safety and security. Availability is a common objective for each system, but the need for reliability, safety and security varies according to the application (Laprie 1992).

Availability has also not been addressed by different security evaluation criteria. European Information Technology Security Evaluation Criteria (ITSEC) sets a requirement of continuity-of-service, but the Canadian CTCPEC has availability as an empty mark holder. In 1985 DoD Workshop on Network security (DoD Computer Security Center Invitational Workshop on Network Security 1985) concluded that no generic, mission independent, denial-of-service conditions can be identified. In the 1990 CTCPEC workshop on availability (CTCPEC Availability Workshop 1990) concluded that difference should be made between loss of availability due to malicious actions by a user, for example Trojan horse, and random failures affecting the functionality.

The problem of availability is here approached by dividing threats and countermeasures into three layers. On the highest level of proposed hierarchy, protection measure against external and accidental threats is transformation of responsibility by signing service provision agreements with external parties. These parties take the responsibility of providing continuous service, for example electricity or data communication service, with a specified cost to the organisation. On the organisational level, administrative routines are considered an effective measure for recovering and correcting, or to reduce the probability of any type of violation of availability. On the technical layer, where threats are logical attacks against the system, not many formal models have been suggested. Recommendations of (Keus 1994) and (Keus and Ullman 1994) also focus on corrective rather than preventive actions. Technical measures must enforce a maximum waiting time policy (Gligor 1983), where each process is attached with a maximum acceptable delay until termination. Millen (1992) has proposed a Denial-of-Service Protection Base (DPB) to enforce acceptable response times within the Trusted Computing Base (TCB).

Before studying different layers in detail, the nature of threats against availability and their countermeasures shall be studied in section 2. Once threats and countermeasures have been identified, different layers shall be studied in detail in section 3. Considering the layered approach, a method to estimate the cost of protection and to align the cost with risks shall be established in section 4. Finally, conclusions shall be drawn and directions for future work summarised in section 5.

2 Threats and countermeasures

Strength of protection measures against violations of availability is not as predictable as that of integrity and confidentiality. Protection of integrity and confidentiality can be estimated and the complexity of breaking the protection calculated. If, for example, confidentiality of information is enforced by encryption, the effect of different encryption schemes and key lengths can be approximated and the most cost-effective method can be chosen. Since violations of availability can originate from an uncontrolled amount of sources, it is not easy to say whether the result of not having violations is the result of protection measures or lack of violation attempts. Therefore, objectives for availability must be slightly different from those of confidentiality and integrity.

Protection of availability shall be seen as protection against any threat that may cause an authorised request to any service or information fail. Failure here refers to an unacceptable long access time. Most important classifications of threats within this paper are those into intentional and accidental (ISO7498-2 1988), internal and external (Simonds 1996), active and passive (ISO7498-2 1988), semantic and syntactic McDermid and Shi 1991), threats through resource allocation and threats through resource destruction (Millen 1992), and to threats caused by human or physical causes (Keus and Ullman 1994). These types shall be described, and examples of each shall be given in table 1. Since the definition of availability is very broad, not all individual threats can be identified (Bailey 1995), and only types of threats can be analysed. A new classification into three shall be established. Threats at the lowest level, technical threats, are mostly threats by resource allocation, and upper level threats

are threats through resource destruction. Technical threats are typically intentional attacks against system, whereas type of higher level threats varies. Characteristics of threats are as follows.

External threats are those that are out of the direct control of organisation. For example, communication services are usually leased from external service providers. Therefore, even if the organisation is dependent on the availability of these services, in the case of violation, all corrective action must be taken by the service provider. Typical examples are different external and accidental threats, like acts of God, floods and falling trees.

Administrative threats can be covered by proper administrative routines. The nature of these threats varies significantly, for example, loss of information due to system failures and accidental loss of files. Administrative routines like proper backup routines, file system duplication, and physical security are adequate measures to minimise the impact of these threats.

Technical threats can be considered as intentional violations of availability, that is denial of service attacks, and originate mostly from internal sources. This is where the lack of formal protection models emerges. Availability is usually considered as an enforcement of finite response time policy, where the protection model should guarantee that systems provide the user with a response in a given maximum waiting time.

Table 1 Characteristics of major types of threats

Threat	*Characteristics*	*Example*
Intentional	Intentional attempt to harm the system	Any planned attack
Accidental	Accidental harming of the system	Accidental removal of a file
Internal	Originates from an internal source	Exceeding of authorisation
External	Originates from outside the system	System intrusion
Active	Changes the state of the system	Alteration of data
Passive	Does not alter the state of the system	Wire tapping for disclosure
Semantic	Violates the spirit of security policy	Exploiting of a flaw in policy design
Syntactic	Violates the letter of security policy	Breaking the policy
Allocation	Improper allocation of resources	Exceeding of authorisation
Destruction	Destruction of resources	Removal of a file
Human	Originates from human causes	Any intentional attack
Physical	Originates from non-human causes	Floods, storms, falling trees, etc.

These threats can be further divided into subclasses, and different types of protection measures can be specified for each layer. In the remaining of this paper, the classification shall be followed where technical protection measures are divided on three and administrative measures into two. Technical measures shall include allocation of hardware (HW) resources to guarantee that system resources are adequate to satisfy the response time policy. On top of HW is the resource allocation by operating system (OS). HW resources must have suitable OS level schemes to guarantee effective and fair allocation. Third component of technical layer is the actual TCB, where the protection is enforced. As HW design and planning and OS design are usually not considered as parts of information security, the focus on technical measures within this paper shall be on TCB level.

Administrative layer shall be divided into two: physical and procedural threats. Physical threats are intentional or accidental violations of availability of information or services by resource destruction. Physical protection measures include, for example, structural protection of computer centers and traffic monitoring. The scope of protection is widened from technical threats to cover also physical attacks and accidental violation of availability of both systems and services. Risks of physical attacks can be reduced by good physical security, that requires adequate administration and administrative procedures including, for example, backup practices and file or device duplication. As physical security is usually not within the scope of information security, it shall not be further studied within this paper.

Proper administrative routines also reduce the risk of threats that are semantic but not syntactic. As information security management and administration is responsible for controlling effectiveness, correctness and consistency of security policies, proper administration can reduce the risk of being susceptible for such threats. Procedural protection measures are most effective after a violation has occurred, and recovery and correction are required. Another significant feature is, that these measures

protect only information and services that can be controlled by the organisations. To protect also services that are external from the organisation, different service delivery agreements with external parties are to control the provision of services and to specify rights and responsibilities in the case of violations.

As the fundamental goal of availability is to guarantee acceptable response times in all circumstances, violations can also be classified into layers according to the severity. Lower layers of protection measures are needed to provide normal circumstances, that is prevention of violations, whereas administrative and external layers are needed mostly to recover from a violation that has already occurred. To match violations with types of threats, as illustrated in figure 1, the assumption shall be made, that the more severe the violation, the higher level measures are needed for recovery, and the more the acceptable response time must increase.

At the top levels, where the actual correction is carried out in the case of a violation, required measures can be further divided into automated and manual controls. Violations of lesser severity can be recovered using automated measures, whereas more severe violations require manual correction. For example, in the case of a disk crash, automated actions may be taken to switch into a duplicate of the disk, or to recover the disk from parity disks. Other possibility is to manually install a new disk and return the information from back up tapes. The justification of the chosen method should be the cost of protection, as shall be analysed in section 4.

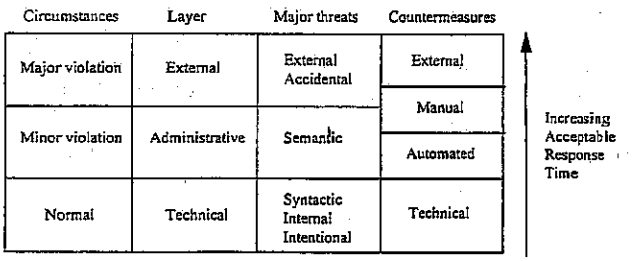

Figure 1 Violations of availability

3 Layers of protection

In this section, each layer of protection, as identified in section 2, shall be studied in detail. Different layers, threats and protection methods are summarised in table 2. It should be noted that external controls are only modified by contracts with service providers. Therefore, only administrative layers, physical and procedural protection, are where the question of automated and manual controls is required. Any measure can be automated or left manual and the cost may be very different. The final should be based on cost of protection and value of information or service. A method to estimate cost of protection and to align that cost with risks shall be provided in section 4.

Table 2 Layered protection of availability

Layer	*Threats*	*Protection methods*
HW	Inadequate HW resources	HW planning
OS	Improper resource allocation	Resource allocation algorithms
TCB	Logical attacks, malicious SW	DPB
Physical	Physical attacks	Physical security
Procedural	Intentional and accidental losses of information and services	Administrative procedures
External	Threats outside of the direct control of the organisation	Inspections and Contracts

3.1 External protection measures

Controls to protect against violations of availability on the large scale are not only internal to the system or organisation. As identified by Baskerville (1988), also external controls are required. Internal and external measures are relative to the level of protection to be established. Under normal circumstances, external controls refer to the administrative controls to support that operation, whereas when a violation has occurred, internal controls refer to detection, correction, and recovery by administrative procedures, and external controls to actions taken outside the organisation.

Protection measures apart from the organisations control can only be affected by inspection of service providers and by contracts that set responsibilities and rights of each party in the case of a violation. For example, most of the organisations lease their WAN solutions from telecommunications or other network operators. In the case of external and accidental threats, the organisation can only assume that the system is recovered within an acceptable time, specified in the contract. Client organisation transfers the responsibility of operation to the third party, and agrees with service continuity on a specified cost. Proper inspection of procedures of the service provider before signing the contract can be used to reduce the risk of incontinuity of service. Service provision agreements should specify all arrangements and resources that the external service provider allocates to guarantee continuity of service according to the client requirements. The establishment and operation of Trusted Third Parties (TTP) shall not be studied within this paper. Details can be found, for example, from (Green Book, 1993).

3.2 Administrative protection measures

On the large scale, major protection measures against violations of availability include proper backup practices, good access control, multiple naming of files, specific utility programs, and shadowed or mirrored files (Parker 1992). The drawback of these measures is, that they easily lead to the loss of integrity of information due to, for example, different versions of a file being stored by different names. Another important feature is also that administrative procedures can not prevent violations unless supported by technical measures. Procedural protection measures listed above do not remove threats but do significantly reduce the risk of service becoming unavailable. For example, redundant arrays of inexpensive disks (RAID) technology employing ten disks, of which two are for parity control, can reduce the mean time to data loss (MTDL) compared to large disks from 2-3 years to 90 years (Silberschatz and Galvin 1994, p.422-424).

Procedural measures can reduce the severity of a violation, that is the loss caused by realisation of a specific risk, but prevention is more complex. Therefore, procedural layer protection of availability must rather focus on recovery and correction than on prevention. A feasible requirement could be, for example, that if a file on a given level of importance is lost, backups should not be older than 24 hours. Of course, the question can be transformed to the protection of those backup files and stores.

The major difference between administrative and technical measures is that administrative measures are carried out when a violation has occurred or to prepare to those actions, whereas technical measures focus on prevention of violations. Typical measures are intended to maintain the information or service, so once a violation has occurred, the cost of recovery and correction can be reduced. Keus and Ullman (1994) have specified seven security functions for availability: error recognition; failure correction; fault removal; resource checking; maintenance, exchange and reconfiguration during operation; audit trailing; and auditing. The important observation is the focus on administrative functions that take place after a violation has occurred. Only fault removal and resource checking are clearly preventative functions.

3.3 Technical protection measures

As high level definitions of availability (eg. ISO7498-2 1988; Muftic et al. 1994) definitions of availability are very broad, a more narrow approach must be taken to enable formal protection models. As shown by Harrison, Ruzzo and Ullman (1976), access control list (ACL) based prevention of denial of service is an undecidable problem and a different approach is required. From the technical point of view, an assumption is made that data is available if the response to an authorised request is provided within a given time constraint (Gligor 1983). This approach has lead to the identification of a key concept within this section, a Denial-of-service Protection Base (DPB) (Millen 1992). DPB enforces an acceptable resource allocation rather than resource access scheme. Violation of availability can be seen as an undesirable event that results in an unacceptable long response time of an access to any resource.

Availability of data communications networks is usually provided by a combination of standard security services, integrity, confidentiality, authenticity and access control (Needham 1994). The attacks can target, and therefore protection measures must address, servers, network itself, or client. Major attack on server is the unauthorised modification of software, that is loss of integrity of server. Unauthorised changes may cause the server to deny access of an authorised client. Attacks on the network can be classified into three: denial of transmitting messages, sending of falsified messages, and message flooding. Attacks on the client include destruction and substitution.

4 Cost of protection

In this section, the cost of layered protection of availability shall be analysed with a comparison to the value of information. First, a formal notation for a high level response time policy shall be given in section 4.1. After this, the cost of protection shall be estimated in section 4.2. Once the cost has been estimated, it can be aligned with the protection requirements and risks, as studied in section 4.3.

4.1 Layered availability requirements

When preparing to the abnormal circumstances, acceptable response time policy should be prepared regarding the severity of violations. Assume the set $A = \{a_i\}$ to be assets (information and services) to be protected. The specification of acceptable response time for each asset $a_i \in A$ is $T_i = \{t_i, t_2, t_3\}$ where each t_j represents an acceptable time in the case of different severity violation, where t_1 represents requirement in normal circumstances, t_2 in the case of minor violations, and t_3 in the case of major violation.

To meet the multilevel security (MLS) requirements, assets shall be classified into priority classes. Let $CL = \{\lambda_i, \lambda_2, \cdots, \lambda_l\}$ be a set of unique priorities. Uniqueness means, that no classes are overlapping, formally it must be that $\forall i, j \le l, \forall a \in A(a \in \lambda_i \wedge a \in \lambda_j) \rightarrow i = j$. Considering these definitions, the acceptable response time policy *P* shall be specified in equation 1. For the policy to make sense, it should be that $\forall i \le n: t_{i,1} \le t_{i,2} \le t_{i,3}$ and for classification to make sense, it should be that $\forall 1 < i \le n, j = 1,2,3: t_{i,j} < t_{i-1,j}$.

$$P = \{(\lambda_1, T_1), (\lambda_2, T_2), \ldots, (\lambda_l, T_l)\} \quad (1)$$

4.2 Cost estimation

To align the cost of protection with the value of information, the cost of protection must be analysed at each layer. It shall also be shown how the total cost of availability depends on the cost of protection at different layers. The scope of availability shall be as specified in section 2. The two fundamental assumptions shall be made:

1. Higher layer actions will cause more costs than those of lower layers.
2. Values of information and services and probabilities of realisation of different threats can be estimated.
3.

The cost of technical layer shall be specified in equation 2. Assume, that on a given interval *t*, there will be *n* access requests, and the total processing overhead required to enforce the resource allocation policy shall be composed of cost of policy consultation C_c^i and policy enforcement C_e^i of asset *i*, and the cost of requests denied C_d. C_d can be specified as $C_d = \sum_{m=1}^{D} c_m$ where *D* is the number of requests denied during the consideration interval, and c_m is the cost of denial of request *m*.

$$C_{tech} = C_d + \sum_{k=1}^{n} (C_c^k + C_e^k) \quad (2)$$

For the automated controls, assume that there are *I* duplicate components, denoted as D_i where $i = 1,2,\ldots,I$. The cost of duplication includes the cost of components and the cost of their operation. Let C_i^{dc} refer to the cost of a duplicate component D_i, and C_i^{do} to the operational cost of this component. Other costs originate from cost of detection of a corruption C_i^{de} and recovery costs of the duplicate C_i^{re}.

The total expected cost of automated action is specified in equation 3, where the cost of duplications is multiplied with the failing probabilities of components. Assume that each component D_i has a failure probability p_i.

$$C_{Automated} = \sum_{k=1}^{J} C_k^{dc} + C_k^{do} + p_k \times (C_k^{de} + C_k^{re}) \quad (3)$$

The cost of manual actions C_{Manual} can be calculated equally to equation 3. Cost of protection can be justified by the comparison of the estimates of different costs of actions. Higher level availability policies may, anyhow, prevent the most desirable solution, if required performance can not be guaranteed. Similarly, in the case of external threat, the cost of protection becomes the cost of a contract C_{co} and the cost of expected violation, that can be calculated as the probability and severity of an interrupt in service, as specified in equation 4.

$$C_{External} = C_{co} + \sum_{k=1}^{J} p_i \times C_{Int} \quad (4)$$

Total cost of protection can be calculated as in equation 5. Because each component includes the alignment of the severity and probability of a violation, summing the components is adequate.

$$C_{Total} = C_{Tech} + C_{Automated} + C_{manual} + C_{External} \quad (5)$$

4.3 Alignment of risks and cost of protection

Assume, that the results *R* of risk analysis can be organised into triples $R = \{(a, \rho, \sigma)\}$, where the interpretation can be given where the loss of asset *a*, with severity σ is of value ρ. As specified in equation 1, availability requirements (availability policy) can be specified as pairs $P = (\{\lambda, T)\}$ where each *T* is a triple (t_1, t_2, t_3). Preliminary weighted assets *WA* can be organised according the severity and cost of violations as in equation 6.

$$WA = \{(a \in A, \rho_a \in R, C_{Total}, \sigma, \lambda, t_\lambda, C_\lambda)\} \; where \; \sigma = \lambda \quad (6)$$

Considering *WA*, an acceptable set of protection measures *WA'* can be specified by selecting feasible alternatives from *WA*, as illustrated in equation 7. Only those instances of *WA* where either the total cost of protection is lower than total costs, or cost of protection at a given layer λ is lower than value of information are selected.

$$WA' = \{(a \in A, \rho_a \in R, C_{Total}, \sigma, \lambda, t_\lambda, C_\lambda) \; where \; (\rho_a \le C_{Total}) \wedge (t_\lambda \le C_\lambda)\} \quad (7)$$

As each cost is known, different protection options can be compared by altering parameters (that is modeling different protection options) in above equations to find the optimal alternative for protection without violating the availability policy. This can be done by finding the option, where the difference between value of information and cost of protection on a given layer λ, $t_\lambda - C_\lambda$ is at the maximum.

5 Conclusions and future work

A calculation to estimate the cost of protection of availability at several layers, and to justify that cost regarding the value of information and acceptable response time policy has been established. As definitions of availability are much broader than those of confidentiality and integrity, it is important to study measures to protect and understand availability at several layers. The major strength of the layered approach is consideration of several sources of information security requirements and support of specification of responsibilities at different organisational layers. In real life, anyhow, violations may not be categorised as simply as the model suggests. Large scale attacks usually involve authorised users misusing their authorisations to enable themselves or an external attacker to harm the system. Attack may then exploit a flaw in the system or protection at technical level, a flaw in security procedures, or at external connections. Therefore, each layer should not be considered separate, but adequate protection should cover all the layers.

Wide spread denial of service attacks on the Internet, such as SYN flooding and TCP ping attack, have recently raised serious concerns about denial of service. As a system is as strong as its weakest

link, it is essential to continue research to balance understanding of different facets of availability. This is difficult, since the difference between denial of service attack and any other accidental event that leads to denial of service is very small. In public networks the problem becomes even more difficult. Internet routing algorithms, for example, are very sophisticated in balancing traffic and optimising routes. Their design has, anyhow, followed some assumptions about the amount of traffic. If the routing function is temporarily unavailable due to excessive traffic, that is the situation where the work load is not according to the assumptions and specifications, it is not clear whether this is due to improper design, implementation or operation, or due to a denial of service attack, or accidental exceeding of acceptable traffic. The HW capacity constraints and user requirements should be balanced, and operation under abnormal circumstances, where the system load is not according to specifications, should be planned. Cost of protection, that is preparation into abnormal circumstances, is controlled denial of requests. Cost of protection is denial of suspicious requests. This may lead to user unsatisfaction, but so would excessive response times. Which option is more desirable, should be specified according to cost analysis.

On the higher level, the lack of preventive measures raises several questions for future research. The fundamental question remains, what can be done on high levels to prevent attacks, or are only indirect measures applicable. For example, reduction of likelihood of attacks by deterrence and physical security is a typical indirect preventive method. The method itself does not directly prevent attacks but reduces the temptation of potential perpetrators to attack the system. All these components are essential facets of the detailed understanding of availability, and are therefore required for the establishment of comprehensive protection.

References

Bailey, D. A Philosophy of Security Management. In M.D. Abrams, S. Jajodia and H.J. Podell, editors, *Information Security - An Integrated Collection of Esseys*. IEEE Computer Society Press, Los Alamitos, CA, USA, 1995.

Baskerville, R. *Designing Information Systems Security*. John Wiley & Sons, 1988.

Bell, D.E. and LaPadula, L.J. *Secure Computer Systems: Mathematical Foundations and Model*. Technical Report M74-244, MITRE Corporation, Bedford, MA, USA, 1974.

Bell, D.E. Concerning "Modeling" of Computer Security. In *Proceedings of the 1988 IEEE Symposium on Research on Security and Privacy*, 1988.

Biba, K. *Integrity Considerations for Security Computer Systems*. Technical Report TR-3153, MITRE Corporation, Bedford, MA, USA, 1977.

Brewer, D. and Nash, M. The Chinese Wall Security Policy. In *Proceedings of the 1989 IEEE Symposium on Research on Security and Privacy*, 1989.

Clark, D.D. and Wilson, D.R. A Comparison of Commercial and Military Security Policies. In *Proceedings of the 1987 IEEE Symposium on Research on Security and Privacy*, 1987.

Communications Security Establishment, Government of Canada. *Proceedings of the 1990 CTCPEC Availability Workshop*, February 6-7, 1990.

Computer Emergency Response Team (CERT) Advisory CA-96.21. *TCP SYN flooding and IP spoofing attacks*. September 1996. Available at ftp://ftp.info.cert. org/pub/cert_advisories/CA-96.21.tcp_syn_flooding.

Computer Emergency Response Team (CERT) Advisory CA-96.26. *Denial of service attack via ping*. December 1996. Available at ftp://ftp.info.cert.org /pub/cert_advisories/CA-96.26.ping.

Denning, D.E. A Lattice model for Secure Information Flow. *Communications of the ACM*, Volume 19, Number 5, PP. 236-243, May 1976.

Gligor, V. A Note on the Denial-of-Service Problem. In *Proceedings of the 1983 IEEE Symposium on Research on Security and Privacy*, 1983.

Harrison, M., Ruzzo W. and Ullman, J. Protection in Operating Systems. *Communications of the ACM*, Volume 19, Number 8, PP. 461-471, 1976.

Information Technology Security Evaluation Criteria (ITSEC). Provisional Harmonized Criteria, Version 1.2. Commission of the European Communities COM(92) 298 Final, Brussels, Belgium, September, 1992.

International Standard ISO 7498-2. Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1988.

Keus, K.J. and Ullman, M. Availability: Theory and Fundamentals for Practical Evaluation and Use. In *Proceedings of the 10th Annual Computer Security Applications Conference*, 1994.

Keus, K.J. Availability: A Central and Up-to-Date user Requirement in IT Security. In *Proceedings of the 10th Annual Computer Security Applications Conference*, 1994.

Laprie, J.C. (Ed.) Dependability: Basic Concepts and Terminology. Springer-Werlag, Vienna, Austria, 1992.

McDermid, J. and Shi, Q. A Formal Model of Security Dependencies for Analysis and Testing of Secure Systems. In *Proceedings of the Computer Security Foundations Workshop IV*, 1991.

Millen, J.K. A Resource Allocation Model for Denial of Service. In *Proceedings of the 1992 IEEE Symposium on Research on Security and Privacy*, 1992.

Muftic, S. ,Patel, A., Sanders, P., Colon, R., Heijnsdijk, J. and Pulkkinen, U. *Security Architecture for Open Distributed Systems*. John Wiley & Sons, 1994.
Needham ,R.M. (1994). Denial of Service: An Example. *Communications of the ACM*, Volume 37, Number 11, November 1994, PP. 42-46, 1994.
Parker, D .B. Restating the Foundation of Information Security. In *Proceedings of the IFIP TC11 8th International Conference on Information Security*, 1992.
Proceedings of the Department of Defence Computer Security Center Invitational Workshop on Network Security. New Orleans, LA, USA, March 19-22 1985.
Reed, A. Computer Disaster: The Impact on Business in the 1990s. In *Proceedings of the IFIP TC11 8th International Conference on Information Security*, 1992.
Silberschatz, A. and Galvin, P. *Operating System Concepts*. Addison-Wesley, 4th Edition, 1994.
Simonds, F. *Network Security: Data and Voice Communications*. McGraw-Hill, 1996.