INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL

Capt John R. McCumber
Joint Staff/J6K
The Pentagon
Washington, DC 20318-6000

INTRODUCTION

At speech to the 13th National Computer Security Conference on 3 October 1990, Michelle VanCleave, Assistant Director for National Security Affairs, Executive Office of the President stated, "We need a comprehensive model for understanding the threat to our automated information systems." I believe I have developed that model. This model not only addresses the threat, it functions as an assessment, systems development, and evaluation tool. The model is unique in that it stands independent of technology. Its application is universal and is not constrained by organizational differences. As with all well-defined fundamental concepts, it is unnecessary to alter the premise even as technology and human understanding evolve.

Computers communicate. Communication systems compute. The evolution of technology has long since eliminated any arbitrary distinction between a computer and its communication components or a communications network and its computing system. Some organizations have attempted to deal with the phenomenon by marrying these functions under common leadership. This has resulted in hyphenated job descriptions such as Computer-Communications Systems Staff Officer and names like Information Technology Group. Unfortunately, these names can mask an inappropriate or poorly executed realignment of organizational responsibilities. Ideally, management will recognize there is a theoretical-as well as organizational-impact.

The same is true for the security disciplines. Merely combining the communications security (COMSEC) and computer security (COMPUSEC) disciplines under an umbrella of common management is unacceptable. Even if we address the other, albeit less technical, aspects of information systems security such as policy, administration, and personnel security, we still fail to develop a comprehensive view of this evolving technology. The reason for this becomes clear when we are reminded it's the information that is the cornerstone of information systems security. In this sense, any paradigm which emphasizes the technology at the expense of information will be lacking.

THE NATURE OF INFORMATION

Defining the nature of information could be a tedious task. To some it represents the free-flowing evolution of knowledge; to others, it is intelligence to be guarded. Add to this the innumerable media through which information is perceived and we have a confusing array of contradictions. How can we present a study of information that has universal application?

It may be best to develop a simple analogy. The chemical compound H_2O means many things to all of us. In its liquid state, water means life-giving sustenance to a desert-dwelling Bedouin; to a drowning victim, it is the vehicle of death. The same steam we use to prepare vegetables can scald an unwary cook. Ice can impede river-borne commerce on the Mississippi River or make a drink more palatable. Science, therefore, does not deal with the perception of the compound, but with its state.

As the compound H_2O can be water, ice, or steam, information has three basic states which I've already depicted. At any given moment, information is being transmitted, stored, or processed. The three states exist irrespective of the media in which information resides. This subtle distinction ultimately allows us to encompass all information systems technology in our model.

It is possible to look at the three states in microcosm and say that processing is simply specialized state combinations of storage and transfer; so, in fact, there are only two possible states. By delving to this level of abstraction, however, we go beyond the scope and purpose of the model. The distinction between the three states is fundamental and necessary to accurately apply the model. For example, cryptography can be used to protect information while it's transferred through a computer network and even while it is stored in magnetic media. However, the information must be available in plaintext (at least to the processor) in order for the computer to perform the processing function. The processing function is a fundamental state which requires specific security controls.

When this information is needed to make a decision, the end user may not be aware of the number of state changes effected. The primary concern will be certain characteristics of the information. These characteristics are intrinsic and define the security-relevant qualities of the information. As such, they are the next major building block of our information systems security model.

CRITICAL INFORMATION CHARACTERISTICS

Information systems security concerns itself with the maintenance of three critical characteristics of information: confidentiality (Pfleeger's "secrecy"), integrity, and availability [PFL89]. These attributes of information represent the full spectrum of security concerns in an automated environment. They are applicable for any organization irrespective of its philosophical outlook on sharing information.

CONFIDENTIALITY

Confidentiality is the heart of any security policy for an information system. A security policy is the set of rules that, given identified subjects and objects, determines whether a given subject can gain access to a specific object [DOD85]. In the case of discretionary access controls, selected users (or groups) are controlled as to which data they may access. Confidentiality is then the assurance that access controls are enforced. The reason

I prefer the term confidentiality to secrecy is merely to avoid unwarranted implications that this is solely the domain of armies and governments. As we will see, it is a desirable attribute for information in any organization.

All organizations have a requirement to protect certain information. Even owners of a clearinghouse operation or electronic bulletin need the ability to prevent unwanted access to supervisory functions within their system. It's also important to note the definition of data which must be protected with confidentiality controls is broadening throughout government [OTA87]. Actual information labeling and need-to-know imperatives are aspects of the system security policy which are enforced to meet confidentiality objectives. The issue of military versus civilian security controls is one which need not impact the development of a comprehensive representation of information systems security principles.

INTEGRITY

Integrity is perhaps the most complex and misunderstood characteristic of information. As I stated, we seem to have a better foundation in the development of confidentiality controls than those which can help insure data integrity. Pfleeger defines integrity as "assets (which) can only be modified by authorized parties" [PFL89]. Such a definition unnecessarily confines the concept to one of access control.

I propose a much broader definition. Data integrity is a matter of degree (as is the concept of "trust" as applied to trusted systems) which has to be defined as a quality of the information and not as who does/does not have access to it. Integrity is that quality of information which identifies how closely the data represent reality. How closely does your resume reflect "you"? Does a credit report accurately reflect the individual's historical record of financial transactions? The definition of integrity must include the broad scope of accuracy, relevancy, and completeness.

Data integrity calls for a comprehensive set of aids to promote accuracy and completeness as well as security. This is not to say that too much information can't be a problem. Data redundancy and unnecessary records present a variety of challenges to system implementors and administrators. The users must define their needs in terms of the information necessary to perform certain functions. Information systems security functions help insure this information is robust and (to the degree necessary) reflects the reality it is meant to represent.

AVAILABILITY

Availability is a coequal characteristic with confidentiality and integrity. This vital aspect of security insures the information is provided to authorized users when it's requested or needed. Often it's viewed as a less technical requirement which is satisfied by redundancies within the information system such as back-up power, spare data channels, and parallel data bases. This perception,

however, ignores one of the most valuable aspects of our model which this characteristic provides. Availability is the check-and-balance constraint on our model. Because security and utility often conflict, the science of information systems security is also a study of subtle compromises.

As well as insuring system reliability, availability acts as a metric for determining the extent of information system security breaches [DOJ88]. Ultimately, when information systems security preventive measures fail, remedial action may be necessary. This remedial activity normally involves support form law enforcement or legal departments. In order to pursue formal action against people who abuse information systems resources, the ability to prove an adverse impact often hinges on the issue of denying someone the availability of information resources. Although violations of information confidentiality and integrity can be potentially more disastrous, denial of service criteria tend to be easier to quantify and thus create a tangible foundation for taking action against violators [CHR90].

The triad of critical information characteristics covers all aspects of security-relevant activity within the information system. By building a matrix with the information states positioned along the horizontal axis and the critical information characteristics aligned down the vertical, we have the foundation for the model.

SECURITY MEASURES

We've now outlined a matrix which provides us with the theoretical basis for our model. What it lacks at this stage is a view of the measures we employ to insure the critical information characteristics are maintained while information resides in or moves between states. It's possible, at this point, to perceive the chart as a checklist. At a very high level of abstraction, one could assess the security posture of a system by using this approach. By viewing the interstices of the matrix as a system vulnerability, you can attempt to determine the security aspects of an information system as categorized by the nine intersection areas. For example, you may single out systems information confidentiality during transmission or any intersection area for scrutiny.

The two-dimensional matrix also has another less obvious utility. We can map various security technologies into the nine interstices. Using our example from above, we note it is necessary to protect the confidentiality of the information during its transmission state. We can then determine which security technologies help insure confidentiality during transmission of the information. In this case, cryptography would be considered a primary security technology. We can then place various cryptographic techniques and products within a subset in this category. Then we repeat the process with other major types of technology which can be placed within this interstice. The procedure is repeated for all nine blocks on our grid. Thus we form the first of three layers which will become the third dimension of our model-security measures.

TECHNOLOGY

The technology layer will be the primary focus of the third dimension. We will see that it provides the basis for the other two layers. For our purposes, we can define technology as any physical device or technique implemented in physical form which is specifically used to help insure the critical information characteristics are maintained through any of the information states. Technology can be implemented in hardware, firmware, or software. It could be a biometric device, cryptographic module, or security-enhanced operating system. When we think of a thing which could be used to protect the critical characteristics of information, we are thinking of technology.

Usually, organizations are built around functional responsibilities. The advent of computer technology created the perception that a group needed to be established to accommodate the new machines which would process, store, and transmit much of our vital information. In other words, the organization was adapted to suit the evolving technology. Is this wrong? Not necessarily; however, it is possible to create the impression that technology exists for technology's sake. Telecommunications and computer systems are simply media for information. The media need to be adapted to preserve certain critical characteristics with the adaptation and use of the information media (technology). Adaptation is a design problem, but use and application concerns bring us to the next layer.

POLICY AND PRACTICE

The second layer of the third dimension is that of policy and practice. It's the recognition of the fact that information systems security is not just a product which will be available at some future date. Because of our technology focus, it's easy to begin to think of security solutions as devices or add-on packages for existing information systems. We are guilty of waiting for technology to solve that which is not solely a technological problem. Having an enforceable (and enforced) policy can aid immeasurably in protecting information.

A study has shown 75% of Federal agencies don't have a policy for the protection of information on PC-based information systems [OTA87]. Why, if it is so effective, is policy such a neglected security measure? It may be due in part to the evolving social and moral ethic with regard to our use of information systems. The proliferation of unauthorized software duplication is just another symptom of this problem. Even though software companies have policies and licensing caveats on their products, sanctions and remedies allowed by law are difficult if not impossible to enforce. No major lawsuit involving an individual violator has come before our courts, and it appears many people don't see the harm or loss involved. Although there are limits established by law, it seems we as "society" accept a less stringent standard.

Closely associated with the matter of policy is that of practice. A practice is a procedure we employ to enhance our

security posture. For example, we may have a policy which states that passwords must be kept confidential and may only be used by the uniquely-authenticated user. A practice which helps insure this policy is followed would be committing the password to memory rather than writing it somewhere.

The first two layers of the third dimension represent the design and application of a security-enhanced information system. The last building block of our model represents the understanding necessary to protect information. Although an integral aspect of the preceding two layers, it must be considered individually as it is capable of standing alone as a significant security measure.

EDUCATION, TRAINING, AND AWARENESS

The final layer of our third dimension is that of education, training, and awareness. As you will see, were the model laid on its back like a box, the whole model would rest on this layer. This phenomenon is intentional. Education, training and awareness may be our most prominent security measures, for only by understanding the threats and vulnerabilities associated with our proliferating use of automated information systems can we begin to attempt to deal effectively with other control measures.

Technology and policy must rely heavily on education, training, and awareness from numerous perspectives. Our upcoming engineers and scientists must understand the principles of information security if we expect them to consider the protection of information in the systems they design. Currently, nearly all university graduates in computer science have no formal introduction to information security as part of their education [HIG89].

Those who are responsible for promulgating policy and regulatory guidance must place bounds on the dissemination of information. They must insure information resources are distributed selectively and securely. The issue is ultimately one of awareness. Ultimate responsibility for its protection rests with those individuals and groups which create and use this information; those who use it to make critical decisions must rely on its confidentiality, integrity, and availability. Education, training, and awareness promises to be the most effective security measure in the near term.

Which information requires protection is often debated in government circles. One historic problem is the clash of society's right to know and an individual's right to privacy. It's important to realize that these are not bipolar concepts. There is a long continuum which runs between the beliefs that information is a free flowing exchange of knowledge and that it is intelligence which must be kept secret. From a governmental or business perspective, it must be assumed that <u>all</u> information is intelligence. The question is not should information be protected, but how do we intend to protect the confidentiality, integrity, and availability of it within legal and moral constraints?

THE MODEL

OVERVIEW

The completed model appears as Figure 1. There are nine distinct interstices, each three layers deep. All aspects of information systems security can be viewed within the framework of the model. For example, we may cite a cryptographic module as technology which protects information in its transmission state. What many information system developers fail to appreciate is that for every technology control there is a policy (sometimes referred to as doctrine) which dictates the constraints on the application of that technology. It may also specify parameters which delimit the control's use and may even cite degrees of effectiveness for different applications. Doctrine (policy) is an integral yet distinct aspect of the technology. The third layer-education, training, and awareness-then functions as the catalyst for proper application and use of the technology based on the policy (practice) application.

Not every security measure begins with a specific technology. A simple policy or practice often goes a long way in the protection of information assets. This policy or practice is then effected by communicating it to employees through the education, training, and awareness level alone. This last layer is ultimately involved in all aspects of the information systems security model. It may also be solely an educational, training, or awareness security control. The model helps us understand the comprehensive nature of information security that a COMSEC/COMPUSEC perspective cannot define.

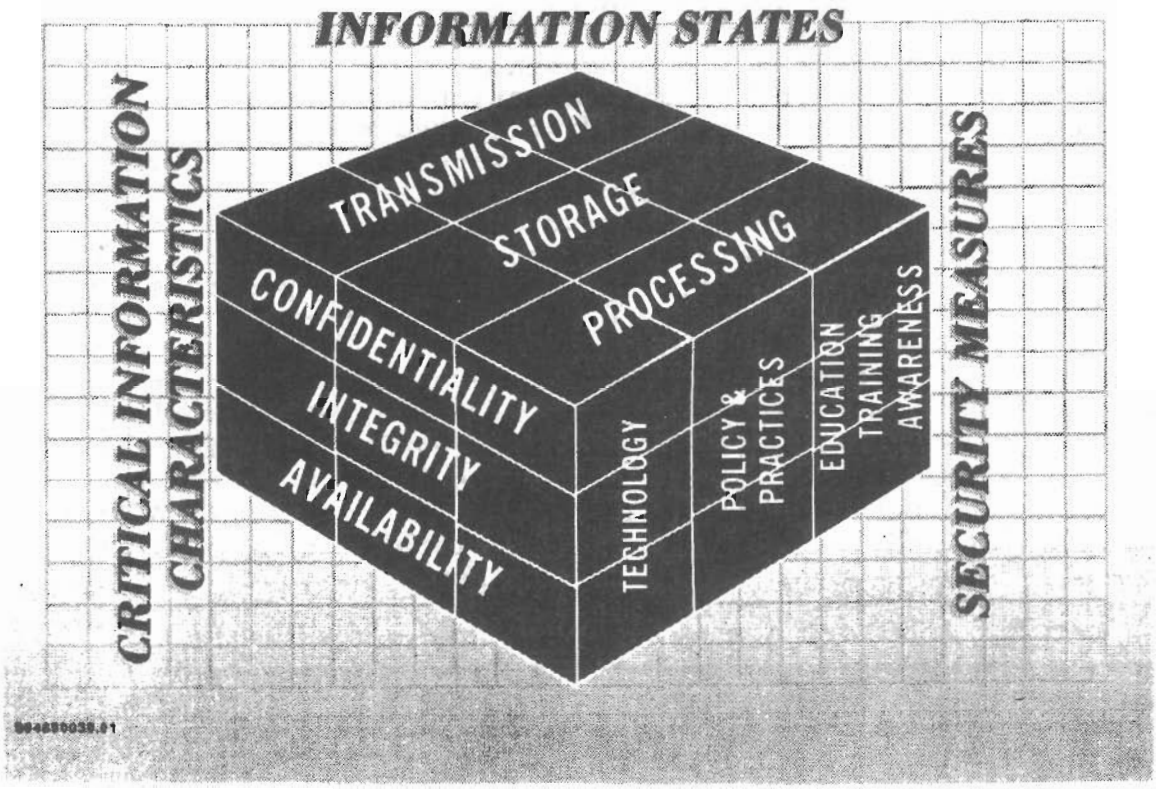

Figure 1

USE OF THE MODEL

The model has several significant applications. Initially, the two-dimensional matrix is used to identify information states and system vulnerabilities. Then, the three layers of security measures can be employed to minimize these vulnerabilities based on a knowledge of the threat to the information asset. Let's take a brief look at these applications.

A developer would begin using the model by defining the various information states within the system. When an information state is identified, one then works down the vertical path to address all three critical information characteristics. Once vulnerabilities are noted in this fashion, it becomes a simple matter of working down through the three layers of security measures. If a specific technology is available, the designer knows that policy and practice as well as education, training, and awareness will be logical follow-on aspects of that control. If a technology cannot be identified, then policy/practice must be viewed as the next likely avenue. (Again, the last layer will be used to support the policy/practice.) If none of the first two layers can satisfactorily counter the vulnerability then, as a minimum, an awareness of the weakness becomes important and fulfills the dictates of the model at the third layer.

Another important application is realized when the model is used as an evaluation tool. As in the design and development application, the evaluator first identifies the different information states within the system. These states can be identified separately from any specific technology. A valuable aspect of the model is the designer needn't consider the medium.

After identifying all the states, an evaluator or auditor can perform a comprehensive review much the same way the systems designer used the model during the development phase. For each vulnerability discovered, the same model is used to determine appropriate security measures. The third dimension of the model insures the security measures are considered in their fullest sense. It is important to note that a vulnerability may be left unsecured (at an awareness level in the third layer) if the designer or evaluator determines no threat to that vulnerability exists. Although no security practitioner should be satisfied with glaring vulnerabilities, a careful study of potential threats to the information may disclose that the cost of the security measure is more than the loss should the vulnerability be exploited. This is one of the subtle compromises alluded to earlier.

The model can also be used to develop comprehensive information systems security policy and guidance necessary for any organization. With an accurate understanding of the relation of policy to technology and education, training, and awareness, you can insure your regulations address the entire spectrum of information security. It's of particular importance that corporate and government regulations not be bound by technology. Use of this model allows management to structure its policy outside the

technology arena.

The model functions well in determining requirements for education, training, and awareness. Since this is the last layer, it plays a vital role in the application of all the security measures. Even if a designer, evaluator, or user determines to ignore a vulnerability (perhaps because of a lack of threat), then the simple acknowledgement of this vulnerability resides in the last layer as "awareness". Ultimately, all technology, policies, and practices must be translated to the appropriate audience through education, training, and awareness. This translation is the vehicle which makes all security measures effective. For a more complete understanding of the nuances of education, training, and awareness see [MAC89].

The twenty-seven individual "cubes" created by the model can be extracted and examined individually. This key aspect can be useful in categorizing and analyzing countermeasures. It's also a tool for defining organizational responsibility for information security. The example shows a policy security measure for protecting the confidentiality of information while it is being processed. By considering all 27 such "cubes", the analyst is assured of a complete perspective of all available security measures. Unlike other computer security standards and criteria, this model connotes a true "systems" viewpoint.

CONCLUSION

The information systems security model acknowledges information, not technology, as the basis for our security efforts. The actual medium is transparent in the model. This eliminates unnecessary distinctions between COMSEC, COMPUSEC, TECHSEC, and other technology-defined security sciences. As a result, we can model the security relevant processes of information throughout an entire information system-automated or not. This important aspect of the model eliminates significant gaps in currently-used security architecture guidance for information systems.

I developed this model to respond to the need for a theoretical foundation for modeling the information systems security sciences. The organizational realignments which have recognized the interdependence of several complementary technologies will need refinement in the near future. We can begin that process now by acknowledging the central element in all our efforts-information. Only when we build on this foundation will we accurately address the needs of information systems security in the next decade and beyond.

REFERENCES

[CHR90] Interview with Agent Jim Christy, Chief, Air Force Office of Special Investigations, Computer Crime Division, 26 March 1990

[DOD85] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Department of Defense, Washington, DC, December 1985

[DOJ88] Basic Considerations in Investigating and Proving Computer-Related Federal Crimes, U.S. Department of Justice, Justice Management Division, Washington, DC, November 1988

[HIG89] Higgins, John C., Information Security as a Topic in Undergraduate Education of Computer Scientists, Proceedings of the 12th National Computer Security Conference, November 1989

[MAC89] Maconachy, W.V., Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality, Proceedings of the 12th National Computer Security Conference, November 1989

[OTA87] U.S. Congress, Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-310, Washington, DC: U.S. Government Printing Office, October 1987

[PFL89] Pfleeger, Charles P., Security in Computing, Prentice-Hall, 1989