A Model for Information Assurance: An Integrated Approach

W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale and Don Welch

***Abstract*-- The model presented in this paper is an extension of work reported in 1991 by John McCumber. His model provided an abstract research and pedagogic framework for the profession. In the decade since McCumber prepared his model, Information Systems Security (INFOSEC) has evolved into Information Assurance (IA). Although the framework remains sound, the growth of the profession has suggested that changes are needed. This extension of the model accommodates the expanded needs of the IA discipline and include three temporal measures have been included.**

***Index Terms*—Information Security, Computer Security, Information Assurance**

I. Introduction

The model presented in this paper is an extension of work reported in 1991 [1]. by John McCumber. His model provided an abstract research and pedagogic framework for the profession. This model is shown in Fig1.

The McCumber model provided a concise representation of INFOFEC discipline. It became widely accepted, for example, it was extended by the author [2] to accommodate the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [3] that explicitly split their criteria into two distinct groups: functionality and trust. In the decade since McCumber prepared his treatise, INFOSEC has evolved into Information Assurance (IA). This is more than a simple semantic change. INFOSEC was an attempt to integrate here-to-fore separate disciplines such as personnel security, computer security, communications security, and operational security, into a coherent identifiable profession.

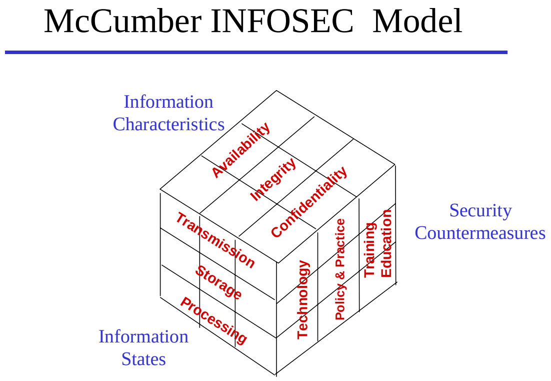


Fig. 1 The Original McCumber Model

Historically, INFOSEC came to be defined as:

Protection of information systems against unauthorized access to or Modification of information, whether in storage, processing or transit and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [4]

In today's information intensive environment, security professionals have expanded the scope, and thus the understanding of information and systems protection under an umbrella term referred to as IA.

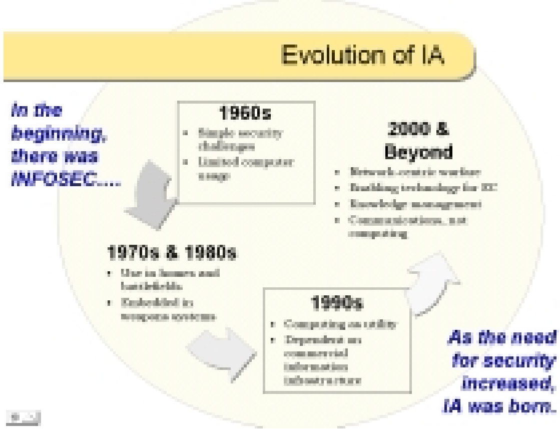

Evolution of IA
In the beginning, there was INFOSEC....
1960s
Simple security challenges
Limited computer usage
1970s & 1980s
Use in homes and battlefields
Embedded in weapons systems
1990s
Computing as utility
Dependent on commercial information infrastructure
2000 & Beyond
Network-centric warfare
Enabling technology for EC
Knowledge management
Communications, not computing
As the need for security increased, IA was born.

Fig 2 Evolution of IA

The National Security Telecommunications and

Manuscript received April 10, 2001.

W. V. Maconachy is with the National Security Agency, Ft. George Meade, MD 80305 USA (telephone: 410.854.6206).

C. D. Schou is with the National Information Assurance Training and Education Center, Idaho State University, Box 4043 Pocatello Idaho 83205-4043 USA (telephone 208.282.3194 e-mail: schou@mentor.net).

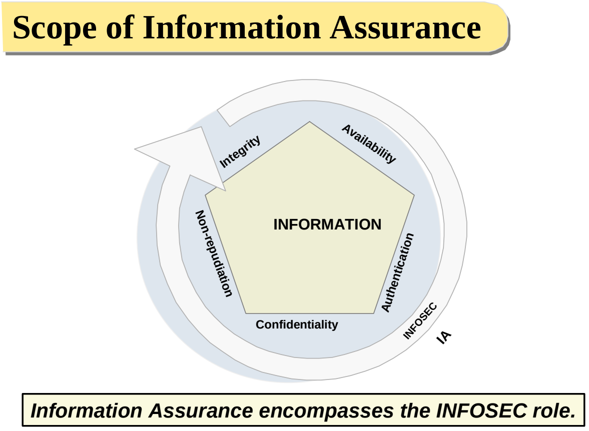
D. Ragsdale is with the Information Technology and Operations Center, Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY 80309 USA, (telephone 845.938.2056 e-mail: daniel-ragsdale@usma.army.mil).

D. Welch is with the Informational and Educational Technology Division, United States Military Academy, West Point, NY 10996 USA, (telephone 845.938.3710 e-mail: Donald-Welch@usma.edu).

Information Systems Security Committee (NSTISSC) has defined IA as:

> *Information operations (IO) that protect and defend information and information systems be ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*

Information Assurance not only expands the coverage, responsibilities and accountability of security professionals. IA also provides a view of information protection that is a subset of Information Operations that include IA defensive measures, but also proactive offensive activities. When viewed from this perspective, the axiom, "Your offense is only as good as your defense" brings a completely new perspective to IA to include such measures as "Active Network Defense".


Scope of Information Assurance

Information Assurance encompasses the INFOSEC role.

Fig. 3 Relationship Between IA and INFOSEC

Information Assurance is now viewed as both multidisciplinary and multidimensional – a critical element of the model presented by John McCumber in his original paper. The strength of this model lies not in any redefining of the field of IA, but in the multidimensional view required to implement robust IA programs. The four dimensions of this model are:

- Information States
- Security Services
- Security Countermeasures
- Time

II. The Nature of Information

Data are observations of the environment while information is 'that which affects ongoing decisions. There are numerous definitions for "information". Very often, information is referred to as the interpretation of data. Thus, the first variance from conventional definitions for the purpose of INFOSEC and IA is that both INFOSEC and IA are measures to protect systems and the information resident in those systems. Fig. 4 shows the modified model that accounts for three of four dimensions of IA.

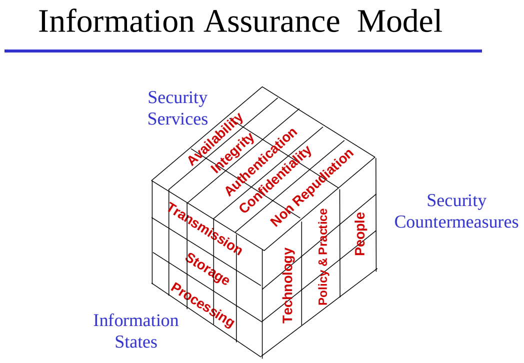

Information Assurance Model

Fig. 4 Information Assurance Model

A. *Information States*

However, within those systems, for any given moment, information is found in one or more of the three states; stored, processed, or transmitted.

Information can coexist in two states as shown by the example of simple message transfer. The data are obviously in the *Transmission* state while it is being moved over the through any medium. However, while this is occurring, the original copy of that file remains in storage on the hard drive and thus in the *Storage* state.

The data asset is in a different state depending on what part of the process one examines, the new model establishes an additional view of the states of information. The fourth dimension to the IA model -- the time state that will be discussed later.

B. *Security Services*

At the heart of Information Assurance is the provisioning of five security services; *Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation*.

1) *Availability*

Availability is the timely, reliable access to data and information services for authorized users. Often, this security service is viewed as a function, which is not entirely security, related. Availability is equated with information system operations such as back-up power, spare data channels, off site capabilities, and continuous signal. Availability is the utility part of security services. There may be times during the course of operations that demand system availability at the expense of the other security services. The decision to abandon the other security services is a risk mitigation decision often driven by threats and vulnerabilities that fall beyond the system security parameters. Broadcasting a decision to

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE

abandon a life-threatening condition may override concerns to do so in a totally secure fashion.

2) Integrity

Integrity is, "The quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data."[5] In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. Data integrity is a matter of degrees of trust. Integrity must include the elements of accuracy, relevancy, and completeness. Data and system integrity implies robustness.

3) Authentication

Authentication is a security service, "designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information". [6] The need for authentication was born out of system spoofing which became rampant in the mid 1990s.

4) Confidentiality

Confidentiality is "the assurance that information is not disclosed to unauthorized persons, processes or devises.[7] The application of this security service implies information labeling and need-to-know imperatives are aspects of the system security policy.

5) Non-Repudiation

Non-Repudiation provides, "The assurance the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data." [8] This is quite a step up from previous identify friend or foe systems. Non-repudiation has ramifications for electronic commerce as well as battlefield orders.

C. Security Countermeasures

Fundamentally, any defense in depth program must account for technology, operations and people. If, in fact, any of those three measures are not accounted for, systems become immediately vulnerable.

1) Technology

Technology is ever evolving. Technology encompasses more than the adjunctive crypto systems of the past. Technology, in a security context now includes hardware, software and firmware that comprise a system or network. Technology, from a security perspective now includes devises such are firewalls, routers, intrusion detection monitors, and other security components.

2) Operations

Operations, as a security countermeasure, goes beyond policy and practices required for use in secure systems. Operations encompass the procedures employed by system users, the configurations implemented by system administrators, as well as conventions invoked by software during specified system operations. Operations also address areas such as personnel and operational security.

3) People

People are the heart and soul of secure systems. People require awareness, literacy, training and education in sound security practices in order for systems to be secured. This progression in thinking has been described as a continuum upon which system users, designers, as well as security professionals increase their knowledge and understanding of IA. We can characterize the people component by describing it as the action users take. Do they follow the policy? What happens when they are confronted by a new situation that is not addressed by the policy?

D. Time

As noted earlier, time is the fourth dimension. It may be viewed in three ways. First, at any given time the access to data may be either accessible on-line or off-line. This introduces the question the element of risk/exposure to that data via remote unauthorized access means. Ergo, the most secure system is one that is not connected to any other system. Risk mitigation, as opposed to risk avoidance, takes on a different urgency depending upon connectivity.

The second and more important view of time as it relates to IA is that at any given time the state of our information and information system is in flux. Well-executed systems will include the IA model during all phases of the System Development Life Cycle.

Fig. 5 shows that early in the lifecycle the elements of the model all exist; however, they may not be complete nor necessarily well formed.

During the operational phases, the model is well defined and well implemented. Late in the lifecycle, certain elements of the model may fall away or become less important. In the late stage of a project, one might be most concerned with storage, confidentiality, and availability of the data in the system while transmission and non-repudiation have become less significant.

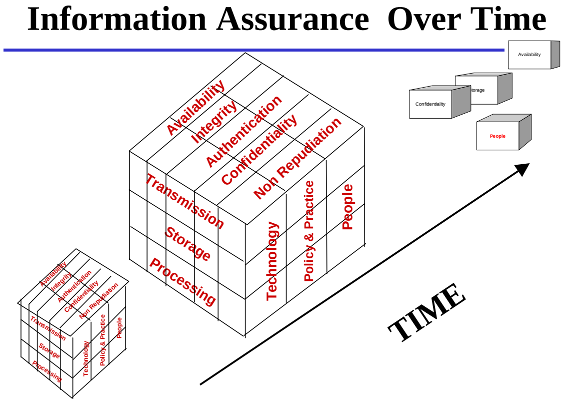


Fig. 5 Information Assurance Model

Time, as a fourth dimension of the integrated model is not a causal agent of change, but a confounding change agent. As an example, the introduction of new technology, over time, requires modifications to other dimensions of the integrated model in order to restore a system to a secure state of operation.

Finally, the human side of the time line leads to career progression. Individuals involved in IA will become better trained and educated. These learning activities, over time, will produce an enhancement to a system security state. Fig. 6 shows the learning continuum that might lead to this people countermeasure becoming more effective.

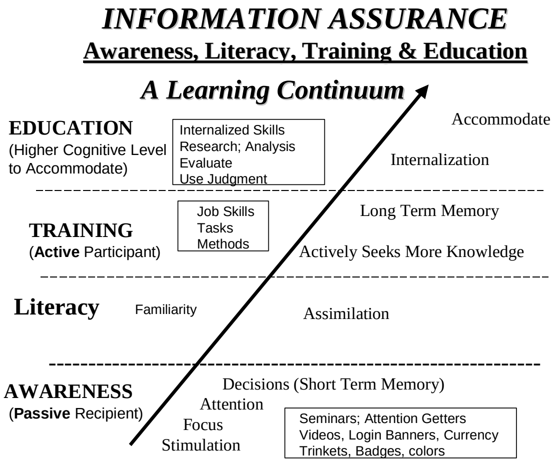


Fig 6 Learning Continuum [9]

III. The Model Overview

The Integrated Model for IA provides a framework for questioning as well as teaching information assurance topics. Examining the intersections of the four dimensions gives the practitioner as well as the student a needed multidimensional view of the scope of IA as it apples to systems security and provides a framework for understanding new aspects of IA in the future.

When teaching an aspect of IA, for example a technology such as Intrusion Detection (ID), students cannot understand the technology without understanding its context. The model provides a structured way to establish this context. To effectively employ an ID component, the proper policy and training must also be present. The student must understand which security service and to what extent the ID software provides each security service. Technological IA solutions cannot be taught out of context.

As analysis in the proper context applies to teaching IA, it applies to thinking about IA to develop secure systems. When an analyst is designing or analyzing a system, this framework insures that he not neglect the interplay of security services, countermeasures, states and time. Research has shown that many countermeasures are the equivalent to putting a tollbooth in the middle of the desert. It is just as easy to go around as to try to go through the countermeasure and so does not effectively increase the system security. This model provides structured way to better understand the context and avoid this pitfall.

IV. Model Example

As an example, we look at how we should teach the technology of client-based anti-virus software. This is obviously a technological counter-measure. However, to fully understand how it fits into system security requires more than teaching the technology.

We start by describing a new virus that is not a derivative of any currently known viruses and thus not detectable to virus-checkers with the latest signature information. This is time T_0. We can start by looking at the security services. If this is a Visual Basic Script (.vbs) like the "ILOVEYOU" virus, then the threat is primarily against the availability of information. It will destroy stored information and possibly make the computer inoperable. It would take an executable (.exe) file to deposit a Trojan Horse like SubSeven on the target that could threaten the confidentiality of the information. In the countermeasure realm, the technology will fail us, as will policy and configuration. The policy to update signature files every two weeks will not help, nor will configuring the software to automatically get new signature files every two weeks. The only thing that will help is the user. If they understand virus threats, they do not normally run programs that are unexpectedly e-mailed to them.

As time proceeds, parameters of the model change and we have to re-look at the services, states and counter-measures. At time T_1, the anti-virus vendor has released signature files that detect the new virus. Therefore, the technology exists to address the new virus. However, the signature files must be deployed to every workstation to be effective. The operations countermeasure comes into play. Updating definition files every two weeks may not be fast enough and leaves a window of heightened risk. A policy that allows for the urgent updating of files would change the availability of our information with respect to this threat. So would a configuration that allowed for the automatic updating of signature files. The people aspect would still be important, but obviously not as important as it was at time T_0. The extent to which the users followed the policy as well as the extent to which the users will actively circumvent the configuration all determine the level of each security service provided.

This technology also must also be examined later. After the signature files are available, the configuration counter-measures have had time to react and the users have had time to comply with the policy, the environment has changed and the model must be re-analyzed. At time T_2, the technology now dominates the countermeasures, but we must still go beyond the technical considerations of how effective the virus-detecting software is and look at the effectiveness from the entire context. In this example, the main threat is still to availability. However, the student must also understand the effect on system security from the perspective the operations (policy and configuration) countermeasure. For example, virus-checkers that terminate for any reason offer no protection. The situation is exacerbated by users who assume that the checker on their system is still functional and depend on it to protect them. This interplay between the technical, operations and people parameters of the counter-measures dimension is critical to understanding this aspect of IA.

V. CONCLUSION

IA for a system cannot be understood by looking solely at the components that comprise the system. The interaction of the components is more important than the individual components themselves. The whole concept of IA is difficult to understand, especially for students whose experience in the field is very limited. Education in general, and IA education even more so must prepare the student to learn about and understand new concepts as he encounters them.

This model provides a framework for the teacher, student and analyst who is dealing with IA. As a student uses this model to understand IA components and their interaction, he is preparing to understand new aspects of IA that he encounters later in life. He can identify that component by where on the counter-measures dimension it falls. He can understand it by determining how and if it protects information in various states. He looks at how it provides or does not provide each of the five security services. He also uses this model to help him not think of IA as static, but dynamic. Thus he looks at IA at critical times, understanding how IA posture of a system changes with time.

REFERENCES

[1] McCumber, John. “Information Systems Security: A Comprehensive Model”. Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD. October 1991.

[2] McCumber, John, “Application of the comprehensive INFOSEC Model: Mapping the Canadian Criteria for Systems Certification, Unpublished Manuscript, February 1993.

[3] Canadian Systems Security Centre, *The Canadian Trusted Computer Product Evaluation Criteria*, Draft Version 3.0e, April 1992.

[4] National Security Agency. National Information Systems Security Glossary. NSTISSI 4009 Fort Meade, MD. Sept. 2000

[5] Ibid

[6] Ibid

[7] Ibid

[8] Ibid

[9] Corey D. Schou, W. V. Maconachy, and James Frost,” Organizational Information Security: Awareness, Training and Education to Maintain System Integrity”, In *Proceedings Ninth International Computer Security Symposium*, Toronto, Canada, May 1993.

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE