What Is Information Assurance?

Dr. Walter L. McKnight
Shim Enterprise, Inc.

This article defines information assurance from a technical viewpoint, addressing the five attributes of information assurance: availability, integrity, authentication, confidentiality, and non-repudiation. An understanding of information assurance is critical because its activities involve many disciplines, and these activities permeate all phases of software life-cycle development and system maintenance.

Each of us defines information assurance based on our own perspective. For example, a security guard might define information assurance as security clearance and access to buildings or rooms. A network administrator might base his/her definition on passwords or permission rights. Personnel at a network operations center might define it as firewalls, intrusions, viruses, and hackers.

In each of these cases, the parameters of the definition determine who does or does not have access to something. However, information assurance is much more than just that. While each perspective of information assurance is correct, the view of the total picture is not.

From a broad perspective, information assurance includes the products, procedures, and policies that allow the timely transfer of information in an accurate and secure way among all parties involved. While the technology, procedures, and policies used to achieve this have changed over the years, the underlying goals of timeliness, accuracy, and non-repudiation have remained consistent.

For example, in early history man wrote or drew in stone knowing that his neighbors could not easily change it. Timeliness was not an issue because people did not carry stone tablets around with them. By the Roman Empire, man had moved to scrolls that were easier to write on and send. However, scrolls were also easier to copy so seals were created to authenticate the sender. The arrival of the pony express raised the delivery issue; the army was asked to help protect the riders to aid in safe mail delivery.

This article defines information assurance and its terms from a technical point of view. Each term is illustrated for better understanding and will show where the various disciplines associated with information assurance fit into the overall picture. There are concluding references that provide a more in-depth understanding.

Defining Information Assurance

The term information assurance has not been defined in many publications. The definition given in "Information Assurance (IA) Awareness Program," (AFI33-204) is similar to that of the Industry Advisory Council, Shared Interest Group on Information Assurance. They define it as follows: "Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

> *"Most of the nontechnical staff equates information assurance to information security. This is an incorrect view of the whole picture."*

This same organization defines information security as "the result of any system of policies and procedures for identifying, controlling, and protecting unauthorized (accidental or intentional) disclosure, modification, or destruction of information or denial of service." As you will see, most of the nontechnical staff equates information assurance to information security. This is an incorrect view of the whole picture.

In this article, the terms *information* and *data* are used interchangeably; data assurance is discussed in the same manner as information assurance. While there is a real distinction between the two, it is not the focus of this article.

The term assurance has many meanings. In the context of information, it is defined as a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the defined security policy. This assumes that a security policy has been defined, security architecture has been approved, and security features have been implemented. This confidence is based on analysis involving theory, testing, software engineering, and validation and verification.

For the Department of Defense (DoD), confidence is documented in a System Security Accreditation Agreement (SSAA) that is signed and approved by the designated accreditation authority (DAA) before a system becomes operational. Each system needs to have a signed SSAA.

Lest you think that information assurance is achieved with DAA signing the SSAA, let us now define the five attributes of information assurance: availability, integrity, authentication, confidentiality, and non-repudiation.

Access Means Availability

According to the National Computer Security Center, availability is the "state where information is in the place needed by the user, at the time the user needs it, and in the form needed by the user" [1]. The issues that most directly affect availability are information system reliability (is it up and running?), the informational level of importance (some information is more critical than others), and timely information delivery (delay of some information has a greater impact than other information).

In the past when we wanted information, we had to go to where the information was. We knew where it was located, and we had almost total control of when we wanted to get it. With the development of the Internet, the picture is reversed. We now want information to come to us, and in some cases we want the information as soon as it is generated. Previously, if the information was in another form that we were not familiar with (like a foreign language), it was our responsibility to translate it into a more familiar form. The computer age has changed that, too. Today, we expect tools to be readily available to automatically translate for us. This does not mean going from one foreign language to another but going from a spreadsheet to a word document or a database. We also expect the tools to be accurate 100 percent of the time.

These changes have brought some real challenges regarding information assurance. On the reliability front, we expect our networks, computers, pagers, Palm Pilots, and other information processing devices to work 100 percent of the time. We have built greater reliability into the devices but certain things are not within our control. For example, if someone cuts a fiber optic cable, the network goes down, and we cannot get needed information. To ensure this reliability is maintained, we rely on product designers, maintenance personnel, network designers, network administrators, and help-desk personnel.

Other information assurance issues affect timely delivery. Sometimes too much information is traveling across the network. On-time delivery becomes a big problem. There are ways to correct this problem, but they involve many disciplines working on all the issues, including software engineers, network engineers, network operations center personnel, and communications engineers. Program managers become involved as well when they address the issue of service vs. cost.

Sometimes the problem is not the amount of required information that transverses the network, but the deliberate introduction of unwanted information into the network. This information creates a problem called *denial of service*. Some people call it *spamming* the network. Some of the disciplines that work on this problem are security personnel, network operations center personnel, security managers, and network administrators.

Some other issues addressed are viruses, worms, and Trojan horses that crash our computers, networks, and other communication devices. This has been a large growth area in information assurance, and many resources are applied daily to make sure these problems do not affect both the reliability of our communication devices and the timely delivery of information.

The last area for availability has been the development of tools that make the presentation of information in the form we want it to be. Typically, we do not think of computer programmers being involved in information assurance, but they play a key role here. Some of the other disciplines involved are requirements engineers, quality assurance personnel, and configuration managers.

Integrity

The second IA attribute is integrity, which is "sound, unimpaired, or perfect condition" [2]. Here we are looking more at system integrity instead of data integrity (although both can be considered).

System integrity looks at the overall architecture of the system and how it is implemented. The design has to follow best practices and considers how various devices affect the overall design. You would not want to put a chokepoint into a network that would become a prime target for an enemy to hit or which could bring down the network if it became inoperable.

> *"Authentication ensures that you have the right to see the information, and that you are who you say you are … not only do people need to be authenticated, so do devices."*

Not only are we concerned with how the system is designed, but also how it will be maintained. We do not want to make it more costly to maintain than what the information is worth. We also look at what happens when unforeseen events happen, such as earthquakes or power failure. We need to have contingency plans in place so we can continue our operations during these types of events. Some of the disciplines involved here are program managers, system designers, contingency planners, operations personnel, and human resources personnel.

Authentication

The third IA attribute is authentication, which is defined by the National Computer Security Center as follows: "… 1) to verify the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system, and 2) to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification" [3]. Authentication ensures that you have the right to see the information, and that you are who you say you are.

The two elements often associated with authentication are logins and passwords. You are generally given a login name when the system administrator is sure you are who you say you are. You then establish a password so the system can be sure you are who you say you are. Helping the system administrator is the security personnel who might look into your background to see who you really are. Instead of a login name and password, a fingerprint device or retinal scanner may help establish who you are.

Not only do people need to be authenticated, so do devices. The network might need to confirm where it is getting its information, and it may require that routers, bridges, and other communicating devices identify themselves to the network. These network devices go through a process of exchanging information to establish their identity. This *authentication process* is often called a network protocol. Here, a different group of individuals are involved such as network programmers and standards committees who determine what valid protocols are, and how they are to be implemented.

Authentication also makes sure that the needed information is not altered between the time it is generated and the time it is received. There are several ways information can be altered, including viruses, worms, or Trojan horses that alter information at any time during generation, transmission, or receipt. For example, an unscrupulous individual monitoring the network could change the information while it is traveling across the network. Or, some of our translation tools could introduce errors into the information.

Some of the disciplines involved in making sure information integrity are maintained include network operations personnel who are looking for unusual activities on the network. Security police might patrol unsecured portions of the network. System designers might include a protected distribution system to make sure intruders cannot get into the network. Software testing personnel could conduct tests to make sure the translation tools work as designed. Configuration management personnel could ensure that the right version of the software is operational on the system.

Confidentiality

Confidentiality is the fourth IA attribute. It is "the concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations" [4]. Confidentiality is often referred to as information security. Here we deal with two issues: clearances and data security.

Access to data is based on two criteria: a security clearance and a *need to know*. In the DoD, there are several agencies whose mission is to determine the trustworthiness of an individual. Security clearances are issued based on that trustworthiness. Normally, security personnel only deal with those individuals who need and/or have a security clearance. It is up to the data owner to determine who has the need to know. The disciplines involved here utilize security managers, investigation personnel, arbitrators, operational personnel, and human resources personnel.

Data security can be provided by building private networks, encrypting the data that travel across unprotected sections of the network, providing protective distribution systems, or building secure enclosures where the data can be processed. These measures use security personnel, communications security personnel, emanation personnel, program managers, communications engineers, and a dozen other disciplines. The National Security Agency becomes involved in the many issues associated with data security.

Non-Repudiation

The last IA attribute is non-repudiation. This is "a service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any third party at any time; or, an authentication that with high assurance can be asserted to be genuine, and that cannot subsequently be refuted" [5].

There are three types of services in non-repudiation: non-repudiation of origin, non-repudiation of submission, and non-repudiation of delivery. Non-repudiation of origin protects against any attempt by the message originator to deny sending a message. Non-repudiation of submission protects against any attempt by message transit point to deny that a message was submitted for delivery. Non-repudiation of delivery protects against any attempt by a message recipient to deny receiving a message. Two of the services that support non-repudiation are data signature and encryption.

Data signature is a fairly new area of information assurance, although ideas for it have been around for a long time. The technology for doing data signatures is still not at the level of confidence that is needed for widespread use. Many legal issues need to be addressed, which utilize two other professions to IA: lawyers and judges.

We have already addressed the issue of encryption. Some new technologies are emerging that will make data encryption less costly and less man-power intensive. Much of this new technology has been developed because e-commerce has created a greater need for encryption.

> *"Confidentiality is often referred to as information security. Here we deal with two issues: clearance and data security … Access to data is based on two criteria: a security clearance and a need to know."*

Several disciplines are involved in IA. Today, IA is an issue that has to be addressed in every phase of a system life cycle. Even in system disposal, information assurance plays a key role. After years of protecting information, you do not want to give it all away with an improper system disposal.

The key document ensuring that all attributes of IA are addressed is the SSAA. This document begins with the concept design phase and is reviewed regularly to make sure that any changes to the system have addressed security issues.

Summary

Information assurance and its attributes have been defined in both technical and nontechnical terms. The author has only brushed lightly across some of the issues associated with IA. A great general source on information assurance for program managers and others who want a general concept review is, "An Introduction to Computer Security: The NIST Handbook" [6]. More technical documents have been developed by the National Computer Security Center (both technical reports and technical guides) and by the National Institute of Standards and Technology (both their own special publications and the Federal Information Processing Standards publications).

We are all involved in information assurance. Not only do we depend on it to do our work, but also we are involved in making sure it works. Remember, information is only as good as the assurance that we apply to it. Not all information needs to be protected at the same level, but all information needs to be protected.◆

References

1. National Computer Security Center. "Glossary of Computer Security Terms." NCSC-TG-004-88. Oct. 1988: 9.
2. Ibid, p. 23.
3. Ibid, p. 8.
4. Ibid, p. 12.
5. Caeli, W., D. Longley, and N. Shain. Information Security Handbook. London: Macmillan, 1991.
6. NIST Special Publication 800-12. An Introduction to Computer Security: The NIST Handbook. Oct. 1995.

About the Author

Walter L. McKnight, Ph.D., is a senior information assurance engineer at Shim Enterprise, Inc. where he is conducting security accreditation for the Ground Theater Air Control Systems. He has more than 30 years of experience as an Air Force officer working in all phases of computer technology. Dr. McKnight has a bachelor's of science degree in mathematics, a master's degree in computer science from the University of Utah, and a doctorate in computer science from Ohio State University.

1732 Westerly Drive
Brandon, FL 33511
Phone: (813) 643-7343
E-mail: wmcknigh@shiminc.com