Assurance - What is it?

M. D. Abrams
The MITRE Corporation, 1820 Dolley Madison Blvd.,
McLean, VA 22102, USA, +1 703-883-6938,
fax +1 703-883-1397
abrams@mitre.org
D. J. Landoll
Arca Systems, 16020 Braesgate Drive, Austin, TX 78717, USA
+1 512-310-2228, fax +1 512-310-9490
Doug_Landoll@arca.com
Gary Stoneburner
National Institute of Standards and Technology
820 W. Diamond, Rm. 426, Gaithersburg, MD 20899, USA,
+1 301-975-5394, fax +1 301-948-0279,
Gary Stoneburner@nist.gov

Abstract

Among information system stakeholders, there are a variety of questions about the meaning of *assurance* (as the term pertains to information security), the means by which assurance is obtained, the means by which degrees of assurance can be differentiated, and the determination of a suitable level of investment specifically for building assurance. This paper identifies differences among stakeholders' perceptions, which contribute to current assurance debates, and it proposes a model to help clarify assurance expectations in system acquisition, operation, and maintenance.

Keywords

Assurance, evidence, information, stakeholder, system

This paper represents the opinions of the authors as individuals only. Affiliations are shows for purposes of identification only.

S. Jajodia et al. (eds.), *Integrity and Internal Control in Information Systems*

1 INTRODUCTION

The purpose of this paper is to help information systems stakeholders to understand 'assurance.' Security concerns include not only the protection of assets, but also the assurance that protection provides. Assurance is a broad concept which is concerned with such questions as:

- Should you believe that your information system will adequately protect your data
- Should you believe that your information system does more good than harm

Consumers have difficulty answering these questions because the evidence available is undifferentiated and often complex. At times this evidence is unbalanced–emphasizing security in one component while ignoring other components, or in support of one policy but not another. At other times, the evidence is understandable only to a specialist.

To understand your system's ability to protect your data it is necessary, not only to gather evidence towards an assurance claim but to understand how that evidence contributes to your assurance. We discuss assurance by:

- Identifying some of the system stakeholders and their security concerns
- Providing a framework for assessing assurance
- Giving an understanding of the different definitions that are being used for assurance

2 THE STAKEHOLDERS

The effect of information system misuse on direct users is often stressed, but for a given system there may be many groups with a stake in system security. The various stakeholders may face different tangible or intangible risks, and thus they may have competing interests or goals. These differences and their relationship to assurance need to be taken into account, and priorities need to be established.

To illustrate, Figure 1 identifies the stakeholders concerned with cellular telephone systems in the United States.

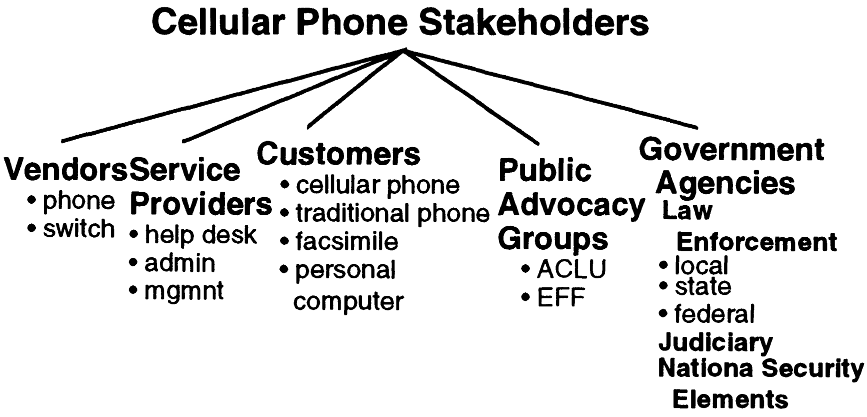

Figure 1 Cellular Phone Stakeholders.

2.1 Service Providers

The most apparent stakeholder organizations are those that operate cellular telephone systems. In the industry jargon, they are the *service providers.* The management of a service provider is a stakeholder. Top management is concerned with business objectives, such as profitability of the enterprise. We may assume that the CEO is concerned with security assurance primarily as it affects business objectives. Enterprise policy and major decisions must be made by, or at least approved by, the CEO.

Another class of stakeholders among the service providers is the system administrators. These personnel are responsible for operating many different technical systems within the enterprise. Some systems are directly involved in delivering service to consumers; others provide internal functions such as inventory and billing. The system administrators are probably all concerned with availability. To some personnel, integrity is more important than availability.

Additional stakeholders are those who interface between customers and various systems. We will use the term *help desk* for this group. In many organizations the help desk staff is strongly encouraged to handle each consumer as rapidly as possible, so their major concerns include availability, ease of use, and response time.

2.2 Advocacy Groups

Customers may be categorized according to the service used, such as traditional fixed location telephone, cellular phone, or data transmission, including fax. Customers are typically concerned with cost and quality of service. They are also concerned with privacy and correctness of billing records. Theft of service is always a concern to the management of the service provider. It becomes a customer concern when the cloning of a mobile telephone number and equipment serial number results in the customer being billed for services s/he did not use. If the customer concern is expressed as an inclination to change service providers or to use conventional telephone instead of cellular phone, then management becomes concerned. The concerns of the various stakeholders are interrelated.

Several public interest stakeholders exist. The American Civil Liberties Union and the Electronic Freedom Foundation lobby or litigate in support of their view of the public interest and the U.S. Bill of Rights. The direct effect of these stakeholders is felt by the service provider, which may be forced to change service offerings. The indirect effects of successful public advocacy are often difficult to predict.

2.3 Vendors

Two principal classes of vendor are the cellular phone manufacturers and the makers of phone switches and other infrastructure equipment. The cellular phone providers are interested in the end customers, primarily from the standpoint of maintaining market share.

The manufacturers of the hardware and software for the industry's infrastructure are interested in satisfying the service providers, who are their direct customers. There are direct effects on profitability and indirect effects on reputation, market share, and legal liability.

2.4 Government

A given law enforcement agency may have several objectives. They have an interest in insisting on the technical capability to conduct legal wiretaps. They have been able to get this interest incorporated into legislation--the U.S. Communications Assistance to Law Enforcement Act of 1994 affect manufacturers by mandating technical features and assurances in their products. The same act also impacts the service providers by requiring them to provide wiretap service.

Through export controls and pressure, certain government stakeholders have convinced the manufacturers and service providers to use weak cryptographic techniques. There is a concern among the service providers that weak cryptographic techniques will not prove sufficient to reduce theft of service. The debate has not been resolved.

3 ASSURANCE FRAMEWORK

An assurance framework providing a hierarchical structuring of the assurance argument has been developed (Williams, 1995). Many of the principles of that approach are relevant to understanding assurance and how it may apply to understanding the confidence you have in your system.

3.1 Assurance Types

It is important to understand what type of assurance is being reasoned about. The following assurance types define the applicability of the assurance towards the claim that a system may be used to protect data. Each type of assurance makes different claims about the system:

- Correctness: Correctness refers to claims that the implementation is a necessary and sufficient representation of the specification.
- Effectiveness: Effectiveness refers to claims that the selected security functions are suitable for countering the identified threats.
- Usability: Usability refers to the ease of configuring and using the security functions without compromising system security.
- Workmanship: Workmanship refers to product or system quality relative to the state of the art, including maintainability, expandability, and durability.

3.2 Assurance Subjects

It is equally important to understand the subject of the assurance claim. The following assurance subjects introduce the elements required to develop, evaluate, and operate a product or system. Each assurance subject contributes (in a different way) to the overall assurance that the system will protect the data with which it has been entrusted.

- Technology: Technology evidence comes from examining a product or system and its security mechanisms directly. Examples of technology evidence include system architectures, models, test results, evaluation results, and configuration parameters.
- Process: Process evidence comes from examining whether the development, evaluation, and operation processes are trustworthy and have been followed. Examples of process evidence include defined plans and procedures, process metrics, and performance data.
- Personnel: Personnel evidence comes from examining the individuals and organizations in the roles of developers, evaluators, and operators. Examples

of personnel evidence include credentials, background checks, hiring guidelines, experience data, and training data.

- Environment: Environment evidence documents reasons that development, evaluation, and operation environments are trustworthy. Environments should be considered to include tools and facilities. Examples of environment evidence include physical protections, tool capabilities, and backup mechanisms.

3.3 Assurance Framework

The framework illustrated in Table 1 provides a structure for mapping assurance subjects to each of the assurance types. Examples of assurance evidence for each category are provided, but there are many more. This framework is intended to apply equally well to products, systems, mechanisms, components, or any other assurance subjects.

Note that there is no indication of which assurance source is best. While one customer may rely heavily on assurance about the correctness of the system gained from analyzing the technology being deployed, others may want assurance about the effectiveness of the system gained from assessing the people who built it, or assurance about the usability of the system gained from reviewing the environment in which it was built.

Table 1 Assurance Framework

	Assurance Subjects			
Assurance Types	*Technology*	*Process*	*Personnel*	*Environment*
Correctness	Design Documents Test Results Requirement to Design Mapping	Configuration Mgmt Plans Coding Standards Peer Reviews	Experienced Developers Training Records Performance Reviews	Design Tools Access Logs Configuration Mgmt Tools
Effectiveness	Penetration Tests Vulnerability Analysis	Risk Mgmt Plans Test Plans Security CONOPS	Background Checks Credentials	Audit Logs System I&A Test Facility Review
Usability	User Trials Prototype Testing	Training Plans Test Plans	Credentials Human Factor Engineers	HF Tools Usability Standards
Workmanship	Improvement Measurements Problems Found	QA Plan	Commitment Corporate Culture Independence	Problem Reports Lab Plan Resource Plan

4 BARRIERS TO ASSURANCE

It has been difficult to obtain a sound basis for confidence in the security effectiveness of our information systems. Two of the primary reasons are discussed below.

4.1 Lack of Understanding

This is listed first because it is arguably the fundamental problem.

4.1.1 Too Many Definitions for Assurance

Webster's dictionary says:

> Assurance - 1. the act of assuring. 2. that state of being assured; sureness; confidence; certainty. 3. something said or done to inspire confidence, as a promise, positive statement, etc.; guarantee

According to Webster, assurance can be both something done to inspire confidence and the state of being confident. The information security community uses assurance in both of these ways and even more:

1. The confidence that the information system is effective in meeting its security objectives. In this usage assurance is a measure of how sure one is that the system will do what it is supposed to do and not do what it is not supposed to do.
2. The above usage plus confidence that the objectives themselves are correct. Even when using assurance as *confidence*, the extent of what one is confident about varies, but the same word, *assurance*, is used.
3. A specific type of measure that provides a basis for having confidence. This is distinctly different from the subjective nature of 1 and 2 above. Here *assurance* is an objective measurement related to the information system not a measure of confidence.

   When used in this manner, assurance relates to a specific type of measurement. While the individual probably understands that other measures are possible, in practical terms *assurance* frequently becomes narrowly defined.
4. Collection of measures of or facts about a system that provide a basis for having confidence. This is very similar to 3 above, but includes multiple types of measurement and fact in the practical, working definition.
5. The inherent security *quality* of the information system. The term *assurance* is used, not as confidence or a metric, but as a statement of a system characteristic. This is distinctly different from how one feels about the system (confidence) and from measurements of the system.

In summary, assurance is being used to mean:

- A subjective measure of human confidence.
- An objective measurement of or fact about an information system.

- A system characteristic which exists independent of confidence in the system or any measurement of, or fact about, the system.

Information system stakeholders are advised to explicitly specify which definitions they are using when they address assurance requirements.

4.1.2 Assurance–A system requirement

Information security is frequently seen, not as a system requirement, but as a hindrance to be minimized (or avoided if possible). The information systems environment has radically changed from stand-alone and supporting to interconnected and integrated. This change greatly increases the potential for our information systems to cause us harm. Diligent management of information-related risks is not a hindrance, but an essential element in the use of information technology.

4.2 Organizational Pressures

Organizational pressures may form barriers to information security; for example:

- Those who know do not decide
- Those who decide do not suffer
- Those who should care are engaged elsewhere

4.2.1 Those who know don't decide

In many organizations those who have the technical experience to understand information systems security (at least in the manner in which it has been relayed to date) are not those who make the buying decisions for the organization. Those who have, by virtue of training and experience, the capability to understand computing security issues are removed from the process owners who make the trade-off decisions between functionality and dependability.

4.2.2 Those who decide don't suffer

Decisions about which information technology product to install or how to automate a specific process are frequently made by individuals who do not feel the security impact of these choices. The support group is often quite removed from direct knowledge of or concern about the specifics of the business or mission process. These individuals simply do not concern themselves with business impacts. Instead their concern is directly related to the technology. They care deeply if the system goes off line, but not because they understand the business impact.

4.2.3 Those who should care are engaged elsewhere

The essence of risk management is to achieve a cost-effective tradeoff between business/mission risks and security countermeasures. Typically, the only individuals who can decide whether a given countermeasure is cost-effective are the owner of the process being automated. In many organizations these individuals are fully engaged in running the business or in accomplishing the mission. Like the information systems organization, the process owners have come to see information security in terms of machines and files. As such, these process owners see information security as a technical detail on which they cannot afford to spend their time.

5 SUMMARY

This paper has focused on introducing assurance issues. We have provided a summary of the concerns of various stakeholders, a framework for assurance, and a description of some of the common barriers to information security.

The list of references contains sources of additional information on assurance.

6 REFERENCES

Common Criteria Project, *Common Criteria for Information Technology Security Evaluations*, Version 2.0, May 1998. This is available at http://csrc.nist.gov/nistpubs/cc/ and is expected to become ISO/IEC 15408 in early 1999.

National Institute of Standards and Technology. (August 1994) A Head Start on Assurance– Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, March 21-23, 1994. Edited by M. D. Abrams and P. R. Toth, NISTIR 5472. This publication and additional material is available at http://aaron.cs.umd.edu/witat/.

Williams, J. R. and Landoll, D. J. (November 30, 1995) A Framework for Reasoning about Assurance (Version 1.0), ARCA Document Number ATR 95044.

7 BIOGRAPHY

Dr. Marshall D. Abrams is a Principal Scientist at The MITRE Corporation in McLean, Virginia. His information security interests span criteria, guidance, policy, security architecture, access control, assurance, vulnerability and threat analysis, security engineering process, and intellectual property protection–in which area he has a patent pending. The author of approximately thirty publications on information technology security, he is coeditor of *Information Security: An Integrated Collection of Essays,* which has been widely acclaimed as necessary for every security practitioner's library. He has taught information security courses on six continents. He received the BSEE from Carnegie Institute of Technology and the MSEE and Ph.D. from the University of Pittsburgh. While at the National Bureau of Standards he received the Department of Commerce Silver Medal Award.

Douglas J. Landoll is an expert in information security and has more than 10 years experience in the field of trusted product evaluations. He has been a lead contributor and project manager on projects to assess the security risk of information systems, develop information security requirements, and evaluate trusted products against established criteria. He is a nationally recognized authority on the subject of information assurance, has chaired numerous national conferences and information security panels, and authored many papers on information assurance and evaluation techniques. Mr. Landoll has been with Arca Systems since 1992 and currently holds the position of Evaluation Facility Manager.

Gary Stoneburner is a member of the technical staff at the National Institute for Standards and Technology (NIST), Computing Security Division. The focus of his efforts is in the area of computing security criteria and assurance. Mr. Stoneburner received a BES from Johns Hopkins University and an MS from The University of Texas at Austin, both in electrical engineering. Previous to NIST he worked for The Boeing Company as its security architect, worked as an electronic engineer with Engineering Resources Incorporated, and served in the US Army. He is presently a member of the Army reserve, working in the area of information operations.