An Enterprise Assurance Framework

Douglas J. Landoll
landoll@arca.com

Jeffrey R. Williams
williams@arca.com

Arca Systems, Inc.
8229 Boone Blvd., Suite 750
Vienna, VA 22182-2623

Abstract

This paper explores generating and conveying confidence in enterprise security. An enterprise assurance framework provides a structure enterprise assurance evidence that strengthens and clarifies the overall enterprise assurance argument. The structure and components of these arguments are defined and then applied to an enterprise. Finally, standards of evidence and evidence trade-offs are mentioned. This paper is largely based on a recent NIST internal report called "A Framework for Reasoning about Assurance."

Keywords: assurance, framework, enterprise, security, confidence, trustworthiness

1. Introduction

Efficiency in business and workflow activities is important to all organizations. The organization's enterprise[1] is responsible for accomplishing these tasks. Due to an increasingly hostile environment, security has become an important organizational need and therefore an important enterprise aspect. Developing an enterprise to meet the organization's security needs involves the creation of an enterprise security architecture and the identification and development of protection mechanisms.

However, protections mechanisms are not enough, confidence in these mechanisms must also be established. Security concerns include not only the protection of assets, but also the assurance in that protection. There are many definitions of assurance used in security; however, the central theme in these definitions is that assurance is the degree of confidence that security needs are satisfied [WITAT95]. Assurance is a broad concept which answers the question, "How sure are you that you're secure?"

Consumers have no way to answer this question because the evidence is undifferentiated and complex. At times this evidence is unbalanced - emphasizing security in one enterprise component while ignoring others. Other times the evidence is not understandable to the customer.

To address this problem, we have developed an assurance framework which provides a hierarchical structuring of the assurance argument [NIST96]. It is useful in specifying a clear and compelling assurance argument and in turn defining and conveying the confidence in the enterprise solution.

2. Assurance Arguments

An assurance argument is a way of presenting evidence in a clear and convincing manner. Instead of providing a massive amount of documentation and analysis that the assurance consumer cannot use, an assurance argument structures the evidence so that it makes sense.

These elements can be organized into a simple hierarchy to form a convincing case showing how the assurance needs are met, see Figure 1. The structure emphasizes how evidence should always be tied back to the original need for assurance with reasoning. This simple approach can be used to structure arguments supporting the complex assurance needs of an enterprise.

Enterprise assurance arguments are recursive in that each argument is composed of lower-level supporting arguments and evidence. For example, since an enterprise comprises an AIS, people, process, and environment, the assurance arguments for the AIS, people, process, and environment support the enterprise assurance argument. Furthermore, since an AIS comprises the products,

[1] The word ***enterprise*** is used here to refer to the collection of people, procedures, environment, and automated information systems (AIS) that support accomplishing the business or mission needs of an organization.

configuration, architecture, development people, development process, and development environment, the AIS assurance argument is supported by the assurance argument for each of these components of the AIS. This cycle continues until the assumption zone, where no evidence is offered to support a claim.

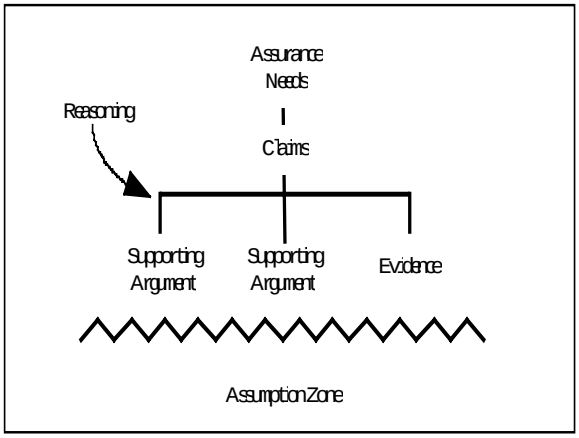

Figure 1: Hierarchy show elements of an assurance argument.

There are five elements that can be used to structure an assurance argument. They are:

- Assurance Need — Desired level of confidence
- Claims — Statements that something has a particular property
- Evidence — Empirical data on which a judgment can be based
- Reasoning — Statements which tie evidence together to establish claim
- Assumption Zone — Limit where claims are no longer supported by evidence

Assurance Need

Assurance needs are statements of the desired confidence in the parts of an enterprise. These needs may be expressed in many forms. A useful statement of assurance need should explain what the consumer is concerned about (breadth) and how much it will take to satisfy those needs (depth). It is not enough to simply state that a "high" degree of confidence is needed. These two important dimensions to assurance need are discussed in more detail below.

The ***breadth*** of assurance need indicates the set of things that the consumer is concerned about. Determining this aspect of assurance need involves analyzing threats, assets, and mission to determine where countermeasures are needed. These needs are usually expressed in terms of policies, such as the need for confidentiality, integrity, availability, or accountability.

The ***depth*** of assurance need indicates the amount of confidence the consumer wants that the countermeasures are effective in countering the threat. Determining this aspect of assurance need involves prioritizing the risks to the system and establishing a standard of proof that will be required. It is possible to state these needs in terms of evidence required or by indicating a desired level of assurance.

Claims

A clear argument is based on claims about specific properties of an enterprise component. A ***property*** is a characteristic trait relevant to establishing assurance. The following list gives some examples of security relevant properties. This list is not intended to be exhaustive nor do all of these properties apply to all the different parts of an enterprise.

- Analyzable — Capable of being checked. This property includes concepts like structure, organization, simplicity, minimality, and modularity.
- Capable — Having required or wanted skills.
- Complete — Having all the necessary parts or providing a total solution.
- Correct — Free from error, defect, or fault with respect to a higher level specification.
- Easy-to-Use — Capable of being put into service or maintained without difficulty.
- Efficient — With a minimum of waste, expense, or unnecessary effort.
- Experienced — Having performed similar events or activities.
- Knowledgeable — Having requisite information.
- Measurable — Capable of having dimensions, quantity, or capacity ascertained.
- Repeatable — Capable of being performed, experienced, or produced again.
- Reputable — The general estimation in which a person is held by the public.
- Strong — Capable of enduring or being defended. Strength also refers to the difficulty of being broken or resistance to known attacks or absence of flaws.
- Trustworthy — Deserving of confidence in the integrity, character, and truth of a person.

These properties may be context-dependent. For example, *strength* takes on a slightly different meaning when it refers to an AIS than when it refers to an environment.

Evidence

In order to establish claims, we need to rely on information that helps to show the truth. Anything that contributes to the believability of a claim can be considered as evidence. Design analysis results are an example of evidence which helps to support a correctness claim. Other examples of evidence include analysis results, design documentation, or background investigations.

Evidence can be "rolled up" into higher levels of abstraction. For example, the Trusted Product Evaluation Process (TPEP) takes in a great deal of evidence and produces a product evaluation rating that summarizes the assurance argument. This sort of repackaging can be extremely helpful in reducing the amount of evidence given to consumers.

Evidence can be thought of as having properties. Some examples of evidence properties are correctness, completeness, and analyzability. Claims about evidence properties can be supported with additional evidence. This ***circumstantial evidence*** also contributes to the believability of a claim, even though it is not directly related. For example, the qualifications of the designers are circumstantial evidence of the quality of the design.

In many cases, a single piece of evidence supports multiple claims. For example, a TCSEC rating represents compliance with a diverse set of criteria. A TCSEC rating may be used to help establish claims that a product is complete, correct, strong and analyzable, as well as claims that some aspects of the development process are defined.

Reasoning

An assurance argument is not a simple collection of the evidence supporting a claim. For example, to establish the claim that an operating system is correct, simply providing a formal model and some user documentation is not enough. Instead, the reasoning points to the evidence and shows why the claims have all been covered well enough.

Reasoning should be documented and included with the assurance package delivered to the consumer. An assurance package could come in the form of a brochure, fact-sheet, white-paper, security documentation, or certification package. Almost all products and systems should have some sort of assurance package, but it may vary considerably in level of abstraction.

A preponderance of evidence does not necessarily establish assurance claims. The evidence most be shown to be relevant, compelling, and cohesive. To create an assurance package, it is necessary to piece together many pieces of evidence. The composition of any complex items is extremely difficult. This is not a new problem. In fact, in his autobiography, Ben Franklin wrote:

> ...it scarce ever happens that a ship is formed, fitted for sea, and sailed by the same person. One man builds the hull, another rigs her, a third lades and sails her. No one of these has the advantage of knowing all the ideas and experience of the others, and therefore cannot draw just conclusions from a combination of the whole.

For assurance, the situation is similar. Assembling all the pieces of evidence at all different levels of abstraction into a logical argument can be quite difficult. Hierarchical assurance arguments help to address this problem.

The Assumption Zone

Since one can never be absolutely sure that a product or enterprise is invulnerable to every attack, one must decide how much of the argument can be assumed without evidence. The ***assumption zone*** is the limit of an argument where claims are presented without evidence and go unchallenged.

To illustrate this point, imagine the following claims: (Note that these claims are presented as a vertical slice of a hypothetical assurance argument. The claims below do not represent an adequate degree of breadth nor are they accompanied by supporting evidence.)

- the enterprise architecture addresses the threats
- the AIS architecture addresses the AIS threats
- the AIS design correctly implements the AIS architecture
- the AIS designers are qualified
- the hiring process is rigorous
- the hiring process is documented
- the hiring process documentation is complete

In this example, the documentation of the hiring process is not likely to have a significant bearing on the security of the enterprise. For most consumers and producers, this sort of evidence is deep in the assumption zone.

The assumption zone should be located at an appropriate depth for the significance of the claim to overall assurance requirements. Using this guideline, one would make sure that all the doors are locked before analyzing the strength of the locks.

3. Enterprise Assurance

An enterprise consists of people, processes, environment, and AIS. All of these parts are important to meeting the assurance needs of the enterprise. For example, one of the most common security flaws is a poor password choice. This is not a flaw in an AIS; it is a problem with the people and procedures in the enterprise.

There are many ways to structure an enterprise assurance argument. In this paper we divide the problem into four supporting arguments: people, process, environment, and AIS, see Figure 2.

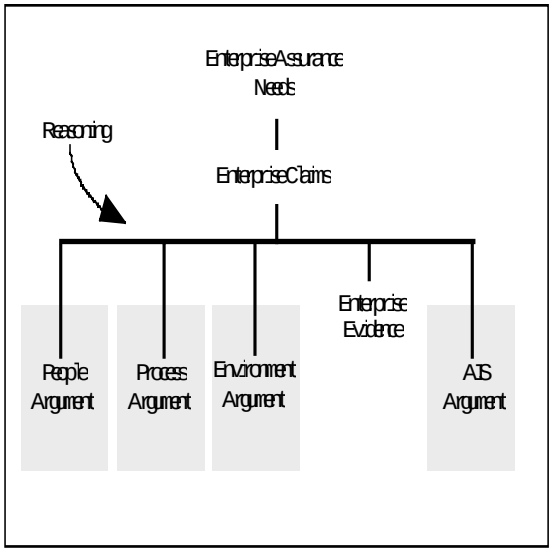

Figure 2: Enterprise assurance argument is established by evidence and supporting arguments.

Enterprise Security Needs

Understanding the risk to the enterprise is critical to determining the breadth and depth of these assurance needs. Assurance needs for the enterprise might include a high degree of confidence that the confidentiality of assets is protected, some confidence that information integrity is preserved, or a high degree of confidence that services are available to customers. Clearly, determining assurance needs is closely related to establishing an enterprise security policy, but must also include the depth or "how much" aspect.

Enterprise Security Claims

The most security relevant enterprise security properties are analyzability, correctness, completeness, and strength. Analyzability implies that the enterprise is not overly complex and is structured such that it can be understood. A correct enterprise indicates that the enterprise accurately performs as specified. Enterprise completeness indicates that all threats to the enterprise are addressed and all the security policies are implemented. A strong enterprise indicates the enterprise's capability to withstand attack.

These claims should be made across all the parts of the enterprise, to show that the assurance needs have been fully met. The assurance argument should show that each of the parts of the enterprise shows these properties. These claims are supported by some combination of evidence and supporting arguments. Each of these is discussed further in the next two subsections.

Enterprise Evidence

The most direct way of demonstrating the fulfillment of enterprise claims is to supply enterprise evidence. This evidence is about the enterprise as a whole rather than any particular part. There are several types of evidence that can help establish that an enterprise can satisfy its claims.

The first type is documentation of how the enterprise works. Examples of this type of evidence include business process models, architectures, plans, and designs.

A second type of evidence supporting enterprise claims is produced by objective analysis. This type of evidence can be extremely strong, depending on the degree of objectivity, the method used to evaluate, and skill of the evaluators. Some examples of analysis evidence include certification reports and security audits.

Finally, a third type of enterprise evidence demonstrates how the enterprise has performed in the past. Examples of this type of evidence include security metrics, financial information, and customer satisfaction.

Enterprise Supporting Arguments

Supporting arguments can also help establish enterprise claims. For an enterprise, arguments about the trustworthiness of the operational people, process, and environment can be quite convincing. Arguments about the effectiveness of AIS in the enterprise are also helpful.

Operational People Argument	Operational people include users, administrators, maintenance personnel, security officers, operators, organizations, and anybody else who influences the security of the enterprise. An argument which establishes the trustworthiness of these people can help to establish the enterprise claims. Operational people who exhibit properties like being knowledgeable, capable, experienced, and trustworthy are much more likely to perform without introducing security vulnerabilities. Evidence about the education, training, past performance, experience, and background is very effective in supporting arguments about operational people
Operational Process Argument	The operational process consists of any activities that establish, affect, or maintain the security of an enterprise. Examples of operational processes include clearing users for access to the system, escorting maintenance personnel, reviewing audit logs, releasing magnetic media, scanning the system for viruses, using the AIS, administering the AIS, handling written logs, monitoring the system, managing the configuration, and assessing risk. Operational processes that are, for example, analyzable, complete, correct, and easy-to-use are much more likely to be performed without vulnerability. Evidence that can support operational process arguments includes process documentation, process metrics, and past performance information.
Operational Envionment Argument	The operational envionment can provide protection from many classes of threats. Environment includes geographical location, structural and the AIS site mechanisms. An operational envionment that is, for example, analyzable, complete, correct, easy-to-use, and strong is less likely to have exploitable weaknesses. Evidence that can establish these properties includes site security plans, physical architectures, blueprints, user test results, design analysis, and penetration test results.
AIS Argument	The AIS is the combination of hardware, software, and communications that is used to automate enterprise processes. Examples of AIS might include cash registers, networks, file servers, trusted workstations, or word processors. Some properties that an AIS should possess include analyzability, completeness, correctness, ease-of-use, and strength. AIS evidence might include product evaluation reports, certification reports, architectures, test results, problem reports, and testimonials.

Note that each of these supporting arguments is also a complete lower level argument. In each one, the assurance needs which flow down from the enterprise level are met with lower level evidence and more supporting arguments.

Enterprise Reasoning

The last piece of the enterprise assurance argument ties together the claims, evidence, and supporting arguments. This reasoning is intended to establish that the enterprise has satisfied its assurance needs. Without reasoning, the user is left with an undifferentiated heap of evidence and supporting arguments. The reasoning serves as a roadmap for navigating the assurance argument.

For an enterprise, the reasoning addresses each of the assurance needs. For each need, the reasoning should point to the supporting arguments and evidence available. The reasoning should conclude by arguing that because the enterprise sufficiently meets all the claims, it has satisfied all the enterprise assurance needs.

4. Using An Enterprise Assurance Argument

There are two interesting areas involving enterprise assurance arguments that need further research. The first is the idea of establishing a standard of evidence to evaluate an argument against. This sort of standard should help consumers decide whether a particular argument convinces them or not. The second area is the idea of assurance trade-offs. There are usually several ways to establish the same claim. Understanding these trade-offs will make it easier to produce convincing arguments.

Standard of Evidence

Everyone who either produces or consumes assurance needs to be able to figure out how much they need. Establishing a standard of evidence for assurance addresses the question, “How much assurance is enough?” This question may be answered by determining the strength and detail required of the assurance claims and supporting evidence. Stating these standards of evidence is a demanding and subjective exercise. Many factors need to be considered including, cost, current state of technology, value of assets, presence of threat, and the importance of the mission.

As the value of the assets and severity of the threats in an enterprise increase, the standard of evidence for the information system should also increase. This directly relates to “assurance levels” concept used today in the TCSEC, ITSEC, CTCPEC, and drafts of the Common Criteria.

Regardless of the accepted standard, doubt will exist. There is always the possibility of missing a critical flaw at the next lower level of detail. The user must accept that a successful security assessment will reduce *but not eliminate*, the possibility of these critical flaws occurring. In other words, the user must carefully consider the location of the assumption zone.

There are several common standards of evidence used in the legal system that are useful in relating the degree of assurance required [WILL95b]:

- Substantial Evidence (a considerable amount)
- Preponderance of the Evidence (more than the evidence against)
- Clear and Convincing Evidence (reasonable person would believe)
- Evidence Beyond a Reasonable Doubt (no reasonable person can doubt)

Further research is needed to determine workable standards of evidence for security of information technology.

Evidence Tradeoffs

Enterprise assurance arguments are structured to tie evidence directly to the claim(s) it supports. Trade-off analysis can help producers and consumers make intelligent choices of claims and evidence to pursue.

The simplest case of an assurance trade-off is when two different pieces of evidence fully establish the same claim. In this case, the assurance producer can choose the easiest or cheapest option. Trade-offs at higher levels in the argument are considerably more complicated, as the claim being supported is more distantly related to the evidence concerned.

However, in any evidence trade-off, the important consideration is the claim being established. Different types of evidence are impossible to compare without the context of what claims they are being used to establish. For example, a formal model is not intrinsically better or worse than security test results, but it may be better at establishing correctness in a particular system. At an even higher level, assurance producers may have to decide between doing formal modeling and hiring trusted developers. Again, it is important to consider what common claim these evidence techniques are supporting.

5. Conclusions

Just as evaluated products do not automatically make a secure system, neither do trusted systems make a secure enterprise. Only by examining all the parts of an enterprise can a judgment be made about security. The confidence that enterprise security needs have been met is called enterprise assurance.

The assurance arguments described in this paper are a general approach to communicating confidence in products, systems, and enterprises. These arguments are flexible and allow for trade-offs to be made with assurance evidence. The arguments are scaleable so they can be applied to all sizes of systems and all levels of assurance.

There is a great deal more work to be done before vendors offer assurance arguments with their products and integrators create them for clients. A good first step would be to continue the research in alternative assurance methods currently underway.

6. References

[ARCA] Arca Systems, Inc., “Using an Assurance Framework to Reason about Security Evaluation Methods,” White paper, December 1995.

[GAL94] Gallagher, Lisa., “Process Assurance” International Invitational Workshop on Developmental Assurance, June 26-27, 1994.

[ISSA94] ISSA, “Exposure Draft of the Generally Accepted System Security Principles (GSSP). 1994.

[ITSEC] Information Technology Security Evaluation Criteria, Bonn, May 1990.

[LANDW93] Landwehr, Carl E., “How Far Can You Trust A Computer?” 12th International Conference on Computer Safety, Reliability, and Security. October 1993.

[LANDW94] Landwehr, C. E., Bull, A. R., McDermott, J. P., Choi, W. S., “A Taxonomy of Computer Program Security Flaws.” *ACM Computing Surveys*, volume 26, number 3, September 1994.

[LANDO94] Landoll, Douglas J.; Ferraiolo, Karen; Sachs, Joel, "Process as a Measure for Assurance Using the Security Engineering Capability Maturity Model," position paper accepted to the Invitational Workshop on IT Assurance and Trustworthiness, January, 1994.

[LANDO95] Landoll, Douglas J.; Ferraiolo, Karen, "Security Engineering CMM Profiles as a Basis for a Process Assurance Metric," position paper accepted to the Invitational Workshop on IT Assurance and Trustworthiness, January, 1995.

[MEAD95] Meadows, Catherine, “The Feasibility of Quantitative Assessment of Security” NRL white paper.

[PAYNE93] Payne, C. N., Froscher, J. N., Landwehr, C. E., “Toward a Comprehensive INFOSEC Certification Methodology.” Sixteenth National Computer Security Conference. National Institute of Standards and Technology / National Computer Security Center, Baltimore, MD, September 1993.

[SACHS93] Sachs, Joel E, Ferraiolo, Karen M., “Determining Assurance Levels by Security Engineering Process Maturity,” Fifth Annual Canadian Computer Security Symposium, May 19-21, 1993.

[SSECMM] Security Engineering Capability Maturity Model Development Workbook, September 1994.

[WICHE94] Wichers, David R., Landoll, Douglas J., Sachs, Joel E., “What Color is Your Assurance?,” Seventeenth National Computer Security Conference. National Institute of Standards and Technology / National Computer Security Center, Baltimore, MD, September 1994.

[WILL94] Williams, Jeffrey R., Sachs, Joel E., Landoll, Douglas J., Carpenter, Diann A., "Assurance is an N-Space, Where N is Hopefully Small", International Invitational Workshop on Developmental Assurance, June 26-27, 1994.

[WILL95a] Williams, Jeffrey R., Wichers, David R., “A Framework for Reasoning About Assurance.” Workshop on Information Technology (IT) Assurance and Trustworthiness, March 1995.

[WILL95b] Williams, Jeffrey R., Schaefer, Marvin, Landoll, Douglas J., “Pretty Good Assurance.” New Security Paradigms Workshop, September, 1995.

[WITAT94] National Institute of Standards and Technology, “A Head Start on Assurance,” Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, March, 1994.

[WITAT95] National Institute of Standards and Technology, Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, March, 1995.

[TCSEC] DoD 5200.28-STD, “DoD Trusted Computer System Evaluation Criteria.” December 26, 1985.