

## The Need for A Framework for Reasoning About Assurance

Jeffrey R. Williams  
Arca Systems, Inc.  
8229 Boone Blvd., Ste. 750  
Vienna, VA 22182  
williams@arca.com

David R. Wichers  
Arca Systems, Inc.  
10320 Little Patuxent Pkwy., Ste. 1005  
Columbia, MD 21044  
wichers@arca.com

### 1. Assurance Beyond the TCSEC

Recently, the security community has focused on understanding an expanded range of assurance types. Traditionally, security assurance has principally meant security testing and analysis (formal and informal) of the system design and implementation. The TCSEC (Trusted Computer System Evaluation Criteria) and TPEP (Trusted Product Evaluation Program) reflect this view. However, there is a growing consensus that this view of assurance should be expanded to include new techniques and new types of evidence.

There has been considerable research into areas such as "process" and "developmental" assurance [GAL94, LAN94]. Others are pursuing risk-based approaches to securing products and systems. We strongly support this trend towards increasingly flexible assurance. This paper is intended to help define a framework for discussing assurance beyond that provided by testing and analysis of the system design and implementation.

The framework presented in this paper can be used for:

- discussing assurance needs
- trading off potential assurance techniques
- identifying needed metrics and research directions

This framework is intended to help system and product buyers, as well as developers of security criteria and policy guidance, to determine the appropriate assurance techniques needed to counter particular threats or risks. This framework will also facilitate trade-off analysis among the different assurance techniques and will help policy developers decide which assurance techniques are required for different types of risks.

[This research was supported by the National Security Agency under Contract Number MDA904-93-C-C029.]

### 2. Assurance Types

Last year's workshop defined assurance as the "confidence that a system meets the security needs of those whom it was intended to serve" [NIS94]. To establish this confidence, one must show that all the right mechanisms are present, that they all work, and that they are usable and of high quality. We believe that producing evidence demonstrating the correctness, effectiveness, usability, and workmanship of the product or system accomplishes these goals.

- Correctness deals with whether the implementation is a necessary and sufficient representation of the specification.
- Effectiveness relates to the suitability of the selected security functions in countering the identified threats.
- Usability refers to the ease of configuring and using the security functions without compromising system security.
- Workmanship refers to product or system quality relative to the state of the art, including maintainability, expandability, and durability.

The definition of these terms has not been decided, but the concepts are valuable. There may be other types of assurance that are relevant to security, but these are likely to be among the most important ones.

### 3. Four Categories of Assurance Sources

There are four categories of things needed to develop, evaluate, and operate a product or system. We argue that these four categories cover all possible sources of assurance evidence.

- System Evidence (WHAT) comes from examining a product or system and its security mechanisms directly. Examples of system evidence include system architectures, models, test results, evaluation results, and configuration parameters.
- Process Evidence (HOW) comes from examining whether the development, evaluation, and operation processes are trustworthy and have been followed. Examples of process evidence which meet this need include defined plans and procedures, process metrics, and performance data.
- People Evidence (WHO) comes from examining the individuals and organizations in the roles of developers, evaluators, and operators. Examples of people evidence which meet this need include credentials, background checks, hiring guidelines, experience data, and training data.
- Environment Evidence (WHERE) documents reasons that development, evaluation, and operation environments are trustworthy. Environments should be considered to include tools and facilities. Examples of environment evidence which meet this need include physical protections, tool capabilities, and backup mechanisms.

The bulk of existing evidence is in the system evidence category. The other categories have been largely ignored, and some have been only partially covered by existing techniques. We believe that everyone has some need for assurance in each of these areas.

### 4. Two Categories of Assurance Techniques

Assurance techniques are methods for creating and evaluating assurance evidence. These two categories cover all the techniques associated with establishing a level of trust in a product or system.

- Evidence Production Techniques produce evidence establishing the correctness, effectiveness, workmanship, and usability of a product or system. Production techniques are performed by developers and operators of a product or system. Examples of evidence production techniques include modeling, testing, process definition, background checks, and environmental guidelines.
- Evidence Evaluation Techniques establish the completeness, relevance and quality of assurance evidence. Evaluation techniques are performed by objective evaluators who analyze evidence to verify assurance claims. Examples of evidence evaluation techniques include design analysis, test coverage analysis, and traceability analysis.

Note that many different people or organizations might perform these techniques. The burden of proving that a system is trustworthy may be shifted to the developer, evaluator, user, or buyer. Maintaining independence of evidence producers and evidence evaluators will help to reduce conflicts of interest.

### 5. A Framework

Determining the right mix of assurance evidence to establish that a product or system is trustworthy can be challenging. There are many possible tradeoffs in making these decisions.

The framework illustrated in the following table provides a structure for mapping existing assurance sources to each of the assurance types. Examples of assurance evidence for each category are provided, but there are many more. This framework is intended apply equally well to products, systems, mechanisms, components, etc...

Note that there is no indication of which assurance source is best. While one customer may rely heavily on system evidence, others may want process, people, and/or environment evidence.

Assurance Sources				
Assurance Types	System	Process	People	Environment
Correctness	Design Docs Test Results Mappings	CM Plans Standards Peer Reviews	Developers Trained Performance	Design Tools Access Logs CM Tools
Effectiveness	Penetrate C&A Vuln. Analy.	Risk Plans Test Plans Sec. Concept	Bkgd Checks Credentials Designers	Audit Logs System I&A Test Facility
Usability	User Trials Prototype Testing	Training Pln Test Plans HFE Plan	Credentials Trained HF Engineers	Tools Standards Test Facility
Workmanship	Probs. Found Improvements Measurements	QA Plan State-of-Art Standards	Commitment Corp. Cult. Independence	Prob. Rpts. Lab Plan Resource Pln

Table 1: Determine assurance type needed...  
...then choose best assurance sources

Note that this table could be expanded to distinguish evidence development techniques from evidence evaluation techniques, but this tends to confuse the picture.

## 6. Tradeoffs

Most users and buyers have not identified the types of assurance they need in terms of the system, processes, people, and environment areas. They only want to know that they are not taking inordinate risks with their assets. Fortunately, this allows a great deal of flexibility in determining the best way to develop and evaluate assurance evidence.

We believe that some assurance techniques are interchangeable. For example, if the process evidence shows that a development organization is following a very rigorous process, considerably less system evidence may be required. Likewise, if a product is to be developed by highly untrustworthy people, more system evidence is probably warranted.

On the other hand, we doubt that it is possible to identify two categories of assurance evidence that are always interchangeable. Choices are relative to the particular product or system being developed. The right choices establish

the desired confidence in the fastest, least expensive, and highest quality manner.

## 7. An Example

Imagine the security needs of a health care provider who wants to move to a computer-based record-keeping system. At risk are the integrity, confidentiality, and availability of their information. Fortunately, they are willing to consider any combination of system, process, people, or environment assurance evidence.

One possible approach is to evaluate the system and documentation to establish a high level of confidence that the system has no flaws. However, this approach requires extensive analysis to verify the design and implementation.

Another option is to examine the process, people, and environment used in operating the system. This approach examines process descriptions, plans, background checks, and system configuration to establish confidence that the system is not exposed to many threats.

Neither of these approaches is likely to be the most efficient. In most real world cases, some amount of evidence from each of the categories is probably needed. The important point is that different types of assurance evidence can be combined or traded as long as the result meets the assurance need.

## 8. Further Research

The TCSEC was never intended to measure many of the types of assurance described above. Additional metrics need to be defined to enable measurement of each type of technique and evidence.

Each of the assurance areas identified in this paper can be subdivided into many additional categories. For example, each of the areas can be divided into categories addressing correctness and effectiveness. Also, evaluation techniques might be subdivided among product and system techniques.

It may be possible to extend this framework to include the relationships with threats, assets, and risks. Perhaps a set of high level risk categories can be established and mapped to assurance types. The role of security policy in this area should also be explored.

## 9. References

- GAL94 Gallagher, Lisa, "Process Assurance", International Invitational Workshop on Developmental Assurance, June 26-27, 1994.
- LAN94 Landoll, Douglas J., Ferraiolo, Karen M., Sachs, Joel E., "Process as a Measure for Assurance Using the Security Engineering Capability Maturity Model", Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness. March 21-23, 1994.
- NIS94 NISTIR 5472. "A Head Start on Assurance," Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness. March 21-23, 1994.
- WIC94 Wichers, David R., Sachs, Joel E., Landoll, Douglas J., "What Color is Your Assurance", Seventeenth National Computer Security Conference, October 11-14, 1994.
- WIL94 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.