TRENDS AND ADVANCES IN THE INFORMATION ASSURANCE ANALYSIS USING SYNTHETIC EVALUATION METRICS

Lt. col. lect. univ. dr. ing. Cezar Vasilescu

Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Universitatea Națională de Apărare „Carol I”

Abstract

Today, the information systems based on computer networks are more and more used to transfer data and information essential to the success of military operations. A topical issue is to develop some metrics that can uniformly apply accurately captures the degree of security of information transfer. The purpose of this paper is to present the current state of international research in the domain of information security metrics, the analysis of current contributions and difficulties in identifying and developing these metrics. The central aim of this paper is to provide a basis for evaluating the existing classifications and to propose a unitary classification that allows for the quantification of the degree of information security.

I. INTRODUCTION

Recently, there has been some effort in utilizing quantitative indicators in a more systematic, coordinated fashion to capture the state of a particular Information Technology infrastructure. Such indicators are intended to reflect the "assurance" of the IT infrastructure to reliably transfer information. These

indicators can be used to identify areas of the information infrastructure that require attention. They can also be used by an IT organization as a means of gauging the return on investment for IT Infrastructure equipment purchase.

Despite the existing work that is underway, there is currently no standard or widely accepted method of capturing and presenting the assurance levels associated with a particular IT infrastructure œ this includes end-hosts, servers, applications, routers, firewalls and the network that allows these systems to communicate. A comprehensive, standardized set of quantitative metrics and indicators would be useful in order to identify areas of the IT infrastructure that are candidates for enhancement and pro-actively implement improvements to the IT infrastructure.

There have been a number of recent industry and research initiatives to develop standardized ratings that would reflect the Information Assurance associated with a specific product or product development process. For example, the Common Criteria (CC) [5] defines a set of rating levels (EAL 1 to EAL 7) which certify a particular vendor *product's security rating*. The ratings serve as a comparative platform that the consumer can utilize when comparing security products of various vendors. There has been good progress in developing product ratings, but little effort in developing a rating or indicator for a Network Infrastructure as a whole. Development of such an indicator remains very much a challenge for a number of reasons.

A first challenge is to arrive at a suitable definition of *Information Assurance.* The definition would then be used to identify key properties of the IT infrastructure that need to be assessed in order to develop a unified indicator or IA metric. Another challenge is that Information Assurance (IA) remains a subjective domain, because the assurance level of a specific piece of IT infrastructure is assessed through intuitive considerations by experts who are familiar with the protocols, architecture and systems utilized in the network.

This paper presents a new definition of Information Assurance and then uses that definition to develop a taxonomy of IA metric groups that would serve to assess the IA rating of IT infrastructure. The intention is to develop *quantifiable measures of Information Assurance* that allow objective analysis and comparison of a particular IT infrastructure in relation to itself over time. The next step would be to develop standardized metrics that can be used to compare the IA rating of an IT infrastructure with itself over time or against other IT infrastructure [9].

II. DEFINITIONS OF INFORMATION ASSURANCE

The term *"Information Assurance"* (IA) is widely used in industry and academia, often with widely varying and divergent understanding of its meaning. There can be suggested three key elements that can constitute the basis of a comprehensive definition of IA when applied against IT infrastructure. These three elements are *Security*, *Quality of Service* and *Availability*. Figure 1 provides an overview of those three key elements and also provides examples of *metrics* or indicators for each element.

Let's see why each of these three elements is important when considering a definition of IA:

- *Security* - can be considered as the ability of a system to protect information and system resources with respect to confidentiality, integrity and authentication. Security also includes vulnerability to active attacks by malicious users, viruses, denial-of-service, access lists, non-repudiation, privacy etc. Availability is sometimes considered part of security, however it can be considered as a separate element, because its definition could also include other factors.
- *Quality of Service (QoS)* - QoS is typically used to reflect the perceived performance of a service in relation to the expected performance. For the purpose of this paper, the performance properties used to describe an IT

infrastructure's Quality of Service include consideration of such indicators as bandwidth, latency, priority over other traffic or users, data loss rate etc. The QoS of a network is a strong contributing factor to its ability to assure the delivery of data from one end of the network to the other.

- *Availability* - Availability of the IT infrastructure is used to reflect its dependability or reliability. Thus, while QoS reflects how a network or system performs, availability reflects whether the network or system can even offer the lowest of service qualities. We consider the following attributes and factors as contributing to define the availability of a system: infrastructure downtime, mean-time between failures (MTBF), self-healing properties of a network/system and the ability of the network or system to operate under catastrophic disasters.

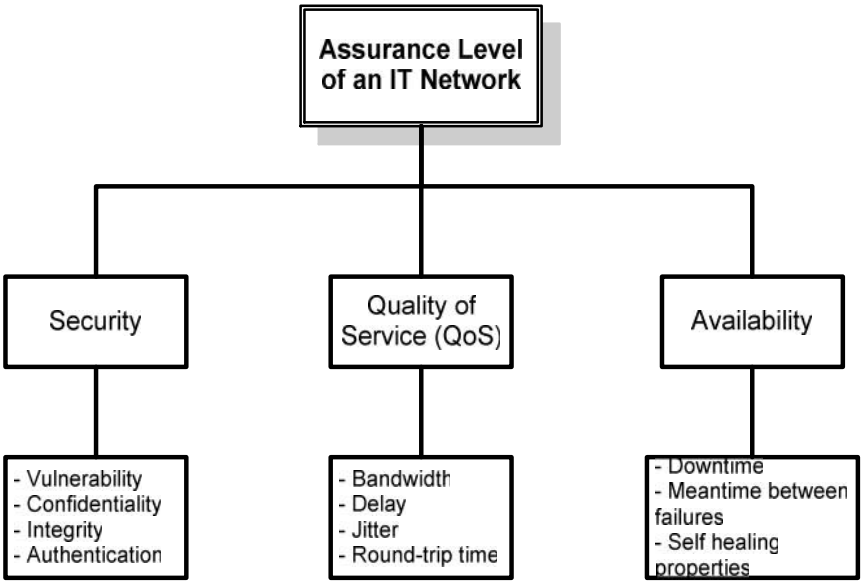

Figure 1. Elements of the Information Infrastructure Assurance.

Various definitions of IA can be found in the literature [8]. The most suitable definition of **Information Assurance** (for the purposes of this paper) could be the following: *„Information Assurance is the ability of a network or system to facilitate the timely transfer of information between two or more parties in an accurate and secure fashion".*

In the next sections, a new taxonomy of IA metrics groups will be proposed based on the above definition. Consequently, it will then be possible to use the taxonomy to develop IA metrics that allow organizations to determine their IT infrastructure‘s IA level, based on the network and system‘s ability to meet their requirements for Security, QoS and Availability.

III. EXISTING STUDIES, TRENDS AND TOOLS

There are three distinct types of US efforts related with the area of Information Assurance Metrics that take place in the following environments: government, university and industry.

A. USA Government Research Agencies

In the late nineties, the United States Defense Advanced Research Projects Agency (DARPA) organization funded a number of exploratory research projects in the area of IA metrics.

One of the projects analyzed some of the challenges facing researchers seeking to develop a set of IA metrics [10]. There is a clear need to develop an integrated environment for IA metrics by defining their purpose, meaning, units, range of values, and inherent taxonomies. The primary initial goal is to identify IA metrics that are measurable, testable and useful and then focus on moving as many of these metrics as possible towards the quantitative side of the scale.

Another project tried to apply a fundamental science-based approach to the problem of IA metrics. The use of Kolmogorov complexity was proposed as a basis for depicting the health of a security system [6]. Using a complexity-based method to depict the health of a system has the advantage that it is a fundamental property of information and can thus be applied without detailed knowledge of the system being analyzed, but additional work is required to extend the applicability of this approach to IT Networks.

Another initiative is the US government‘s National Institute of Standards and Technology (NIST) has recently developed a guide to security metrics for

information technology systems [11]. In this work, the authors provide guidance that an organization can utilize to measure the effectiveness of security-based controls and techniques. The authors propose a seven-step process that an organization can use to develop its own IA security metrics.

The MITRE Corporation is another government funded organization with research in the area of IA metrics. MITRE was the co-sponsor of a workshop on security metrics - Workshop on Information Security System Scoring and Ranking (WISSRR) [12]. In the workshop's papers, it was highlighted some of the challenges for the information system security engineering community as they related to the area of IA metrics [3]. It is important to clarify the IA assessment goals and scope, because the approach for a specific set of IA metrics may differ depending on the goals and scope.

Another paper was focused on the distinction between "*measures*" and "*metrics*" [1], and [2] described the approach taken by the United States Internal Revenue Service to develop security metrics as a basis of conducting an evaluation of its cyber security program. The IRS established taxonomy of metrics that consisted of 15 categories of security metrics.

B. University Research

The Information Assurance group at Mississippi State University has been conducting research in the area of IA metrics for a number of years. The findings and observations of the WISSRR 2001 workshop on security metrics were summarized [13]. Among the findings that they highlighted was the different uses that government and commercial sectors have for IA metrics. The workshop participants came to the conclusion that there does not exist a single set of IA metrics that are applicable across various systems. They also observed that the number of quantitative IA metrics were at present in short supply.

A taxonomy of IA metrics was proposed, that can serve to provide a framework for development of metrics and their inclusion in an evaluation or assessment framework. The authors suggest that there are five ways of viewing

specific IA metrics: objective/subjective, quantitative/qualitative, static/dynamic, absolute/ relative and direct/indirect. The most interesting part of this paper appears to be the sections that focus on the proposed IA metrics taxonomy as this provides a basis for commentary and future work.

C. Industry - Common Criteria

There have been a number of collaborative commercial efforts to define standards for the rating and assessment of security systems. To date, most such efforts have resulted in standards that assist in rating specific vendor products. They do not yet have standards which rate complicated systems such as an IT network. This is to be expected, as it is difficult to gain widespread acceptance of a standard means of evaluating a set of products. It is expected that in the future such efforts may focus on standard means of evaluating and rating the IA of IT networks as a whole.

One such industrial effort which is gaining momentum in terms of practical deployment is the Common Criteria (CC) initiative [4]. The CC is based on a combination of several other national standards for security, including:

- TCSEC (Trusted Computer System Evaluation Criteria);
- ITSEC (Information Technology Security Evaluation Criteria);
- CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) and
- FC (Federal Criteria for Information Technology Security).

In particular, the CC has defined Evaluation Assurance Levels (EAL) certification that provides the consumer with a basis on which to compare security ratings of various vendor products. Microsoft Windows 2000 and Sun‘s Solaris 8.0 are among the products that have received EAL certification. The use of CC is still not widespread and at present it is unclear if CC will achieve widespread commercial adoption.

D. Industry - Tools

Multiple inputs are required in order to derive a set of indicators that capture the IA posture of an IT network. Due to the complex nature of an IT network and the many inputs, it would be useful to have a single software-based data fusion tool that would serve to receive the inputs, undertake the transformations and arrive at the quantitative indicator that would capture the IA health of the network. There are no tools currently available that can undertake the scope of IA evaluation that is proposed. However, in [7] it was described a prototype next generation IA tool that correlates and collects results from multiple IA tools into a single assessment of a network‘s security posture.

There has been significant progress in developing automated tools to routinely and systematically undertake measurements and tests on an IT network. Such tools would provide the input to the data fusion tools.

With regard to such automated tools, there are a wide variety of security related assessment tools. These tools probe a network for security weakness, reporting what security hazards are present. It should be mentioned that there are still no standards in the area of what type of tests to be conducted though there are many types of tests that are commonly used across a variety of tools. There are also a number of tools available that measure another aspect of IA as it was defined - the QoS performance of a network. The tools test such things as QoS performance metrics including Internet delay, round trip time, packet drops, and application quality from the users’ perspective.

There are fewer tools available to measure the third aspect of IA as it was defined - availability and reliability. Availability of an IT network is in general, harder to measure than other aspects of the network. If a network seems to be always available to its users and has never failed, how would one classify its level of availability and reliability? The tools focusing on these areas cover issues such as network segment outages, associated services affected that outage, associated services that were not impacted by that outage, data storage problems, bit error rates etc.

IV. PROPOSED TAXONOMY TO EVALUATE INFORMATION ASSURANCE OF COMPUTER NETWORKS

In this section, it is proposed a new taxonomy for IA metrics that can be applied to assess a computer network. The proposed taxonomy is based on the definition of IA presented before. The evaluation of an IT network's IA health should include an assessment of its network *availability* and *QoS* aspects in addition to aspects of *information security*. Figure 2 captures the highest levels of the IA taxonomy tree.

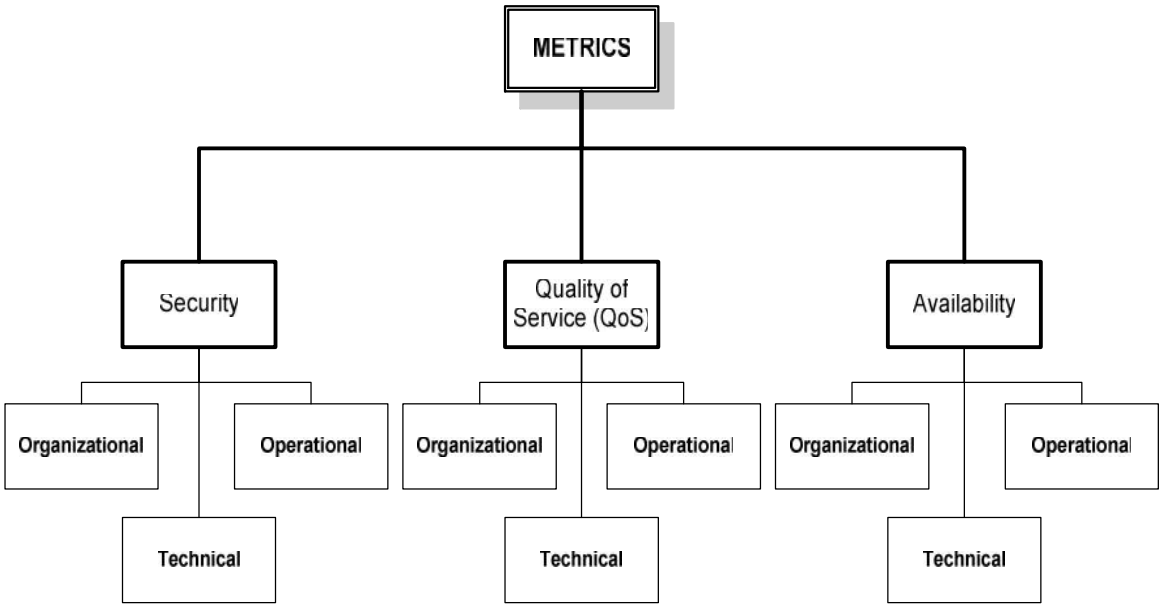

Figure 2. Proposed Information Assurance Metrics Taxonomy for Computer Networks.

The metrics space is divided into three categories: Security, QoS, and Availability. Under each of these three we consider the different technical, organizational, and operational aspects. Each of these sub-categories are further divided into another level of this tree. More details can be found in the following subsections (A, B, C and D).

The top level of the taxonomy tree has been deliberately organized as in Figure 2 in order to allow the assessment of a subset of the IA aspects. If the

organization only wishes to focus on the operational aspects of security, it can do so without having to undertake measurements related to QoS or technical security.

A. Sub-Categories of the Taxonomy Tree

The proposed definitions and use of the three sub-categories in the second level of the IA taxonomy tree differs slightly from those used in the NIST and WISSRR taxonomies. Below are presented the meanings for each sub-category:

- *Organizational Management*: this group of metrics evaluates an IT organization‘s emphasis on IA (in terms of goals and policies) and its commitment to IA (in terms of allocated resources).
- *Technical Elements*: this group of metrics evaluates how the technical components of an IA network are capable of providing IA. A subset of this group is static which provides a rating of the technical components capabilities in relation to IA. The remaining metrics under this group are dynamic as they are measured at different points in time after the IT infrastructure is deployed.
- *Operational Practices*: this group of metrics evaluates the operations of an IT organization in terms of complying with the IA goals and policies set by that organization.

In some cases, it is possible to argue that certain metrics could go under more than one category or sub-category of the taxonomy metric tree. Though it is possible to set out objective criteria that determine which part of the taxonomy tree a metric falls under.

Each of the three categories below Security, QoS and Availability is further broken up into metric sub-categories. The full IA taxonomy along with sample metrics is available in [14], but due to space limitations, only the technical elements sub-tree of the other categories will be discussed.

B. Security - Taxonomy

The security metrics attempt to quantify the process of evaluating each sub-category of characteristics for the IT network - *Organizational Management*, *Technical Elements*, and *Operational Practices* (Figures 3a, b). The figures depict the parts of the security taxonomy and captures how each of the metrics sub-categories are organized.

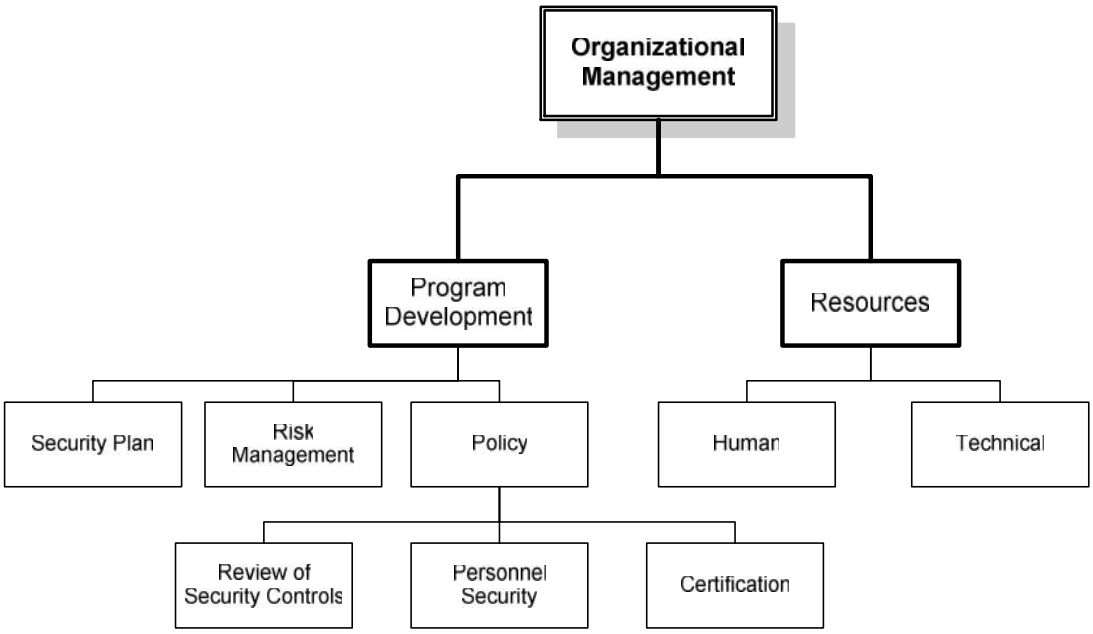

Figure 3 a. Security Metric Taxonomy: Organizational Management.

The Organizational Management Program Development metrics evaluate the development of the organization‘s security program:

- The Security Plan checks whether the organization has a security plan in place and how often it is updated;
- Risk Management checks whether risk is periodically assessed and how many departments have risk assessment procedures in place;
- Policy checks the organization‘s security policy by considering the following subgroups;

- Review of Security Controls checks the levels of personnel access controls to different resources and how often security controls are reviewed;
- Personnel Security checks the required level of personnel background checking before hiring them. This issue will have different levels of relevance according to the type of infrastructure and the organization‘s activities;
- Certification checks the certification level requirements set by the organization. This includes the certification required for the personnel‘s technical capabilities as well as the certification required.

The Resources sub-category deals with the quality and the quantity of the resources allocated to the organization‘s security, both human and technical:

- Human metrics evaluate the resources allocated for the developing the organization‘s security human resources;
- The Technical metrics evaluate the resources allocated towards the organization‘s security technical resources (software, hardware, and networking).

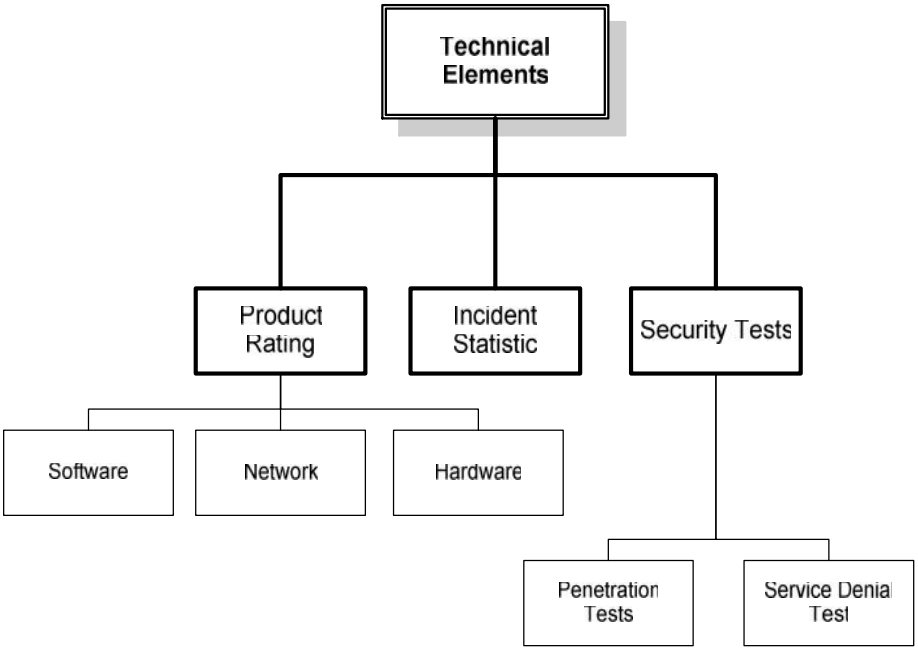

Figure 3 b. Security Metric Taxonomy: Technical Elements.

The Technical Element Product Rating sub-category is intended to assess the security rating of the products used in the infrastructure:

- Software metrics assesses the security ratings of the software products used on the network;
- Network metrics assesses the security ratings of networking equipment such as routers or switches either based on recognized standards or a pre-established set of required features;
- Hardware metrics check the security ratings of the hardware systems such as servers and desktops.

The Incident Statistics sub-category is intended to assess security incident statistics collected from the deployed systems. These statistics should be indicative of the effectiveness of the technical elements.

The Security Tests sub-category is intended to assess how the IT network copes with a variety of security-related tests:

- The Penetration Test sub-category is intended to actively test the capability of the network to keep out malicious users who do not have the requisite privileges to access or control parts of the IT network;
- The Service Denial Test sub-category is intended to assess the level of service provided by a network during active tests to bring down parts of the it due to security problems.

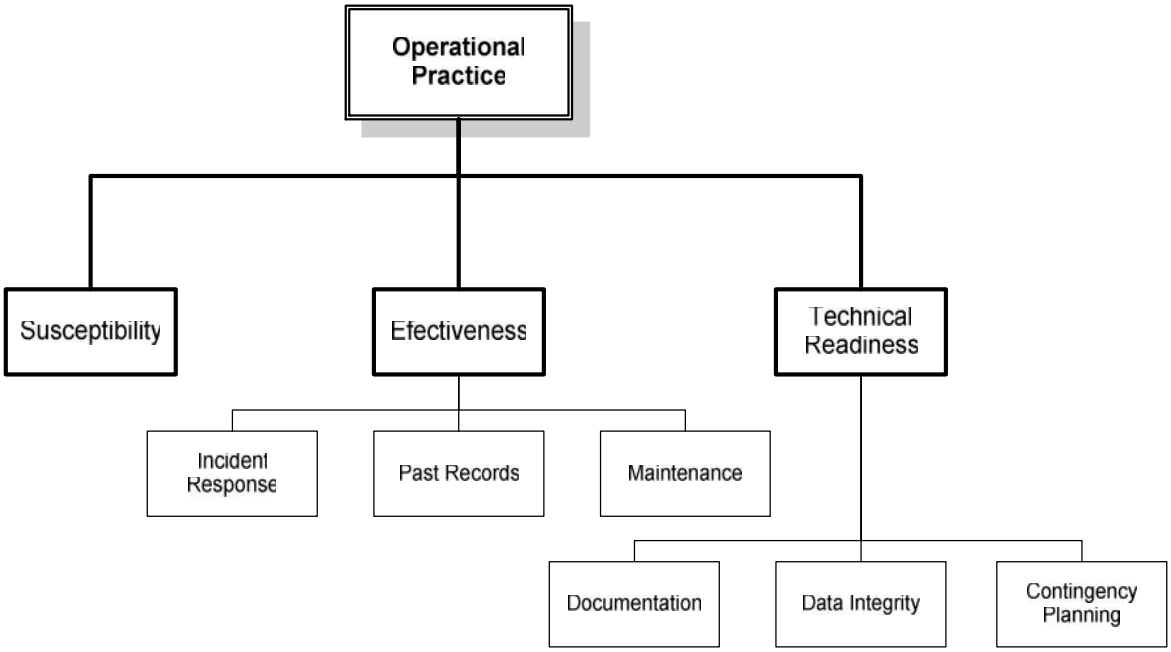

Figure 3 c. Security Metric Taxonomy: Operational Practice.

The Operational Practice Susceptibility group of metrics assesses the infrastructure security vulnerability due to its existence in a certain environment.

Effectiveness checks the effectiveness of the security operational practices:

- Incident Response checks the capabilities of responding to security incidents;
- Past Records checks the archiving process for past records of operational practices and measurements. It also evaluates the examination of system logs to check the system effectiveness;
- Maintenance checks the effectiveness of the security maintenance of software, hardware, and networking equipment.

Technical Readiness checks the technical readiness of the security operations:

- Documentation checks and evaluates documentation of the security operations;
- Data Integrity checks and evaluates regulations for insuring the integrity of the data;

- Contingency Planning checks and evaluates the contingency plans of the security operations.

C. QoS Technical Quality of Service

Technical Elements metrics are intended to assess QoS performance characteristics of the network and its associated elements. These metrics evaluate the taxonomy leaf properties in a quantitative fashion to facilitate unambiguous and clear indications of QoS network performance. Figure 4 depicts this part of the proposed IA taxonomy sub-tree.

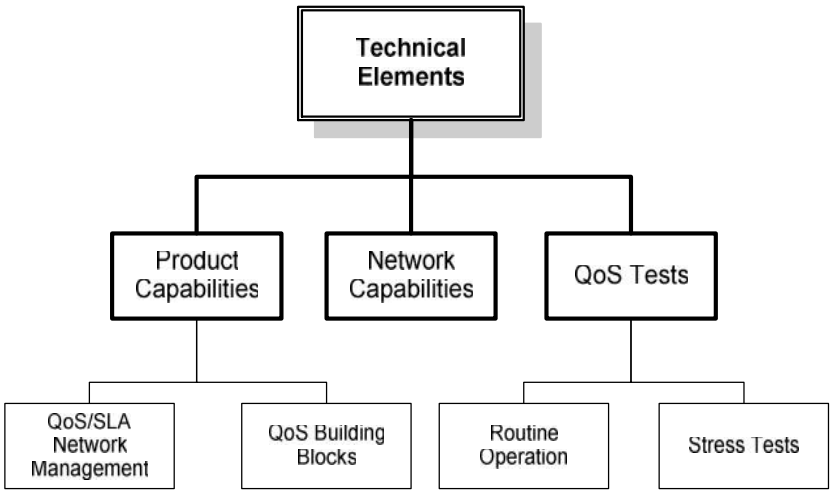

Figure 4. QoS Elements Metric Taxonomy.

The Product Capabilities sub-category is intended to assess whether products deployed in the network have the requisite features to allow the identified QoS characteristics to be achieved:

- In this regard, QoS/SLA Network Management metrics grade the QoS features of the network management software. These include such properties as configuration and monitoring, policy enforcement, and specification of service level agreement (SLA) support;
- QoS Building Blocks metrics ensure that the network devices include various required QoS building blocks such as multiple queues, priority

scheduling, traffic conditioning and policing, differentiated services support, and buffer management.

The Network Capabilities sub-category is intended to assess whether the network as an end-to-end entity contains the requisite capabilities to provide QoS. A network that contains both QoS capable and non-QoS capable devices may only be able to offer a certain level of QoS.

The QoS Tests sub-category is intended to assess the extent to which the network manifests the desired level of QoS:

- Routine Operation metrics assess the characteristics of the network under normal operating traffic loads. They are intended to reflect the extent to which the actual QoS behavior compares against the required QoS characteristics. These metrics include such things as amount of data lost through congestion, end-to-end delay etc.
- Stress Tests metrics are intended to assess the network‘s capability to handle situations when it is stressed outside of normal operating conditions. The metrics are based on executed tests that help identify weak spots in the network.

D. Availability - Technical

The Network Availability technical metrics are intended to assess the availability characteristics of the network. Network Availability technical elements part of the IA taxonomy sub-tree is shown in Figure 5.

The Redundancy sub-category is intended to assess the degree of Network Availability that is achievable with the current network infrastructure:

- The Product metrics assess the product properties of each network device such that the required network availability is achievable. These properties include such features as high reliability, load balancing, fault detection, and protection switching;

- Network metrics determine whether the specified degree of network availability for the network as a whole is achievable. A network may have devices that can do protection switching, but the network may not be designed such that they can be used.

The Availability Tests sub-category assesses the level of Network Availability attained under active tests:

- Routine Operation metrics are intended to reflect the characteristics of the network under normal operating traffic loads. These metrics compare the actual Network Availability versus the desired Network Availability. These metrics include downtime (frequency, length, and severity), uptime, and end- user feedback;
- Stress Test metrics are intended to reflect availability characteristics of the network under active stress testing. i.e. when the network is stressed outside of normal operating conditions. Tests are executed to help identify weak spots in the network and ensure that the availability is guaranteed.

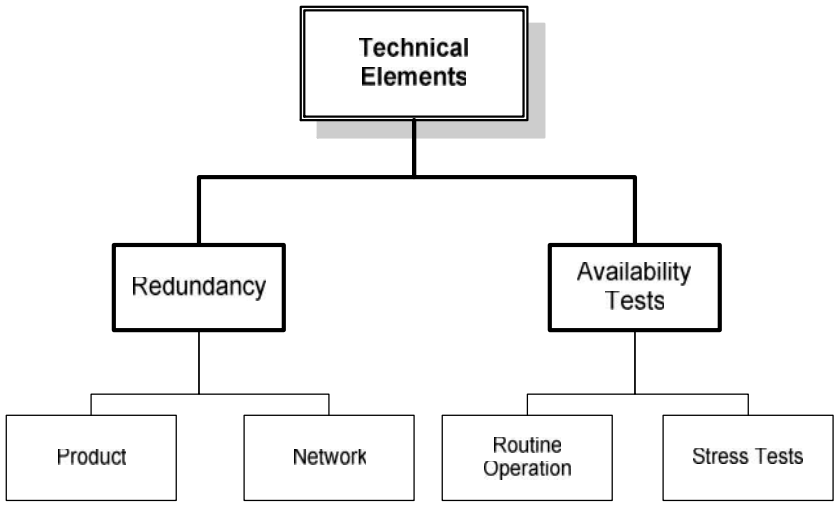

Figure 5. Availability Technical Elements Metric Taxonomy.

V. CONCLUSIONS

The survey in the area of Information Assurance Metrics indicated that it is an emerging area which should be given considerable attention in the coming years as the reliance on IT infrastructure continues to grow. Most of the research undertaken so far has focused on the security aspect of IA metrics. This paper evaluated and analyzed three previously proposed specific taxonomies and sets of IA metrics.

The taxonomies had their strengths and weaknesses, but overall none were sufficient to be used to assess the IA posture of an IT network. This paper proposed a new definition of *Information Assurance* that was based on three key attributes related to IT infrastructure:

- Security
- Quality of service and
- Availability.

The ability of an IT network to deliver information from one user to another is dependent on all three factors. Therefore, a new taxonomy and category of metrics that could be utilized for the specific purpose of capturing the Information Assurance rating of an IT network was proposed.

This taxonomy divided the Information Assurance Metrics aspects of a network into three categories: Security, QoS, and Availability. Each of these categories in turn was subdivided into three sub-categories: Organizational measures, Technical Elements, and Operational Practices.

The area of Information Assurance evaluation and assessment is a complex one. Future efforts should be concentrated to develop an IA framework along with sample metrics and measurement methodology, probably integrated in an expert system tool.

IV. REFERENCES

[1]. Alger J. - *"On Assurance, Measures and Metrics: Definitions and Approaches"*, Proceedings of WISSR 2001, May 21-23, 2001, Virginia.

[2]. Bicknell P. - *"Security Assertions, Criteria and Metrics Developed for the IRS"*, MITRE Technical Report, May 2001.

[3]. Bodeau Deborah - *"Information Assurance Assessment: Lessons Learned and Challenges"*, Proceedings of WISSR 2001, Williamsburg, Va, May 2001.

[4]. *** - *"Common Criteria"*, http://csrc.nist.gov/cc/index.htm

[5]. *** - *"Common Classification Criteria"*, http://www.commoncriteria.org

[6]. Evans S, Bush S and Hershey J. - *"Information Assurance through Kolmogorov Complexity"*, DARPA Information Survivability Conference and Exposition II (DISCEX-II-2001) 12-14 June 2001, Anaheim, California.

[7]. Fox K, Henning R, Farrell J, and Vaughn R. - *"A Prototype Next Generation Information Assurance Tool - A DataFusion Model for Information Systems Defense"*, White Paper, Harris Corporation, 2003.

[8]. McKnight W. - *"What is Information Assurance"*, CROSSTALK, The Journal of Defense Software Engineering, July 2002.

[9]. Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, I., Hatfield, A. - *"Current Trends and Advances in Information Assurance Metrics*", Proc. of the 2nd Ann. Conf. Privacy, Security and Trust (PST 2004), Fredericton, NB, Oct., 2004.

[10]. Skroch M, McHugh J and Williams JM - *"Information Assurance Metrics: Prophecy, Process or Pipedream"*, Workshop, National Information Systems Security Conference (NISSC 2000), Baltimore, October 2000 .

[11]. Swanson M, Nadya B, Sabato J, Hash J and Graffo L. - *"Security Metrics Guide for Information Technology Systems"*, National Institute of Standards and Technology Special Publication, July 2003.

[12]. *** - *"Information System Security Attribute Quantification or Ordering"*, Workshop on Information, Security System Scoring and Ranking (WISSSR, 2001), May 21-23, 2001,Williamsburg, VA.

[13]. Vaughn, Rayford, Ambareen Siraj, and David Dampier - *"Information Security System Rating and Ranking"*, CROSSTALK, The Journal of Defense Software Engineering, May 2002, pp. 30-32.

[14]. Nandy B, Pieda P, Seddigh N, Lambadaris J, Matrawy A, Hatfield A. - *"Information Assurance Metrics"*, Technical Report prepared for the Canadian Federal Government Department Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), March 2004.