Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2010

Cyber Forensics Assurance

Glenn S. Dardick
Longwood University, USA

Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/77

Cyber Forensics Assurance

Glenn S. Dardick[1,2]
[1]Longwood University, USA
gdardick@dardick.net

[2]secau - Security Research Centre
Edith Cowan University
Perth, Western Australia

Abstract

As the usage of Cyber Forensics increases, so does the potential for errors in the practice of applying Cyber Forensic. Errors in opinions derived from faulty practices have resulted in grievous miscarriages of justice. However, utilizing the foundations of Information Systems Assurance and Information Quality, a solid foundation for improving the quality and effectiveness of Cyber Forensics can be derived. The foundations of Information Systems Assurance and information Quality provide a solid foundation for improving the current efforts in Cyber Forensics. With increasing computer and network systems usage as well as the increasing frequency of attacks on information systems, the need for controlling risks in information systems have become more apparent. Meeting that need, Information Systems Assurance has continued to evolve: from the CIA (confidentiality, integrity, and availability) into variations such as the five pillars (confidentiality, integrity, availability, authenticity, and non-repudiation) and the Parkerian Hexad (confidentiality, integrity, availability, authenticity, possession, and utility). Also, with the continuing growth of information systems, the need for improving the quality of such systems has also evolved focusing on various components of information Quality (accuracy, relevance, consistency, timeliness and completeness). Utilizing the foundations of Information Systems Assurance and information Quality a model is derived for Cyber Forensics Assurance.

Keywords

Cyber forensics assurance, digital forensics, cyber forensics, information assurance, information quality

INTRODUCTION

It is not uncommon in today's legal environment to have unsuccessful prosecutions based upon the faulty presentation of Cyber Forensics evidence and the resulting opinions and testimony given by "expert" witness. In defining unsuccessful, we can refer to cases where the guilty is not proven guilty or where innocent people are "proven" guilty when in fact they are not. These cases come to light when, ultimately, the opinions given and relied upon are repudiated. As such, the risk of repudiation needs to be minimized. Cyber Forensics Assurance is about reducing the risks of repudiation.

"There is nothing more deceptive than an obvious fact."
Sherlock Holmes in The Boscombe Valley Mystery

THE LEGAL ENVIRONMENT

In terms of research methods, it is hopeful that a better understanding of the assurance of computer forensics will result in better prosecutions of the guilty (having less Type II errors - or letting the guilty off) and less mistakes in finding innocent people guilty of actions they did not commit (having less Type I errors - or "proving that which isn't so").

"Guilt" as Hypothesis

Guilt can be viewed as a hypothesis - one that states that someone's actions are responsible for a certain consequence(s).

The "Null" Hypothesis

If guilt is the hypothesis, then the "Null" hypothesis is one which shows there is no relationship between one's actions and the consequences in question.

“Innocent Until Proven Guilty” and the Burden of Proof

Under U.S. law, one is considered innocent until proven guilty. In research terms this would be equivalent to having to reject the “Null” hypothesis to prove guilt. In effect, we are proving that the defendant is “not innocent”. The defendant does not need to prove the “Null” hypothesis - however, the prosecutor needs to prove that the “Null” hypothesis needs to be rejected.

Type I Errors - False Positives

Incorrectly rejecting the “Null” hypothesis when in fact it is true is referred to as a Type I error, or a false positive. In effect, by rejecting the “Null hypothesis” we are proving that the defendant is not innocent. By incorrectly rejecting the “Null” hypothesis, we are falsely proving guilt when in fact the defendant is innocent.

Type II Errors - False Negatives

Not rejecting the “Null” hypothesis when in fact it is false is referred to as a Type II error, or a false negative. In effect, by not rejecting the “Null hypothesis” we are not able to prove that the defendant is not innocent. By incorrectly not rejecting the “Null” hypothesis, we are unable to prove guilt when in fact the defendant is not innocent

Blackwell’s Formulation

The legal system’s willingness to accept Type II errors in lieu of accepting Type I errors is based upon Blackstone’s Formulation.

"Better that ten guilty persons escape than that one innocent suffer."

William Blackstone, English jurist 1760’s

However to minimize the risk of either Type I or Type II errors an emphasis should be placed upon Cyber Forensics Assurance or minimizing the risk of repudiation. By minimizing the risk of repudiation, we maximized the quality of the Cyber Forensics analysis.

INFORMATION SECURITY (IA)

The Cyber Forensics Assurance Model herein is based upon Information Assurance which itself has its root in Information Security. One of the earliest models, or definition, or Information Security is the CIA Triad.

CIA Triad - Information Security

The Federal Information Security Management Act of 2002 (FISMA) defined three security objectives for information and information systems [FIPS Pub 199]:

- Confidentiality
- Integrity
- Availability

Confidentiality is defined as “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.

Integrity is defined as “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.

Availability is defined as “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

Figure1. Information Security Components of the CIA Triad

Table 1. Potential impact definitions for each security objective—confidentiality, integrity, and availability [FIPS Pub 199].

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on Organisational operations, Organisational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on Organisational operations, Organisational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on Organisational operations, Organisational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on Organisational operations, Organisational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on Organisational operations, Organisational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on Organisational operations, Organisational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on Organisational operations, Organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on Organisational operations, Organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on Organisational operations, Organisational assets, or individuals.

INFORMATION ASSURANCE (IA)

Information Assurance (IA) evolved from the definitions and concepts of Information Security. One of the initial definitions of Information Security is referred to as the CIA Triad. Later, Information Assurance incorporated the CIA Triad into a definition of Information Assurance referred to as the Five Pillars.

Five Pillars of Information Assurance

The Five Pillars of Information Assurance model is defined by the U.S. Department of Defense (DoD) within the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. That publication defined Information Assurance as "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation

The Five Pillars model added to the CIA Triad model the attributes of authentication and non-repudiation which are not attributes of information or systems but are attributes used to describe the procedures or methods to assure the integrity and authenticity of information, and to protect the confidentiality of those same.

Authenticity is the attribute of being authentic or of established authority for truth and correctness (Verification) – genuine –not fabricated.

Non-repudiation is the attribute of assuring that the conclusions of an analysis are the complete and only relevant truth and cannot be repudiated.

Parkerian Hexad

The Parkerian Hexad, introduced by Donn B. Parker in 1998, also added to the CIA Triad model. Parker's Hexad adds the three attributes of authenticity, utility, and possession (or control). Confidentiality

- Integrity
- Availability
- Authenticity
- Possession or Control
- Utility

The attribute of authenticity in the Parkerian Hexad model, is not identical to the pillar of authentication as described in the Five Pillars.

Possession or Control may be defined as reliable while Utility is defined as usability or usefulness.

It is also noted that the Parkerian Hexad model does not include the Five Pillars attribute of non-repudiation.

INFORMATION QUALITY

Dimensions of Information Quality may be broken down in several ways including Intrinsic, Contextual and Representational. Several models exist focusing on different perspectives. Building upon the model of Fox (1994), Miller (1996) refers to several dimensions of Information Quality which can very well be applied to forensic information.

- Accuracy – “Is the information factual?”
- Relevance – “Is it the right information?”
- Consistency – “Is it right all of the time?”
- Timeliness – “Applicable to the appropriate timeframe?”
- Completeness – “The whole truth?”

Four of the five qualities of Information Quality are similar to various attributes in the Information Security and Information Assurance models while a fifth, Completeness, represents an additional attribute very relevant to Cyber Forensics testimony and can ultimately affect the attribute of Non-Repudiation.

FOUNDATION OF CYBER FORENSICS ASSURANCE

In defining Cyber Forensics Assurance relative to its importance to investigations, it is important to take into account both the quality of information as well as the security and assurance of that information and the methodology used in acquiring that information. Perhaps in the legal system, where ultimately such information will be used to determine whether or not culpability or guilt has been proven, it is imperative that such information should be of the highest calibre. Too often evidence is given which "could" be true, but could very easily be repudiated.

Synthesis

In establishing a model of Cyber Forensics Assurance, the CIA Triad, the Five Pillars of Information Assurance the Parkerian Hexad and the dimensions of Information Quality were reviewed and synthesized as in Table 2. While some attributes of quality for a Cyber Forensics examination and analysis are well know and often taught or covered through rules of evidence, there were still cases where the outcomes of a cyber forensics effort were not correct and were later repudiated. In reviewing which attributes were common among the four models used, it was hoped that while some attributes were already being utilized within Cyber Forensics efforts, that it would be evident that there were additional attributes which could be utilized in a Cyber Forensics Assurance model which could be used to improve future Cyber Forensics efforts and hopefully reduce the potential for Type I, II, III and IV errors.

Table 2. Foundations of Cyber Forensics Assurance

CIA	5 Pillars	Hexad	IQ	CFA	Components
●	●	●		●	Confidentiality – ensuring that information is accessible only to those authorized to have access
●	●	●	●	●	Integrity/Consistency – perceived consistency of actions, values, methods, measures and principle – unchanged "is it true all of the time?" (Verification)
●	●	●	●	●	Availability/Timeliness – the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time)
	●	●		●	Authenticity / Original – quality of being authentic or of established authority for truth and correctness – "best evidence" (Validity)
	●		●	●	Non-Repudiation / Accuracy – transaction cannot be denied (Validity) – no alternate hypothesis
		●		●	Possession / Control – i.e. chain of custody
		●	●	●	Utility/Relevance – "Is it useful? / is it the right information?"
			●	●	Completeness – "Is it the whole truth?"

CYBER FORENSICS ASSURANCE

In defining the model of Cyber Forensics Assurance, the eight attributes used in developing the foundation are logically paired into the model represented in Table 3.

Table 3. Model of Cyber Forensics Assurance

CFA	Components
I	a) Confidentiality – ensuring that information is accessible only to those authorized to have access
	b) Possession / Control – i.e. chain of custody
II	a) Integrity/Consistency – perceived consistency of actions, values, methods, measures and principle – unchanged "is it true all of the time?" (Verification)
	b) Authenticity / Original – quality of being authentic or of established authority for truth and correctness – "best evidence" (Validity)
III	a) Availability/Timeliness – the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time)
	b) Utility/Relevance – "Is it useful / is it the right information?"
IV	a) Completeness – "Is it the whole truth?"
	b) Non-Repudiation / Accuracy – transaction cannot be denied (Validity) – no alternate hypothesis

COMPONENTS OF THE CYBER FORENSICS ASSURANCE MODEL (CFAM)

In the Cyber Forensics Assurance Model (CFAM), eight components are defined and paired into 4 sections. The four sections are as follows:

- Section I
  - Confidentiality/Admissibility
  - Possession
- Section II
  - Integrity/Consistency
  - Authenticity/Accuracy/best evidence
- Section III
  - Availability/Timeliness
  - Relevance
- Section IV
  - Non-repudiation
  - Completeness

Section I of the CFAM includes the attributes of Confidentiality and Possession or Control. Confidentiality relates to the distribution of information while Possession or Control relates to the distribution of the media upon which the information resides. Confidentiality is becoming more of an issue in the Courts as privacy is recognized and Protective Orders are issued placing constraints on Cyber Forensic investigations. Violation of a protective order can result in sanctions or of evidence being inadmissible. Possession or Control relates to the general maintenance and verification of the chain of custody of evidence used in a cyber forensics investigation.

In section I, Confidentiality, is rooted in the CIA Triad of Information Security and both the 5 Pillars of Information Assurance and the Parkerian Hexad. Possession or Control however was added by the Parkerian Hexad and omitted in both the CIA Triad of Information Security and both the 5 Pillars of Information Assurance. Possesion is very much a part of Cyber Forensics Investigations due to the necessity of maintaining chain of custody while maintaining confidentiality has long been noted as a quality of professionalism in cyber forensics. As such section I of the CFAM has a foundation in the attributes Information Security and Information Assurance and consists of attributes already well-know and required in Cyber Forensics.

Section II of the CFAM includes the attributes of Integrity/Consistency and Authenticity/Accuracy. Authenticity/Accuracy is relative to the rules of evidence regarding hearsay as well as original or best evidence. Authenticity/Accuracy may be viewed as a way of maintaining Integrity/Consistency.

"We must look for consistency. Where there is a want of it we must suspect deception."
Sherlock Holmes in The Problem of Thor Bridge

In section II, Integrity/Consistency is rooted in the CIA Triad of Information Security and both the 5 Pillars of Information Assurance and the Parkerian Hexad. Authenticity/Accuracy was introduced as part of Information Assurance and not covered in the CIA Triad of Information Security. Authenticity/Accuracy has already been very much a part of Cyber Forensics Investigations due to its application to rules of evidence. Integrity/Consistency has also been very much a part of Cyber Forensics Investigations. As such section II of the CFAM also has a foundation in the attributes Information Security and Information Assurance and consists of attributes already well-know and required in Cyber Forensics.

Section III of the CFAM includes the attributes of Availability/Timeliness and Relevance. Determining the availability and timeframe of evidence is an important step in determining relevance. It is important to not only determine if facts are true, but whether they were true for the given timeframe and environment.

It is section III of the CFAM where the contribution of the Information Security model and the Information Assurance models begins to become apparent, especially when also compared to the Information Quality model.

"There is nothing more deceptive than an obvious fact."
Sherlock Holmes in The Boscombe Valley Mystery

There have been cases where facts are presented which may in fact be true, but have little to do with accepting or rejecting the "Null" hypothesis - that is whether or not a defendant's action(s) may be responsible for certain consequences. These errors could be because the facts were not relevant to the time period in question or may have had nothing to do the relationship between the defendant's action(s) and the consequence(s) in question. In research, these have been referred to as Type II and Type IV errors.

- **type III errors** - In 1974, Ian Mitroff and Tom Featheringham defined type III errors as either "*the error... of having solved the wrong problem... when one should have solved the right problem*" or "*the error... [of] choosing the wrong problem representation... when one should have... chosen the right problem representation*" arguing that "*one of the most important determinants of a problem's solution is how that problem has been represented or formulated in the first place*". (from Wikipedia - emphasis added)
- **Type IV error -** In 1970, L. A. Marascuilo and J. R. Levin proposed a "*fourth kind of error*" — a "Type IV error" — which they defined as being the mistake of "*the incorrect interpretation of a correctly rejected hypothesis*" (from Wikipedia - emphasis added)

Section IV of the CFAM includes the attributes Completeness and Non-repudiation – ensuring that the facts and conclusions of the analysis cannot be repudiated. Often "expert" witness opinions are dangerously given in which conclusions are inductive instead of deductive. Unfortunately, using inductive reasoning might determine that the facts support the conclusions the rather than determining that the facts support the conclusions *and only* those conclusions. If the facts can support another conclusion, then non-repudiation is a very real possibility. In determining conclusions, alternate conclusions (or alternate hypotheses) should be considered so as to provide a complete, or thorough, analysis.

"One should always look for a possible alternative, and provide against it. It is the first rule of criminal investigation."
Sherlock Holmes in The Adventure of Black Peter

In addition to section III, section IV also has a significant contribution from primarily the Parkerian Hexad model and the Information Quality model. The attribute added by utilizing the Information Quality model is the attribute of completeness. It is here that the idea of reviewing all potential "alternate" hypotheses against the "Null" hypothesis becomes tantamount to assuring Non-repudiation. In fact, the Guidelines for Expert Witnesses in the Proceedings in the Federal Court of Australia states "an expert witness does not compromise objectivity by defending, forcefully if necessary, an opinion based on the expert's specialised knowledge which is genuinely held … but may do so [compromise] if the expert is, for example, unwilling to give consideration to alternative factual premises or is unwilling, where appropriate, to acknowledge recognised differences of opinion or approach between experts in the relevant discipline." (emphasis added). Generally, Cyber Forensics professionals are professionally, and ethically, committed to being unbiased, but not necessarily oriented to the concept of non-repudiation. A greater recognition of the importance of Cyber Forensics Assurance, and specifically greater focus on assuring non-repudiation coud result in less Type I, II, III, and IV errors.

CONCLUSION

The definition of a Cyber Forensics Assurance Model (CFAM) is useful in understanding the attributes of a thorough, professional and successful investigation involving electronic evidence. The CFAM can be further developed to assist in the training of Cyber Forensics professionals as a way of conducting complete investigations which will be less prone to repudiation. In terms of research methods, it is hopeful that a better understanding of CFA will result in better prosecutions of the guilty (having less Type II errors - or letting the guilty off) and less mistakes in finding innocent people guilty of actions they did not commit (having less Type I errors - or "proving that which isn't so").

FUTURE RESEARCH AND APPLICATION

The application of the Cyber Forensics Assurance Model (CFAM) will hopefully result in a better understanding of how to conduct investigations compliant with the changing legal and technological landscape. As privacy becomes more and more of a "victim" in investigations, it is important to develop better methods in conducting investigations. The ongoing changes in technology also represent major challenges in conducting successful Cyber Forensic investigations. It is hopeful the CFAM can provide a framework in developing better methods to meet these challenges.