

Existing Integrity Concepts and Mechanisms and their Main Limitations - Bird's eye view

Vijay V. Mandke

Research Leader,

Center for Information Integrity Research,

Delhi Center: B-64, Gulmohar Park, New Delhi – 110 049,

Pune Center: Flat A-2, Nikash Skies, Someshwar Wadi, Pashan, Pune-4110 08

Visit us at: centerforinformationintegrityresearch.org

Information Integrity/Integrity Information System/Management Information System
Course Lecture # 34-35
2006-2007

Lecture # 34-35:
Existing Integrity Concepts and
Mechanisms and their
Main Limitations
- Bird's eye view

OVERVIEW - 1

- Plethora of Integrity Mechanisms
- Their Main Limitation
- Security based Definitional Approach to Integrity
- Accounting/ Auditing Research
- Quality Paradigm
- Communication Theory

OVERVIEW - 2

- Expected Utility Theory
- Summary of Main Limitations
- Exercises

PLETHORA OF INTEGRITY MECHANISMS

- Lecture # 8 Slide No. 8, observes that there exist a plethora of integrity mechanisms.
- Literature reports approaches to integrity studies from different angles such as:
 - Security based definitional approach to integrity,
 - Auditing research,
 - Process centered quality approach,
 - Noise reduction based technology under communication theory, and
 - Expected utility theory under decision-making.

THEIR MAIN LIMITATION

- The main limitation of these approaches is that the *IS* models considered do not address the issue of “economic” processing of information (information economics), which as argued in Lecture # 8 is the central point in integrity emerging as the key issue in the study of *IS* for competitive advantage.
- This lecture elaborates on this.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 1

- Database research community has always acknowledged impact of data errors on Databases, and accordingly there are concepts of Data Security and Data Integrity.
- However, Date distinguishes between the two by observing that while security involves ensuring that users are *allowed* to do the things they want to do, integrity involves ensuring that the things they are trying to do are *correct*.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 2

- In other words, security means protecting the database against *unauthorized* users, whereas integrity means protecting it against *authorized* users (direct as well as indirect).
- Indeed, integrity, unlike security, is applicable even in a single-user system (it is always desirable to avoid errors); and it is far more relevant when the system is shared.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 3

- With military requirements dominating the research in information systems, the issue of secured computer systems and of confidentiality of information gained a high priority query.
- As a result, for over forty years, there have been efforts to work on information security programs. Security has normally been taken to mean confidentiality, integrity and availability.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 4

- Researchers involved with information security issue are at ease with this terminology *except* that the meaning of the word "integrity" is not adequately resolved, the word being frequently used to describe a range of attributes (or requirements) such as:
 - validity of information in a computer system (Integrity Model by Biba, 1970);

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 5

- prevention by customer of unauthorized program from: circumventing memory protection mechanisms, avoiding access control mechanisms and obtaining supervisor state (IBM concept of System Integrity, 1981);
- preventing unauthorized modification of data (Lipner's Integrity Application, 1982);

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 6

- correctness and protection of Trusted Computing Base and Procedures (Trusted Computer System Evaluation Criteria (TCSEC, 1983);
- reliability, accuracy, faithfulness, non-corruptibility and credibility of information transmitted, protection from noise in communication systems and equipment failure, consistency, accuracy, concurrency, data recovery, modification access, credibility of information (The Network Interpretation (TNI) of Integrity, 1985);

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 7

- internal consistency of a system (a correctness aspect) and external consistency (correspondence with reality – an appropriateness aspect) (Clark-Wilson Integrity (CWI) Model, 1987);
- property of data which have not been subject to unauthorized alteration or destruction (Integrity Model of International Standards Organization);

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 8

- property of internal correctness of a system - error control objective, and property of correspondence to the real world – fraud control objective (Terry and Wiseman view of Integrity, 1989);
- correctness and consistency of data and their classification labels (Sea View Model of Integrity); etc.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 9

- A critical look at the research investigations reported above shows that, in addition to lack of precise Information Integrity attribute definition, there is a recurring realization that security and integrity are different in that the security policies are only concerned with controlling dissemination of information (confidentiality), while there is also the problem of the validity of information in a computer system - requiring control over modifications made to information (termed as integrity or correctness of information).

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 10

- In fact CWI model, which has provoked constructive reaction from within computer science fraternity and academia, suggests that:
 - separate policies are required for confidentiality and data integrity, and that,
 - with the exception of common requirements such as user authentication, much of the mechanism for supporting these two - security and (data) integrity - policies would also be different.
- There is also appreciation that integrity has two different notions involved: that of correctness and of appropriateness.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 11

- Further, concept of Trusted Computing Base (TCB) appears to be fundamental to above security and integrity definitions.
- However, literature in information systems research argues that *this is a narrow view of what constitutes integrity and it is confined within the logical bounds of an information system as it excludes the material impact of the people and business application processing necessarily involved in any system.*

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 12

- In fact, IFIP deliberations go to state that "the concept that a system can be trusted over time without the ability to provide the evidence that the trust is well placed is incompatible with internal control principles (so mandatory to safeguard assets from misappropriation and ensure reliable information systems)".

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 13

- Further, database integrity models and methods, while context specific, do not lend themselves to any comparative, analytical studies. In the computer security field, despite the Clark-Wilson model and the considerable integrity discussion it prompted, there is still nothing like coherent framework.

SECURITY BASED DEFINITIONAL APPROACH TO INTEGRITY - 14

- The integrity research effort has been either very pragmatic, and/or technological, or almost semantic in nature, and in any case there is no reference to the cost benefit framework for Information Integrity – an aspect so crucial to business decisions.

ACCOUNTING/AUDITING RESEARCH - 1

- In accounting/auditing research there seems to have been no corresponding debate concerning the exact meaning of “integrity”.
- Traditionally, researchers working in the area of Electronic Data Processing (EDP) have been looking at integrity issues.
- Specifically, in the early days of computing, numerous studies were carried out on errors in data transcription.

ACCOUNTING/AUDITING RESEARCH - 2

- Many commonly used data validation techniques, along with handwriting and forms design standards, evolved on the basis of these findings.
- Another popular research area has been the formulation of check digit algorithms, supported by verification studies with real numbers. These studies yielded confidence levels for the various algorithms.

ACCOUNTING/AUDITING RESEARCH - 3

- Initial application of this research direction is to be seen in accounting literature that places emphasis on internal systems and audits.
 - Indeed, as early as 1968, Feltham identified accuracy, timeliness and relevance as the three dimensions of data quality and analyzed their relationship with the value-in-excess-of-cost criterion within the context of the data consumer.

ACCOUNTING/AUDITING RESEARCH - 4

- The current literature on data/information quality considerably expands this list of integrity attributes to include requirements of: accuracy, usability, reliability, independence, timeliness, precision, completeness, relevance, sufficiency, understandability, freedom from bias, consistency, trustworthy, brief, etc.

ACCOUNTING/AUDITING RESEARCH - 5

- Coming to auditing research, the auditor assesses control risk, according to Statement of Auditing Standard: SAS 55, as determined by the relevant parts of the entity's (Auditee's) internal control structure.
- With respect to accounting information, relevant part of the internal control structure is thus made up of three parts (categorizations): the control environment, the accounting system, and the control procedures.

ACCOUNTING/AUDITING RESEARCH - 5

- This certainly offers a way of structuring the analysis of different possible control mechanisms. However, there is a problem in that there is no explicit coupling to cost and benefits in the sense items in different categories can be compared. The categorization in three parts is essentially ad-hoc.

ACCOUNTING/AUDITING RESEARCH - 6

- Then there is the COSO report that provides an extended framework, but it is qualitative in nature. It sees internal control, from the management point of view, as consisting of five interlocking factors: monitoring, information and communication, control activities, risk assessment, and control environment. However, the same line of inadequacy that is leveled at SAS 55 above, that is, lack of explicit cost-benefit links between the components of model, applies here.

QUALITY PARADIGM-2

- This is an extensively addressed research area. Traditionally, auditing has been used to check whether the various *IS* quality assurance procedures are being carried out correctly, and whether they are successful.
- Quality paradigm came in to prominence in the wake of globalization, international competition, and changing customer expectations. Specifically, it has its origin in the high-volume mechanical manufacture.

QUALITY PARADIGM-3

- Accordingly, it has two aspects; namely, (a) quality assurance concentrating on the process and attempts to ensure that it is done correctly, and (b) quality control aiming to ensure that the product delivered to customer is correct, where the term ‘product’ represents a system or component or service.
- In practice, however, the quality paradigm operates in the ‘standard’ product mould, emphasizing incremental changes, and sees its operable goal as ‘reduced defects’; thereby emphasizing cost reduction aspect but not the cost-benefit angle.

QUALITY PARADIGM - 4

- This leaves the quality emphasis weighing more on the side of ‘process’-centered issues rather than ‘product’-centered issues.
- Unlike in the case of standardized industrial products, information product is so because it is ‘unique’. As a result, for an information system, although quality assurance is vital, it alone is not sufficient to achieve an adequate level of quality.

COMMUNICATION THEORY-1

- Then there is information system (*IS*) model as in communication theory involving source, channel, and destination (receiver) as its fixed parts and the coder and decoder as the variable parts.
- In Shannon's words, "the fundamental problem of communication is of reproducing at one point (destination) either *exactly* or approximately a message selected at another point (source)".

COMMUNICATION THEORY-2

- The cause of this problem is the ever-present channel noise, which tends to disfigure the message, and the noise reduction technology envisaged is optimization of variable parts so as to improve reliability, increase the data rate, or decrease the cost.

COMMUNICATION THEORY-3

- Indeed this model is so widely used that, as a result of Shannon's work, in less than 50 years information theory has scaled the heights of new mathematical discipline.
- Even then from the point of view of the research query under consideration, it is important to note that this *IS* model does not take a decision process based view of the message through the channel.

COMMUNICATION THEORY- 4

- In fact, although the measurements in information theory are significant to communications engineer, they are not related to decision issues, except by chance.
- Accordingly, then there is no reference to the cost-benefit framework for the degree of “exactness” of message achieved.

EXPECTED UTILITY THEORY-1

- The Savage (Subjective) Expected Utility (SEU) Theory presents a mathematical model based on the concept of information value to analytically study a decision process model in the presence of uncertainty. In view of this, when an *IS* is modeled as a decision process characterized by uncertainty, to study its integrity issues, SEU model emerges as an obvious candidate.

EXPECTED UTILITY THEORY-2

- The elegance of the SEU framework is almost beyond compare in the field of economics. However, to this date there is confusion as to the descriptive validity of SEU maximization.
- The sources of confusion partly, at least, seem to lie in the fact that SEU maximization is descriptively *invalid* – falsified – as a model of how individual decision makers behave.

EXPECTED UTILITY THEORY-3

- Nevertheless it is descriptively *valid*, or at least constitutes the best alternative currently available, as a model of individual decision making when building theories of collective decision making at the market level. This apparent paradox has caused much of confusion.

EXPECTED UTILITY THEORY-4

- Further, it defines the monetary value of perfect information as amount of money which renders the decision maker indifferent between using and not using information; and thus does not consider in its treatment any explicit coupling to cost-benefit analysis for the information value it measures.

SUMMARY OF MAIN LIMITATIONS - 1

- In summary, the *IS* models presently in vogue in integrity research literature do not account for the requirement of continuous origination of information endogenous to the specific decision situation.

SUMMARY OF MAIN LIMITATIONS - 2

- Their main concern is only that information technology accesses, communicates, processes and distributes the already generated information; information technology costs ever decreasing and it costing as much to provide 100 units of information as it did to provide 1 unit a couple of decades ago.

SUMMARY OF MAIN LIMITATIONS - 3

- The information processing for decision-making is, therefore,
 - taken as a *costless* activity;
 - resulting in *IS* models having no explicit reference to cost-benefit of information processed, and,
 - as a result, there being no analytical basis for comparing two situations of information processing with reference to net information use quantum delivered.

SUMMARY OF MAIN LIMITATIONS - 4

- Certainly, these *IS* models are characterized by uncertainty resulting in information errors leading to loss of Information Integrity, which is seen as data integrity problem.
- Accordingly, it is appreciated that it is good to have data integrity, *except* that how much remains the issue.

SUMMARY OF MAIN LIMITATIONS - 5

- This certainly is not amenable to any analytical comparison and selection for competitive advantage; thereby integrity not receiving its deserving attention in terms of resource allocation for systems emphasizing it.
- The reality and its requirements though are different.

SUMMARY OF MAIN LIMITATIONS - 6

- As argued in Lecture # 6 and as will be argued later in the course while discussing the impact of 5“C”s (complexity, change, conversion, communication, and corruption) on *IS* view, for the open system view, the *IS* under consideration comprises individual decision process stages that are characterized by activities of information origination.

SUMMARY OF MAIN LIMITATIONS - 7

- And, with complexity and change demands ever on increase, it is now costing to originate endogenous to situation one unit of information as it did to generate 100 units exogenous to situation a couple of decades ago.
- In other words, information “origination” is a *costly* activity.

SUMMARY OF MAIN LIMITATIONS - 8

- This then calls for cost-benefit analysis framework for information originated and processed, so as to work towards ensuring economic processing of information.
- It is through control of Information Integrity that this economy is ensured; thereby the cost-benefit analysis framework required in fact being that of Information Integrity.

EXERCISES

- (E10.1) Analyze the existing approaches to integrity to show that the main limitation of these approaches is that the *IS* models considered do not address the issue of “economic” processing of information (information economics), which as argued in Lecture # 8 is the central point in integrity emerging as the key issue in the study of *IS* for competitive advantage.

Stated differently show that, given the reality of the requirement of individual decision situation in the presence of uncertainty, the *IS* models considered do not account for the costs of analysis and evaluation of the searched flexible information decision, which in fact is the cost of I^*I .

THANK YOU