The effects of Time on Integrity in Information Systems*

W. List CA FBCS
The Kingswell Partnership
46 Snakes Lane
Woodford Green
Essex IG8 0DF
UK
Telephone/Fax: +44 181 504 6480
Email: 100416.13@compuserve.com

Abstract

One of the definitions of Integrity contained in the Common Criteria {2} is "The property....... that assumptions about the known or expected state of information or resources remain true". This paper seeks to identify the effects that time has on the user assumptions about the expected state of information. Today people are designing world-wide systems accessed by PCs where information can be obtained instantly. Can the user be confused by the information provided by such systems?

The paper concludes that there is a risk of the users being confused. Therefore, there is a requirement for future systems to provide metadata relating to time, and time dependent activities, to enable the user to confirm that the information provided is "fit for purpose".

Keywords

Time, Integrity, Users, Information, "fit for purpose".

* This paper has been presented at the IFIP TC-11 SEC'96 conference in Samos, Greece and is included in the proceedings "Information Systems Security: Facing the Information Society of the 21st Century", edited by Sokratis Katsikas and Dimitris Gritzalis, published by Chapman & Hall, ISBN 0 412 78120 4

Integrity and Internal Control in Information Systems Volume 1
S. Jajodia, W. List, G. McGregor & L. Strous (Eds) © 1997 IFIP. Published by Chapman & Hall

1 INTRODUCTION

Some of the potential problems caused by time in a worldwide system can be illustrated by the following example:

There is a meeting in London, England at 9 a.m. local time. The meeting was called to review the worldwide sales of the organisation's main product line. The director's PA had retrieved the sales information up to close of business the night before. The managers present had retrieved their figures at 8 a.m, London time. These sales figures were different. On investigation it was discovered that the managers figures included a full day's American sales which were not included in the Director's figures and there had been an input fault at the Malaysian hub during the previous day therefore certain Far East sales were input after the director's PA had extracted the information. The fact that the figures were different caused confusion because no one knew which figures were "right".

This paper identifies the potential problems caused by time and sets out certain systems actions which can mitigate the potential ill effects. The paper is divided into the following sections:

- Basic principles;
- The user's perceptions;
- What is time in a computer system?
- What is a day?
- Time dependent processing;
- Input cycles;
- Processing cycles;
- Errors and Recoveries;
- Consistency of processing time.

In the paper Integrity in Information systems {1} it was postulated that Integrity should be defined as "sufficiently right at the time of use for the purpose to which the user wishes to put the output". In that paper the impact of time on the user's perception of Integrity was identified as a material element which would affect the user's decision on "fit for purpose".

In the Preliminary Draft of the Common Criteria for Information Technology Security Evaluation {2} Integrity is defined as "The property that assumptions about the known or expected state of information or resources remain true". Clearly the information user's assumptions about time have a material bearing on his/her perception of an expected state of the information received from the computer.

The assumption in this paper is that a person is accessing data in a worldwide distributed database containing the record of the events within an organisation. The principles in this paper are also applicable to other types of system but the examples will be framed in the context of the assumed system.

2 BASIC PRINCIPLES

All databases are always out of date relative to the real world time simply because it takes a finite time to record an event (process a transaction). Whilst the time taken to update a database may be undetectable by a person, it is finite.
All systems must therefore take account of this absolute time delay when seeking to ensure integrity of output to users.

3 THE USERS' ASSUMPTIONS

The person accessing the data will probably assume that it is "up to date". The precise interpretation of "up to date" will vary from person to person and may also be relative to the purpose for which the data is being extracted. The perception of a specific user at a specific time is undefinable in systems terms.

In design terms therefore there is a choice of how to handle this:

- Ignore it completely and only do the basic time identification for data where it is a specified requirement;
- Provide additional information to the user on how "up to date" the data elements are; and
- Provide additional information to the user identifying data which is not "up to date".

Within the user's perception of "up to date" there is a belief that the all data should be present. Clearly if some portion of the data is absent then it is not "up to date".

4 WHAT IS TIME IN A COMPUTER SYSTEM?

Time is both a date and a time, often recorded in fractions of a second. Computers record time on a clock within the machine. Most clocks are set to UTC (Universal Time Clock) time adjusted for the appropriate time zones. This adjustment is made when the machine is set up in a particular location or is made in presenting time information through a software adjustment. Clocks are changed in most countries twice a year to implement daylight saving. When such changes occur there is a possibility of error in the new settings giving rise to erroneous dating of transactions within the system. In addition systems require to cope with leap years.

Erroneous dating of transactions will cause difficulties in any recovery process or examination of log files.

The system should check the correctness (or at least consistency) of the machine clocks throughout a network. In some networks it may be possible to set clocks on all devices centrally.

If clocks are changed during recovery in order to facilitate the recovery; specific checks require to be made that duplicate transactions are not created and that all real world transactions are correctly dated at the completion of the recovery.

5 WHAT IS A DAY?

The world is divided into 24 time zones. Therefore the activities of a worldwide concern "today" may well include activities in all 24 zones. If a manager required the sales of a specific fast moving product "today" from the worldwide database, the answer would probably be different if the question was asked at 6 p.m. German time to that at 8 p.m UK time. The different answers can lead to confusion in management and possibly simple distrust of the figures thereby inhibiting decisions.

Each business therefore needs to operate to a convention relating to "days" which is well understood by all staff and management and appropriate for the business transactions being processed; for example: what is sensible for a manufacturing company may be inappropriate for a derivative trader with a worldwide book.

The application of any convention may well be arbitrary but if everyone understands it, this does not matter. The position to avoid is a number of conventions applying to different systems in the same organisation.

The convention must specify:

- What is start of day; for example: 00.00 or start of business day - say 08.00
- What is end of day; for example: 24.00 or end of night shift - say 03.00.
- The format for printing dates on reports. As conventions vary throughout the world it is suggested that the use of letters for the month is a convenient solution.
- Rules relating to transfers of value or responsibility between units in the worldwide operation require to be embedded into the application programs. Similar requirements exist where data is required by a number of organisations relating to transfers. For example:

  A shipment of goods from unit A is recorded in unit B's records as "in transit from A to B" at the same time as it is deducted from A's inventory.

  An aircraft manifest is assembled over a period of time. Once the aircraft is loaded the manifest is final. The aircraft itself will travel through time and the manifest will logically travel with it. Many organisations will require access to the details and there is an agreed convention between airlines to deal with this situation.
- All reports from the database should be accompanied by information showing the recipient the time that information was extracted from the database. This should show the local time. Where data is extracted that relates to units in other time zones then the time relative to the other units should also be shown, For example: if a report was extracted at 8 p.m. London time and included figures relating to a unit in New York, then the New York figures would show 3 p.m. Eastern Standard Time.

- Rules to avoid differing management reports because they were extracted at different times from the database. Summaries are the usual cause of confusion to management if they are extracted at different times (for example: sales today, commitments today, etc.). Reports relating to the immediate position do not confuse (for example: is there enough stock in a warehouse to supply a customer). One solution to this problem is to categorise data into three groups: basic data; "official" summaries (management information) and personal data extracts. The "official" summaries are generated at fixed times whereas the personal data extracts can be at any time. If management use the "official" summaries for decisions then this procedure overcomes the problem.

6 TIME DEPENDENT PROCESSING

All events recorded in a system have at least two dates: when they happened and when they were recorded as happening. Certain transactions have additional dates (for example: an invoice will have the date issued by the supplier, the date entered into the system, the accounting period or date to which it refers in the records, and possibly also the date received in the organisation, the date of approval and dates on which corrections were made to the original entry of the invoice).

Where processing or reporting is date dependent (for example sales this week, computation of interest, destruction of old records, etc.) it is necessary to have a convention as to which dates are to be used. Confusion arises where, in response to the same request or process, differing results are obtained because of changes made to the data between the two points in time.

The convention requires to cover:

- The date to be used for processing or reporting. Ideally the date when the event occurred or was first known by the organisation.
- A definite limit on the time difference between the event happening (or being known about) and the recording in the system. This limit may well vary depending on the type of event being recorded and the need for formal reporting regulations to be applied to processing of certain events. If the event is recorded outwith the limit then it falls into the next "period". (see also input and processing cycles below).
- All other dates are reference dates and should not be used to govern reporting or processing, but may well be important elements relating to the event.

An archiving policy is required for each application to create an orderly process of moving "old" data to a separate storage area (or medium). The archiving policy should be available to the users of the data. The organisation must ensure that archive data held for many years can be retrieved in a form that complies to any legal requirements. This requirement may involve retaining programs and equipment in the archive.

In certain systems (for example: news items, competitor intelligence information) it may not be possible to decide centrally what is out of date. In this case date information must be supplied to the user so that the user can decide the appropriateness of the information for the user's purpose.

The systems should check:
- At a minimum to ensure that all dates are plausible - i.e. impossible dates are not allowed into the system.
- Impossible relativities of dates in the complete record of an event should be identified. Note: this test can only be made once the total logical record of the event has been input, which may not all take place at the same time. The test may therefore only be able to report errors for subsequent manual correction.

7 INPUT CYCLES

All input enters a system on a cycle. This may be:
- an immediate input (for example: from a machine on a factory floor, telesales recording of orders or statistics, etc.);
- a daily cycle where all information received in a day is input that day (or perhaps with a time delay of some days - for example: data received in a day will be input 3 days later);
- a longer cycle where input is entered periodically (for example: input of inflation statistics is monthly).

Users of information should be aware of the input cycle relevant to the data that they are using to create the information. The cycles may be widely known in an organisation, but where they are not, an indication of what they are could be maintained as part of the data dictionary or a processing diary.

The potential hazard for users of information is that the expected cycle has not been adhered to for whatever reason. Where it is possible to predict that a data source should supply data on a regular basis it is possible to construct a diary to indicate that data was received as expected, and to highlight missing input. Additional information may be supplied to indicate the completeness of the input (for example: batch totals, transmission session totals, etc.) from a particular source.

Where data is received with no particular pattern it is very difficult to determine that input is missing. Certain applications (for example: inventory systems) include procedures for identifying missing items (for example: sequence checks, goods received for which no invoice has been received after say 1 week etc.). Where such checks exist users of the data should be made aware of them.

8 PROCESSING CYCLES

8.1 Administrative systems

In administrative systems many necessary processes are not performed immediately but on a predetermined cycle (for example computation of interest on a bank account is usually done at end of day, orders to suppliers are transmitted in batches, closing an accounting period, etc.). A diary should exist setting out the cycle, and providing information as to when processes will be performed and when processes were not performed at the expected time. Users of data should have access to this diary to enable them to confirm their assumptions about the processing cycles and the "up-to-dateness" of the data they are using.

Where data is created and stored during a process (for example: an interest charge to an account) it should be dated at the time the processing took place. Where the data element in the database holds the "current" value which is amended during the processing, the data dictionary entry for that element should include a clear indication of the updating cycle (for example: an element 'cumulative interest this month' would include in the data dictionary a notation say - updated at end of day to include today's interest).

If there is a necessity to reperform processing at a later date (consistency of processing time below) then there requires to be a convention established as to whether:

- An adjustment transaction, dated on the processing day, is created, or
- The old date is overwritten with the new date, or
- The old date is overwritten with the old date.

The convention may differ depending on the nature of the generated data. This convention should be available in the data dictionary.

8.2 Document systems

In document processing systems it may be possible for either:

- Multiple versions of documents to exist or
- The ability of a number of people to update the same version of a document.

When processing documents the system should be able to identify the "current" version. Users should check before making amendments that the current version is being used. If many people can amend one document, one person should be made responsible for ensuring that all amendments are correctly applied, and all are included in the final version. For important documents it is highly desirable that they are fully proof read before issue to third parties.

9 ERRORS AND RECOVERIES

In any input system there will be some errors. Where these are detected by the system then a correction cycle is started. From a data user's point of view it is probably easiest to treat these errors as missing items until such time as they are corrected.

Processing fails from time to time, and the fact that a process did not perform correctly should noted in the diary. Where processes are dependent on preceding processes being completed correctly, then the system should be so constructed that the later processes are delayed until the cause of the failure is rectified.

10 CONSISTENCY OF PROCESSING TIME

In order to process data correctly it is necessary to process the event details using the program(s) which were current at the time of the event, including any parameters relevant to those programs. Application systems should provide a means whereby it is possible to prove that this was the case.

When events are input within their normal cycle and the processing cycles are followed there is usually no problem in meeting this requirement. Potential problems occur if:

- There is delay in inputting event details;
- The processing cycle is disrupted for any reason;
- Error correction causes a delay in processing; or
- Retrospective processing is required to be performed following a late change in business requirements or following a prolonged recovery process.

Many systems include a convention covering the delay in processing limited numbers of events. This convention usually causes the event to be processed as if it had occurred during the normal cycle within which it was input. Particular controls are required to monitor both the volume and effect of such transactions so that they do not distort prior information. Application programs should produce reports to management of these transaction for positive approval of correctness of the treatment

Very particular attention is required where volumes of events are delayed or substantial reprocessing occurs to check positively that:

- The events were processed in the correct order;
- Using the programs, including parameters, applicable to the time the events took place; and
- No further difficulties were encountered bringing the total database up to a consistent point in time.

If, for any reason, formal summaries of events or the generation of entries could be compromised by the delay or reprocessing, then all potential users of the information should be notified that reworked data is available and requested to destroy any information based on the old data.

11 SUMMARY

Users have expectations as to the timeliness of data and information. These expectations require to be managed so that they are in broad concurrence with the real world status of the data. The main concepts to achieve this are:

- Effective validation of all dates within the system;
- Enforcement of well understood conventions regarding the dating of transactions;
- Provision of information to users relating to input and processing cycles and any failures to conform to those cycles; and
- Enforcement of time commonality and time consistency between the events being processed, the programs performing the processing and the parameters governing the specific detail of the program's processing.

Failure to manage time effectively can give rise to kaleidoscopic effect on management information where no one is clear which information is right or even "fit for purpose".

12 REFERENCES

List, W. and Melville, W.R. (1994) Integrity in Information Systems, *City University Business School Working Paper*

Preliminary draft of the Common Criteria for Information Technology Security Evaluation Version 0.9

13 BIOGRAPHY

William List CA FBCS

He is a director of The Kingswell Partnership; a consultancy specialising in all aspects of business risk limitation. He served for over 15 years as a computer auditor partner in KPMG in UK. He is an acknowledged international expert in the use of control and security techniques in application systems, including those involving networks, EDI and distributed processing.

He is currently:
Chairman of the British Computer Society (BCS) Security Committee
Visiting Fellow City University Business School
BCS representative on IFIP TC 11 - Information Security Technical Committee
Member of the Institute of Chartered Accountants of Scotland IT Committee
Member of the Electronic Commerce Association accounting special interest group