

Time in the Business World

*Contributed by Steven W. Tepler,
CEO Time Certain LLC*

The Issue of Time in the Business World

Time plays a critical part in the everyday processes and operations of the business world. All financial and other business transactions, communications, and business records are ultimately time based and time dependent. Information is an enterprise's most valuable asset, and that asset is now electronically generated. Without some time reference, however, these records would have little or no worth. In the old days, physical records were recorded, and some time references (i.e., a stamp, or other mark) would be affixed to the physical record (usually paper and ink). If the record or the timestamp were tampered with, or forged after the fact, a wide array of forensic tools could be used to ascertain the genuineness of either the record or the notation of the time it was created. With the onset of electronic data as source records for business and government enterprise, there has arisen a vulnerability unique to electronic data that has not yet been addressed, and that is the issue of time-based data manipulation. Since electronic data is comprised of zeroes and ones, and are not physical in nature, they are uniquely susceptible to manipulation. No auditor, CEO, or technology expert can read binary data and interpret them as a spreadsheet, an email or database table element.

Time Travel used to Manipulate Audit Data

Einstein theorized that time travel was possible, which raised the classic paradox of a person going back in time and killing their grandfather. We cannot travel to our past per se, but it turns out that our audit data can travel back in time. An unscrupulous person can modify, substitute or destroy existing audit data (e.g., reports) and by resetting the system clock to an earlier time, can cover their tracks, completely and without any way to "audit" back to ascertain what is real, and what is not. The following articles show that such unprofessional and illegal activity exists today:

- **Ex-Ernst &Young Partner: New York Times, September 26, 2003**

In the NextCard matter, the SEC invoked Sarbanes-Oxley and charged a former partner of E&Y with criminal destroying and altering audit workpapers related to a federal examination of NextCard. An E&Y audit manager was also charged, and pleaded guilty to fraud. A senior partner at E&Y was also charged with obstruction of justice, as the SEC claimed that he knew of the altered workpapers but took no action. The two E&Y auditors accessed workpapers contained in an archive and revised them. The revised versions were saved, and original workpapers were deleted. To ensure that the computer did not record the revisions as "after the fact" the team reset the internal clock on their computer to make an earlier date appear. NextCard was a 400 million dollar public company flameout and is being liquidated.

The SEC attorney in charge of the investigation lamented that the biggest crime here was that [they] would never know the extent of the fraud, because they would never be able to obtain the original data...

- **Rite-Aid Articles: Wall Street Journal, June 10, 2003; New York Time, October 18, 2003;**

In the RiteAid Case, the general counsel was convicted of conspiracy and conspiracy to obstruct justice. The General Counsel, CEO and CFO were involved with backdating severance letters so that the senior executives could receive huge payouts. The computer used to backdate the letters had its clock altered and then reset, and then was later dumped into the Atlantic Ocean.

- **Sirena Corp.- USAO/CDCA Press Release April 24, 2001; U.S. Securities and Exchange Commission Litigation Release No. 16730 September 27, 2000**

In another SEC action, the CEO and the CFO of publicly traded Sirena Corp were charged by the SEC and later found guilty of securities fraud, conspiracy to commit securities fraud, and circumventing a publicly traded company's internal accounting controls. In order to meet analyst sales expectation for a prior quarter's sales, the CEO and the CFO caused all sales in a subsequent quarter to be reported as sales that occurred during a prior quarter. They accomplished this by turning back the network system clock, so that all April sales were recorded as March sales.

- **Autotote.- New York Times, October 22, 2003**

In 2002, a senior trusted programmer at Autotote, a subsidiary of publicly traded Scientific Games, manipulated a program and data to alter a losing Breeder's Cup ticket into a 3 million dollar winning ticket. He was able to alter the contents of the losing ticket by resetting the network's system clock. He pleaded guilty and is now in prison. What is most interesting about this case is that while the three million dollar winning bet was detected by a statistical sampling program, it appeared that the programmer had been altering losing bets into \$1,000 winners every week for the past few years, and had paid off his house and car loan. These alterations were never detected. Further, Autotote was again the victim of time-based data manipulation in October, when it was revealed that "past-post" betting was still occurring, and that a large part of it had been done by race-track employees.

The Problem

System clocks are essentially untrusted time stamp sources. The bottom line is that if the organization that creates (or manages) the audit data also can alter the system clock, the data (as well as the audit data) is untrustworthy.

If we can assume that information is a company's most vital asset, and that at present most information is generated in digital form as *source data*, then a material weakness in that data generating process may result in a material misrepresentation sufficient to call into question the certification, and place both the certifier as well as the auditor in peril. In the United States, other data-protection oriented laws (Gramm-Leach-Bliley and HIPAA) both require that data integrity be maintained on a continuing basis and be protected from internal as well as external attack.

Computer evidence in truth is not what we read, or what we see on the screen. Those are "views". What is evident is really ordered compilations of binary data, i.e., zeroes and ones. These zeroes and ones are rendered by one or more computing process (which are themselves comprised of zeroes and ones) to become human readable. Read in their native format, one set of binary data is completely unreadable by human perception and therefore it's content, as well as time of creation (the when and the what, rather than the "who") is indistinguishable from any other set of binary data, including fraudulently manipulated or created data. Unless these zeroes and ones can be anchored and authenticated in some reliable way not under the control of human intervention, digital data, and computer output, is highly suspect.

There is vulnerability in current computing environments that may affect both admissibility as well as weight of digital evidence. That vulnerability is the insider control over time in the data generating system. Where insider control over network time exists, the capability for digital data fraud (manipulation, re-creation, substitution or alteration) exists.

Singapore Law

The Evidence Act Sections 35 and 36: Singapore law currently addresses requirements for the admissibility of electronic (or computer generated) evidence. In order to be admissible, such evidence must generally satisfy two requirements as to proof of operation and accuracy:

Requirement One: It must be shown that no reasonable ground for believing output is inaccurate because of improper use, and that no reason exists to doubt or suspect the truth or the reliability of the data. This requirement poses challenges in that the re-setting of time in a computer can be seen as an aspect of proper operation, but may involve improper use. Further, if an insider has engaged in improper time-based data manipulation, it will be impossible to ascertain after the fact what has been altered or tampered. In the United States, the Rite Aid lawsuit brought by the SEC noted that the original data that had been tampered and altered could never be retrieved or "audited".

Requirement Two: Reasonable grounds to believe at all material times that the computer was operating properly. Again, a computer may operate properly, but the time-based manipulation and vulnerability (i.e., resetting the system clock) is a predicate to what is commonly accepted as proper operation.

The Solution: Achieve Content Authentication by TimeCertain Technology

The solution to this relatively new, largely undetectable, but growing problem is independent trusted time sources. Indeed, the issue has been well recognized in the United States by the American National Standards Institute (ANSI) that formulates security standards for the financial services industry and is working on the new American National Standard X9.95 Trusted Time Stamps.

TimeCertain enables businesses and relying parties to trust digital data by proving that the data is unchanged. TimeCertain supplies the mechanisms and technology that let companies trust digital data by preventing time-based digital forgery. Companies will be able to use TimeCertain technology to detect and prevent fraudulent data manipulation in business any transactions, allowing companies to minimize risk, develop transparency and preparedness, enhance confidence and provide digital data auditability. TimeCertain technology also provides key data security compliance components for enterprises subject to laws and regulations such as Sarbanes-Oxley (Public Companies), HIPAA (HealthCare), Gramm-Leach-Bliley (Banking and Finance), and 21 CFR Part 11 (Pharmaceutical Manufacturers)

TimeCertain provides data content integrity authentication and protection services by offering a trusted timestamp capability that is local to the client's data generating facilities. The timestamping appliance, which is offered in a 2u rack mount format, provides the service inside a client security perimeter. It is access independent (no wired or wireline access to the Internet or other remote source outside the client firewall is required) and can provide content authentication for any binary data at throughput of up to 90 timestamps per second.

Trusted timestamping, or data content authentication, enables a company or auditor to claim that electronic source data is what it purports to be and *could* not have been undetectably changed by any party (including the data generator). TimeCertain's service includes a hardware and software component. The hardware component is an appliance server which contains a FIPS validated hardware security module protecting clock, serial number generator and signing keys used for timestamping. The software component consists of a toolkit that contains sample code and a crypto library for producing trusted timestamps utilizing robust commercial grade cryptographic processes. Further, the timesource used by the timestamp server is directly auditable back to a national timing authority (Spring Singapore).

Trusted timestamping removes the risk of undetectable data tampering, manipulation, alteration or deletion by "trusted" insiders, and so removes both the exploit vulnerability (which constitute a material weakness resulting from a lack of sufficient internal controls) as well as the vulnerability to a legal challenge. It also provides an enterprise with the benefit of transparency and immediate fraud detection in the data and data audit trails that it does generate.


Frequently Asked Questions:

How does TimeCertain improve business performance? TimeCertain Trusted Facility™ Timestamping technology may be used to provide immunity from content challenge for any digital data, thereby making data generating events trusted, reliable, and auditable.

How does TimeCertain help organizations manage risk and liabilities? TimeCertain eliminates the possibility that digital data can be undetectably altered or forged after its generation.

How will TimeCertain assist in eliminating internal and external exploits? TimeCertain technology can detect any instance of data manipulation on a real-time basis, in accordance with client requirements.

What is TimeCertain's ability to quickly and cost-effectively deploy expanded services within existing infrastructure? TimeCertain technology is based upon industry standard processes in the generation and verification of timestamps issued. Any infrastructure adhering to these standards can quickly and efficiently deploy our services.

<p>TimeCertain, LLC</p>  <p>TimeCertain, based in Florida, USA is the leading provider in the digital data content authentication marketplace serving businesses worldwide. Utilizing patent pending technology, TimeCertain solutions offer cost effective, high volume digital data time stamping and audit technology that prevents digital data forgery by proving the exact content of digital data at generation.</p> <p>This White Paper is for informational purposes only. This White Paper is published on 24th November 2003.</p>	 <p>Opus IT Services Pte Ltd</p> <p><i>Exclusive Distributor for Time Certain</i></p> <p>Opus IT Services Pte Ltd is a leading provider of IT services and e-Business outsourcing company in Singapore. With deep industry expertise on how to run and manage IT operations, Opus is committed to helping its customers to streamline their IT infrastructure and operations, thus making them more efficient and competitive in their respective marketplace.</p> <p>Opus is able to successfully achieve this by providing the following core services to their clients - End-User Helpdesk Services, Onsite Technical Support, Data Centre Operations, Service Centre, Network Connectivity Operations and Systems Administration.</p> <p>For more information about TimeCertain Trusted Time stamping solution and services, please contact:</p> <p>Mr Kenneth Koh OPUS IT Services Pte Ltd 31 Kaki Bukit Road 3, #06-13 TechLink, Singapore 417818 Tel: +65 6842 7600 Fax: +65 6842 1776 Email: kenneth.koh@opusit.com.sg</p> <p>© 2003 Opus IT Services Pte Ltd. All rights reserved.</p>
---	--