Proving the Integrity of Digital Evidence with Time

Chet Hosmer, President & CEO WetStone Technologies, Inc.

Background

During the latter half of the 20th century, a dramatic move from paper to bits occurred. Our use of digital communication methods such as the world-wide-web and e-mail have dramatically increased the amount of information that is routinely stored in *only a digital form*. On October 1, 2000 the Electronic Signatures in National and Global Commerce Act was enacted, allowing transactions signed electronically to be enforceable in a court of law. (Longley) The dramatic move from paper to bits combined with the ability and necessity to bring digital data to court, however, creates a critical question. How do we prove the integrity of this new form of information known as "digital evidence"?

Digital evidence originates from a multitude of sources including seized computer hard-drives and backup media, real-time e-mail messages, chat-room logs, ISP records, web-pages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards, and digital cameras. The trust worthiness of this digital data is a critical question that digital forensic examiners must consider. Many vendors provide technology solutions to extract this digital data from these devices and networks. Once the extraction of the digital evidence has been accomplished, protecting the digital integrity becomes of paramount concern for investigators, prosecutors and those accused.

The ease with which digital evidence can be altered, destroyed, or manufactured in a convincing way – by even novice computer users – is alarming. To make matters worse, the need to preserve, archive and protect the integrity of digital evidence for long periods of time has arrived, and the methods used today rely on the integrity of individuals, process, procedures, and physical access security. These methods are costly to implement, fraught with potential errors, vulnerable to accidental or malicious modification, and constrain the widespread utilization of digital evidence in crucial litigious procedures.

Fortunately the computer science and information security field has defined what digital integrity is and has contributed a multitude of methods for protecting the integrity of digital data – at least in the general case. Digital integrity can be defined as, "the property whereby digital data has not been altered in an unauthorized manner since the *time* it was created, transmitted, or stored by an authorized source" (Vanstone et.al. 1997). Applying and adapting methods from computer science and information security to the domain of digital evidence is complex and involves technology, and the expertise and understanding of what it means to prove the integrity of digital evidence. The question then actually is what are we actually trying to prove?

In the simplest case let's assume that we have seized a piece of digital evidence in the form of a floppy disk. At a minimum we would like to prove that the contents of the floppy disk (the digital data) have not been altered in any manner from the moment that we seized the disk. We

need to be able to prove this fact many years after the evidence was originally seized, independent of those involved in the original seizure.

Proving the Integrity of Digital Evidence Today

To date, several methods have been adapted from the computer science and information security to the domain of digital evidence. The table below illustrates the method, advantages and disadvantages of each.

Method	Description	Common Types	Advantages	Disadvantages
Checksum	A method of checking for errors in digital data. Typically a 16- or 32-bit polynomial is applied to each byte of digital data that you are trying to protect. The result is a small integer value that is 16 or 32 bits in length and represents the concatenation of the data. This integer value must be saved and secured. At any point in the future the same polynomial can be applied to the data and then compared with the original result. If the results match some level of integrity exists.	CRC 16 CRC 32	⇒ Easy to compute ⇒ Fast ⇒ Small data storage ⇒ Useful for detecting random errors	⇒ Low assurance against malicious attack ⇒ Simple to create new data with matching checksum ⇒ Must maintain secure storage of checksum values ⇒ Does not bind identity with the data ⇒ Does not bind time with the data
One-way hash algorithm (MD2, MD4, MD5, SHA	A method for protecting digital data against unauthorized change. The method produces a fixed length large integer value (ranging from 80 – 240 bits) representing the digital data. The method is said to have one-way ness because it has two unique characteristics. First given the hash value it is difficult to construct new data resulting in the same hash. Second given the original data it is difficult to find other data matching the same hash value. (Schneier)	SHA-1 MD5 MD4 MD2	⇒ Easy to compute ⇒ Can detect both random errors and malicious alterations	⇒ Must maintain secure storage of hash values ⇒ Does not bind identity with the data ⇒ Does not bind time with the data
Digital Signature	A secure method of binding the identity of the signer with digital data integrity methods such as one-way hash values. These methods use a public key crypto-system where the signer uses a secret key to generate a digital signature. Anyone can then validate the signature generated by using the published public key certificate of the signer. The signature produces a large integer number (512 – 4096 bits)	RSA DSA PGP	⇒ Binds identity to the integrity operation ⇒ Prevents unauthorized regeneration of signature unless private key is compromised	⇒ Slow ⇒ Must protect the private key ⇒ Does not bind time with the data ⇒ If keys are compromised or certificate expires digital signature can be invalidated

Adding Time to the Equation

Using the best practices afforded us today – digital signatures – we are able to successfully bind "who" (the signer) with the "what" (the digital data). However, digital signatures have shortcomings that leave two critical questions unanswered:

1. When did the signing of the digital evidence occur? How long after the evidence was seized, was its integrity protected?
2. How long can we prove the integrity of the digital evidence that we signed?

For both of these questions, time becomes a critical factor in proving the integrity of digital evidence. We need to determine how we can bind time, and more importantly, a *trusted* source of time to digital evidence. To understand this we first must understand a little about time itself and what is necessary if we are to trust that it is accurate.

From ancient societies to the present day, time has been a function interpreted in many ways. Time essentially is an agreement that allows society to function in an orderly fashion – where all parties are able to easily understand the representation. Examples of time measurement include:

- Earliest calendars were based on the moon because everyone could easily agree on this as a universal measure of time. The Egyptians were the first to understand the solar year and develop a calendar based on the rotation of the earth around the sun. The calendar we use today uses this solar basis to arrive at the number of days in the year.

- In 1582, Pope Gregory XIII introduced his calendar, which is the calendar used today and referred as the Gregorian Calendar.

- In 1967, an international agreement defined the unit of time as the *second,* measured by the decay of Cesium using precision instruments known as atomic clocks.

- In 1972, the Treaty of the Meter (established in 1875) was expanded to include the current time reference known as Coordinated Universal Time (UTC), which replaced Greenwich Mean Time (GMT). More than forty countries running a collection of over two hundred atomic clocks administer UTC. This is where the time reference originates, enabling government entities to establish their respective "national time."

Establishing the "when" of an event in the emerging digital world necessitates new agreements on how time is used. Time as a quantified value is used in nearly all aspects of commerce and security in order to bind validity, grant access, and reconstruct the order of events. In manual systems, an authorized individual, such as a notary, can attest to the date-time of a transaction based upon some standard practice. Notarization, in particular, can provide three valuable time services: an accurate date from an authoritative source, a certification that the date supplied applies to the transaction in question, and a format that can be verified by disinterested or trusted third parties under a broad range of circumstances.

Secure and Auditable Time

This problem has created an opportunity to establish a new standard of secure and auditable time stamps that are represented electronically. In the course of the past two years many providers and users of digital signature technologies have begun to understand the importance of using the same rigor in authenticating the source of the time as they have with authenticating an individual. This process utilizes the same types of public key infrastructure processes used by Certificate Authorities and combines this with the official world sources of time.

This approach is able to secure the time stamp and simultaneously provide the evidentiary trail of the time source within the time stamp. Once you have created a time stamp that is resistant to manipulation and provides an authenticated audit trail you can electronically "bind" these secured date/time stamps to digital evidence so that they can be verified by a third party.

Ideally then, "secure, auditable digital date/time stamps" will have the following attributes:

- **Accuracy.** The time presented is from an authoritative source and is accurate to the precision required by the transaction, whether day, hour, or millisecond.
- **Authentication**. The source of time is authenticated to a National Measurement Institute (NMI) timing lab so that a third party can verify the precision and accuracy of the time.
- **Integrity**. The time should be secure and not be subject to corruption during normal "handling." If it is corrupted, either inadvertently or deliberately, the corruption should be apparent to a third party.
- **Non-repudiation.** An event or document should be bound to its time so that the association between event or document and the time cannot be later denied.
- **Accountability.** The process of acquiring time, adding authentication and integrity, and binding it to the subject event should be accountable, so that a third party can determine that due process was applied, and that no corruption transpired.

Adding secure and auditable time to digital evidence eliminates the potential for fraud and unintended errors. The use of secure date/time stamps can not only improve the integrity of digital evidence, but also can provide higher assurance required for digital chain of custody. Quite simply, using secure and auditable time ensures that any important electronic event has a time stamp that cannot be corrupted and has an evidentiary trail of authenticity.

Proving the Integrity of Digital Evidence with Time

In order to effectively use digital evidence to prove the motive, opportunity and means of cyber-criminals we must:

- Significantly advance the accuracy and trust of digital time.
- Digitally bind this trusted electronic time with digital data and computer events on a routine basis.
- Make the process routine, ubiquitous and standardized throughout the digital world.
- Make this trusted electronic time traceable to a legal time source(s).

The steps are:

Step 1: Traceability to Legal Time Sources

Since 1972 over 40 countries throughout the world have adopted Coordinated Universal Time or UTC as their official time source. This agreement between nations has resulted in a stable source of time that we can all agree upon. In order for the time of digital evidence to be considered *trusted* we must be able to trace any digital timestamp back to at least one of the UTC time sources in the world.

Step 2: Time Distribution

The secure distribution and traceability of time from these UTC sources is certainly a significant undertaking but a necessary one if we are to effectively bind meaningful time with digital events. The solution we arrive at must provide continuous audit and provable traceability to UTC sources. This solution must be resistant to attack, malicious or accidental altering of critical time sources and denial of service.

Step 3: Secure Digital Timestamping

The secure issuance of timestamps for digital evidence has at least these critical components.

1. First the binding of time with digital data must occur itself within a trusted computing environment in order to assure the efficacy of the time stamping process.
2. The accuracy of the clock used as the source for time stamping should be appropriate for the application. For example, the accuracy of a timestamp denoting access to a secure facility through the use of a card access or biometric device of 30 seconds may be reasonable. However, the time stamping of an electronic stock transaction or money transfer may require a finer resolution.
3. The calibration and audit of the local trusted clock used as the source for time stamping must be routine, continuous and traceable. Furthermore, a trusted, disinterested 3rd party must be relied on to accomplish this calibration and audit of such clocks.
4. The validation of the resulting timestamps must be verifiable by issuer and by any party that has the need to evaluate the accuracy, validity, trust-worthiness or traceability of a timestamp.

Summary

Proving the integrity of digital evidence with time offers significant advantages over existing best practice methods. We can now bind for the first time the "who" (the identity of the signer), the "when" (the time the signing took place) and the "what" (the digital data we are trying to protect). This new digital integrity mark will allow us to prove the integrity of digital evidence today and in the future. We hope that this new level of protection for digital evidence will advance the collection, preservation, and use of digital evidence.

References

Hosmer, C., (2001). The Importance of Binding Time to Digital Evidence. Paper presented at the 12th Annual Economic Crime Investigation Institute Conference, McLean, VA.

Hosmer, C., (1998). Time-Lining Computer Evidence. Paper presented at the IEEE Information Technology Conference.

Hosmer, C., Feldman, J., & Giordano, J., (1998). Advancing Crime Scene Computer Forensics Techniques. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.

Hosmer, C., (1998). Using SmartCards and Digital Signatures to Preserve Electronic Evidence. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.

Longley, R. (2001). E-Sign – Be Careful What You Ask For. U.S. Gov Information Resource [On-Line]. Available: http://usgovinfo.about.com/library/weekly/aa072300a.htm.

Schneier, B. (1996.) Applied Cryptography (2nd ed.), John Wiley & Sons.

Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.

WetStone Technologies, Inc. (2001) Sovereign Time™ Providing the "When" for the Electronic World. unpublished manuscript.

© 2002 International Journal of Digital Evidence

About the Author

Chet Hosmer (chet@wetstonetech.com) is a co-founder, President and CEO of WetStone Technologies, Inc. He has over 25 years of experience in developing high technology software and hardware products, and during the last 11 years, Chet has focused exclusively on information security technologies. This focus has resulted in technology innovations in secure time

stamping, steganography, network and host based intrusion detection systems, digital watermarking and digital forensics.

Chet is a co-chair of the Technology Working Group, one of the seven working groups of National Cybercrime and Terrorism Partnership Initiative sponsored by the National Institute of Justice. He is also the Research Advisor of the Computer Forensics Research and Development Center (CFRDC) of Utica College and serves on the Board of Directors for the Economic Crime Investigation Institute. Chet is a member of IEEE and the ACM, and holds a B.S. degree in Computer Science from Syracuse University.