

The Digital Signature Paradox

Jeff Stapleton, Paul Doyle, Steven Tepler Esquire

Abstract – Paradox is a term often associated with Hollywood’s fanciful time travel; however in the real world a time paradox does in fact exist. The system clock is the immediate source of time for any computer, and is the sole source for a time stamp determining when a document was created, modified and printed; or more interestingly when a digital signature was generated. Fraud has already been perpetrated by turning back system clocks leading to the falsification of information for which individuals have been disbarred or incarcerated. The application of a digital signature would not have resolved these issues; which is why digital signatures are time-insensitive. However, an independent clock source providing a trusted time stamp would and can circumvent individuals taking such illegal liberties. This paper presents the concept that data integrity needs to be redefined within the context of a time-sensitive mechanism.

I. INTRODUCTION

A. Digital Signatures and Time Stamping

Asymmetric (public key) cryptography provides digital signatures, whereby a hashing function is applied to data strings to produce a hash value; and the asymmetric private is applied to the hash value to generate the digital signature. The digital signature can be verified by a relying party using the corresponding asymmetric public key. In a classical public key infrastructure the identity of the signer is cryptographically bound to its public key via an X.509 public key certificate issued by a certification authority.

Most networks provide a system time such that data can be time stamped with the year, month, day, hour, minute, and second. Presumably the time stamp indicates a sequence to the relying party and implies when the digital signatures were generated. However, note that the system generated time stamp is not independent of the digital signature generation processes, which induces a paradox.

II. PARADOX

A. Digital Signature Paradox

Consider the scenario whereby the system clock has been reset such that the same time stamp is generated at different times for different versions of the same data. The time paradox is that a relying party now has versions of the same data with the same time stamp; and despite the presence of a legitimate digital signature the relying party has no practical method to distinguish between the versions, has no method to prioritize the versions and has no option but to distrust all versions. In order for the relying party to

distinguish between the versions and continue to trust the digital signatures, the signer needs to implement a verifiable mechanism such that the time stamp generation is independent of the signature generation. This method is referred to as a trusted time stamp.

B. Trusted Time Stamp

In a trusted time stamp scheme, there are five entities: time source entity, time stamp authority, requestor, verifier, and relying party. The relying party can be the requestor or any other third party. The time stamp authority (TSA) calibrates its clock with an upstream time source entity such as Master Clock (MC) or directly with a national measurement institute. The TSA provides a trusted time stamp token to the requestor. The time stamp token can be verified by a third party verifier. Figure 1 - Trusted Time Stamp shows the relationship between the time source entities, the TSA, and the requestor.

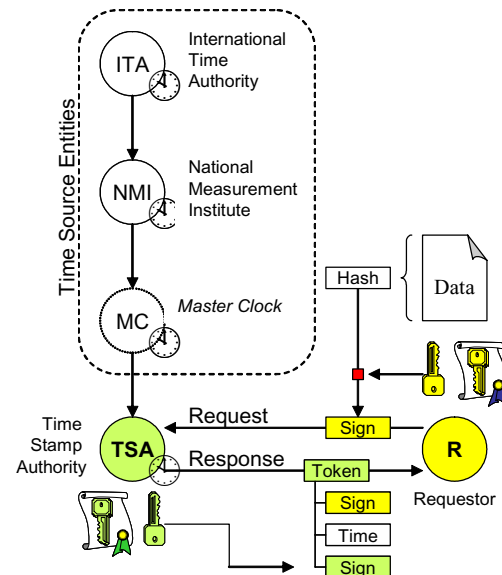


Figure 1 - Trusted Time Stamp

The requestor generates a digital signature by hashing known data and applying its asymmetric private key to the hash. The digital signature is presented to the TSA as a request for a time stamp token. Note that the TSA only knows the digital signature, not the original source data, and therefore has no liability as to the data content. The TSA appends a time stamp to the requestor’s signature and cryptographically binds them, such as another digital signature. The requestor signature, the time stamp and the TSA signature are the essential elements of the time stamp token returned to the requestor. The requestor can then

provide the original data and the time stamp token to a relying party for verification.

The definition of data integrity “a property whereby data has not been altered or destroyed” must therefore be expanded to embrace time-sensitive mechanisms such as trusted time stamps. An alternate definition is then “the continuity of data at a provable point in time.” With this definition a relying party can verify that data integrity is currently contiguous from a previous point in time.

C. X9.95 Standard

The American National Standard X9.95-2005 Trusted Time Stamps was developed based on RFC 3161 and ISO/IEC 18014, but goes much further in its analysis and offerings. X9.95 defines time stamp schemes that provide a high assurance level of data integrity and non-repudiation not achievable by digital signatures alone; suitable for regulatory compliance. The standard (i) defines roles, responsibilities and requirements for the time source entity, the time stamp authority, the requestor, and the verifier; (ii) specifies data objects; message protocol; and trusted time stamp methods; and (iii) provides sample time stamp policy and practice statements along with evaluation compliance criteria suitable for use by a professional practitioner.

III. CASE HISTORY

A. Enron (CFO)

Mr. Fastow, the Chief Financial Officer and other members of the Enron executive team made it a habit engage in time-based data manipulation, i.e., to alter or change financial data to suit whatever it was they wanted the investing public, or governmental authorities to know, or not know. Mr. Fastow has pleaded guilty and is now a guest of the federal government.

Nancy Temple was the Andersen attorney assigned to the Enron matter. When asked by a Congressional committee whether any data had ever been altered or changed after the fact, she responded that no final reports was ever altered or changed. The clarity of her response (and the admission by implication that everything prior to those final papers were altered by time-based data manipulation) earned her a disbarment from the practice of law.

B. Rite-Aid (CEO, CFO)

The CEO and the CFO of this publicly traded company backdated compensation grant letters to enrich themselves by millions of dollars. They then attempted to remove any evidence of their wrongdoing by dumping the computer they used to backdate the documents into the Atlantic Ocean. These gentlemen are now guests of the federal government.

C. Next-Card (Auditors)

NextCard was the largest issuer of Internet MasterCard and Visa credit cards. Executives fraudulently and illegally re-

characterized loan losses, thereby reducing the amount of cash reserves required. Assisting in this billion dollar flameout, auditors from Ernst & Young perpetuated the fraud by backdating their work papers and final reports. These auditors are also currently guests of the federal government. The SEC attorney investigating this matter stated that there was no way to ascertain or recover the real information because of the time-based data manipulation of these insiders.

D. Autotote (Programmers)

A senior trusted programmer for the largest electronic wagering organization in the United States back-dated data to create a 6 million dollar winning ticket in the Maryland Breeder’s Cup race. This gentleman is now a guest of the state.

E. Sirena Corp (CEO)

The Securities and Exchange Commission fined publicly traded Sirena Corp. for holding the quarter open for days after the end of that quarter in order to squeeze additional revenues to meet analysts projections. Sirena eventually declared bankruptcy.

F. Parmalat (CEO, CFO, and Family)

In this 18 billion dollar 2003 bankruptcy, the entire CxO level of this mutli-national conglomerate engaged in time-based data manipulation by creating a false letter of credit from Bank of America asserting that an offshore bank account holding 5 billion euro on account. There are currently at least three lawsuits, including two class actions, pending in various courts around the world.

H. Adelfia Communications (executives)

Adelfia’s top executives manipulated time-based data to hide the embezzlement of over 400 million dollars. The company subsequently entered bankruptcy, two of its top executive were convicted and the company is now being acquired by one of its competitors.