IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 60-63
www.iosrjournals.org

A Comparison of Digital and Handwritten Signatures

REBECCA

Abstract
This comparison helps to understand the outline of Digital and traditional Handwritten signatures. Handwritten signature implies the prearranged name or lawful characteristic of an individual manually written by that individual and executed or took on with the current goal to verify a writing in a super durable structure. Whereas the digital signature depends in the insurance managed the cost of private signature key by the signee and the techniques executed by a Certificate authority.
Forgery of the handwritten signatures has been polished for quite a long time, though falsification of digital signatures, without compromise of the private signature key, or seizing of the signature instrument, is basically inconceivable.
Finally, the paper will suggest that although digital signatures will likely revolutionize electronic commerce, handwritten signatures will almost certainly continue to be used for some purposes into the foreseeable future.

I. INTRODUCTION

During our lives, we sign our name multiple times - on cheques, applications for loans, marriage licenses - the list is endless. People in positions of authority can certify the existence of a person with a signature on a birth certificate or end a life with a signature on a death warrant. Signatures have been applied in much the same way since ancient times - by scribing one's own name. Within the past few years, cryptography has made a new way to affix signatures practical. The legal and business communities are rushing to adopt these new cryptographic signature techniques to replace handwritten signatures - but how analogous are handwritten and digital signatures? This paper will explore the similarities and differences between traditional and cryptographic signatures from a technical, legal, and practical perspective. In the end, this paper will suggest the signature method which will be continued.

A BRIEF HISTORY OF AUTHENTICATION

It is probably not surprising that the inventors of writing, the Sumerians, were also the inventors of an authentication mechanism. The Sumerians used intricate seals, applied into their clay cuneiform tablets using rollers, to authenticate their writings. Seals continued to be used as the primary authentication mechanism until recent times.

Use of signatures is recorded in the Talmud (fourth century), complete with security procedures to prevent the alteration of documents after they are signed. The Talmud even describes use of a form of "signature card" by witnesses to deeds. The practice of authenticating documents by affixing handwritten signatures began to be used within the Roman Empire in the year AD 439, during the rule of Valentinian III. The practice of affixing signatures to documents spread rapidly from this initial usage, and the form of signatures (a hand-written representation of one's own name) remained essentially unchanged for over 1,400 years. It is from this Roman usage of signatures that the practice obtained its significance in Western legal tradition.

Use of networked computers to conduct electronic commerce began in the 1960s, starting with proprietary systems to move data within individual corporations, and later within industry groups, such as the railroad and food industries. During the early days of Electronic Data Interchange (EDI), there was no way to apply cryptographically based signatures to electronic documents, so the industries relied heavily upon "trading partner agreements." These paper agreements, signed by the parties involved, described the rules to which the EDI trading partners agreed with respect to honoring purchase order requests, dispute resolution, and so on. Trading Partner Agreements have been remarkably successful, with legal disputes regarding EDI transactions being exceptionally rare.

The means to provide digital signatures for computer communications that are roughly equivalent to handwritten signatures on paper documents became available with the advent of public key technology.

SIGNATURES AND SECURITY SERVICES

Whether signatures are handwritten or digital, they are applied to achieve three security services:

- **Authentication** - which is concerned with assurance of identity. When a salesclerk compares the signature on the back of a credit card with the signature on a sales slip, the clerk is using the handwritten

signatures as an authentication mechanism, to verify the person presenting the credit card is the person the card was sent to by the issuing bank.

- **data integrity** - assurance that data has not been modified since the signature was applied. While a handwritten signature does not in itself provide data integrity services, the security practices traditionally surrounding handwritten signatures, including the use of indelible ink and tamper-evident paper, provide some measure of data integrity. Digital signatures provide excellent data integrity services by virtue of the digital signature value being a function of the message digest; even the slightest modification of digitally signed messages will always result in signature verification failure.
- **non-repudiation**, which is concerned with providing evidence to a third-party (like a judge, or jury, for example) that a party participated in a transaction, and thereby protect other parties in the transaction against false denials of participation. The buyer's signature on the credit card sales slip provides evidence of the buyer's participation in the transaction and protects the store and the card-issuing bank from false denials of participation in the transaction by the buyer.

CAPABILITY OF SIGNATURES

No security mechanism, whether manual or automated, provides absolute assurance. There is evidence that forgery was practiced shortly after the invention of writing, and that it has remained a problem ever since. In the year 539 AD (100 years after the Romans started using signatures) the Romans generated legislation (in the code of Justinian) that established requirements that forensic document examination experts be sworn, and specifying under what circumstances their testimony may be given in cases of forgery.

Modern forensic document examiners commonly compare a suspect signature with several examples of known valid signatures, and look for signs of forgery, which include:

• Signatures written at a speed which is significantly slower than the genuine signatures.
• Frequent change of the grasp of the writing implement.
• Blunt line endings and beginnings.
• Poor line quality with wavering and tremor of the line.
• Retracing and patching.
• Stops in places where the writing should be free.

These techniques are supplemented with ink and paper analysis, electrostatic detection of writing imprints, and so on.

It is difficult to quantify the strength of handwritten signatures. It seems that the level of assurance that one can place in a handwritten signature depends largely on the technical expertise of the forensic document examiner used to investigate the signature. Certainly, expert forgers have succeeded in some cases, but handwritten signatures continue to be used, because they generally provide a strength of security services sufficient for the purposes to which they are applied. The basis of the assurance provided by a digital signature is fundamentally different than that of a handwritten signature. Whereas the judgement of whether a handwritten signature is valid or not depends on the skill of the examiner (be it the clerk comparing the credit card against the sales slip, or the forensic document expert), the judgement of whether a digital signature is valid depends on a great many processes and procedures working correctly.

Another difference between handwritten and digital signatures concerns the mechanism of association between the signer and her signature. A handwritten signature is biologically linked to a specific individual, but cryptographic authentication systems bind signatures to individuals through technical and procedural mechanisms. There are strong, mathematical links between a private signature key, its associated public key, and the message signature, but the association between the signer and her private key depends on the protection afforded the private key.

The association between the signer and her public key depends on the honesty and diligence of the Certification Authority (CA) issuing the signer's public key certificate (a public key certificate is a digitally signed statement by a CA that binds a public key to a signer's identity). Hence, the strength of the security services provided by a digital signature is a function of the methods used to safeguard the private signature key, methods used by the CA to identify and authenticate those applying for digital certificates, the protections provided against corrupt CAs, safeguards against the computers used by the CA being subverted, and so on.

DIGITAL SIGNATURES - WILL THEY LAST?

When considering digital data archival, it is important to remember digital signature verification requires each bit in the signed document be preserved and read correctly, just as it was when the signer applied the signature. For example, the flipping of a bit that changes an "s" character to an "S," while undesirable in any electronic document, would render a digitally signed document completely unverifiable, just as if every word in the document had been changed.

There are at least four problems associated with the long-term archival of signed electronic records. Briefly, they are:

• Deterioration of the source media
• Obsolescence of the record data format
• Evolution of cryptographic algorithms and related standards; and,
• Certificate life cycle.

Source media (tapes, optical disks, floppy disks, etc.) are subject to deterioration over time. Magnetic media are prone to hydrolysis of the binder in which the magnetic particles are embedded. Hydrolysis causes the binder to become soft and sticky, and transfer from the media substrate to read/write heads and other surfaces. Another problem with magnetic media is the magnetic domains within the media "topcoat" can reverse, thus changing recorded 1's to 0's and vice versa.

The "weak link" in terms of optical disk archival is the metal reflecting layer, used to reflect the optical disk reader's laser. This reflecting layer is typically made of aluminum, and subject to oxidation, because the reflecting surface is enclosed in materials that can be oxygen permeable. As with magnetic tape, quality of the media and storage conditions play the dominant role in determining the useful archive lifetime, but manufacturers estimate, and independent studies indicate that read-only optical disks should last for 100 years under ideal conditions. Lifetimes for writable optical disks are usually less - between 10 - 50 years (Dual alloy disks being an exception, with an estimated life of 100 years.)

A more intractable problem is associated with changing standards for representation of the data on the media. Very few documents written with the Disk Operating System (DOS) based word processors available ten years ago are readable with the word processing applications available today. Some historically important data has already been irretrievably lost to data processing system obsolescence. For example, the data collected from the first Landsat satellite, launched in 1972, can no longer be read.

Digital signatures exacerbate the problem of technological obsolescence. They make the most common coping technique - conversion to new formats during transition periods - impossible unless the original signer can resign under the new format - a solution which is always burdensome and often impossible. From a digital signature perspective, a change to a document format is indistinguishable from a change to the document content and will result in an unverifiable signature.

To address the problem of long-term archival of digitally signed documents, the Federal Public Key Infrastructure Technical Working Group has broken the life of a digitally signed document into three phases. During the first phase, the certificate is still valid, and revocation data should be available through "normal" channels - directories, on-line verification, and so on.

The second phase begins upon expiration of the certificate. For some time after the certificate expires, a public key infrastructure should be able to support non-repudiation dispute resolution by providing evidence concerning the history and status of the certificates it issued. In other words, a Certification Authority should be able to state that a particular certificate was valid at a particular point in time or be able to say when and why a certificate was revoked.

SIGNATURES AND THE LAW

As was mentioned earlier, the legal standing of handwritten signatures for business contracts is based on the Statute of Frauds, which states that for certain kinds of contracts to be enforceable, "some note or memorandum in writing," "signed by the parties" must exist.

The Uniform Commercial Code states that:

" 'Signed' includes any symbol executed or adopted with present intention to authenticate a writing."

By this definition, a record is "signed" if such a symbol is included with the record, regardless of the degree of security associated with that symbol. For example, the initials some people place at the end of an e-mail could be considered a "signature," even though forgery of such a "signature" is trivially easy.

The question, then, is not whether digital signatures have legal standing, since they can be used to commit to a contract under the UCC and can be used to put people in prison if abused - but whether digital signatures provide an equivalent level of evidence of fraud (or the lack of fraud) as do handwritten signatures. There are differing opinions on this matter. The Food and Drug Administration commissioned a study, completed in 1992, to examine the use of electronic authentication, and found digital signatures to be proscribed by regulation for certain applications because of the perception that they provide a lower level of assurance than handwritten signatures. [29] The Federal Public Key Infrastructure Legal and Policy Working Group, composed primarily of Federal Government lawyers, has expressed a somewhat contrary opinion that is more in line with that of the American Bar Association - that use digital signatures should be adopted widely within the Federal Government. It seems likely that use of digital signatures within the Federal bureaucracy will start with low-assurance applications where the risk of fraud is minimal, and increase in scope over time as practical and legal experience with the technology is acquired.

II. CONCLUSIONS

Handwritten and digital signatures share some similarities:
• Both provide the security services of authentication, data integrity, and non-repudiation.
• Both handwritten and digital signatures have legal standing, and the legal standing of digital signatures is increasing with the passage of various state and national laws to become the equal (or more) of handwritten signatures.

Handwritten signatures are extremely simple, and easy to understand. The forensics techniques used to detect fraud are easily explained to lawyers, judges, and juries. Digital signatures are fiendishly complex, involving arcane number theory, the workings of computer operating systems, communications protocols, certificate chain processing, certificate policies, and so on. There are very few people on this planet (if any) who completely understand every process involved in generating and verifying a digital signature. The potential for confused lawyers, judges and juries is extreme.

Digital signatures have the potential to have the greatest impact on commerce since the invention of money. Digital signatures allow us to identify ourselves and make commitments in cyberspace in much the same way as we do in actual space. Nonetheless, digital signature has important limitations, the most significant being their temporary nature. The differences between handwritten and digital signatures will likely have some practical consequences:
• The use of digital signatures for high-value financial transactions outside the protection of trading partner agreements is likely to proceed relatively slowly, until experience with the risks associated with use of digital signatures is accrued.
It seems unlikely that digital signatures will fully replace handwritten signatures in the foreseeable future. Handwritten signatures have a lot going for them - they are fast, cheap, easily understood, and last forever. Digital signatures will probably never be used for treaty authentication, signing bills into law, or other ceremonial or historical occasions.
When handwritten signatures were invented, they augmented seals, which had been in use for over 3,000 years - they did not replace them. In fact, seals continue to be used today. Instead, handwritten signatures took their place beside seals as an authentication mechanism useful for purposes, and over time, handwritten signatures gradually increased in the frequency and scope of their usage. It is likely to be much the same with digital signatures, which are the latest authentication tool in the continuing advancement of communications technology.

LITERATURE CITED

[1]. https://www.hindawi.com/journals/sp/2022/8170424/
[2]. https://www.researchgate.net/publication/220919900_Graphical_and_Digital_signature_Combination_for_fulfilling_the_cultural_gap_between_traditional_signature_and_current_smart_card_digital_certificatesignature/links/5472da8d0cf24bc8ea19a344/Graphical-and-Digital-signature-Combination-for-fulfilling-the-cultural-gap-between-traditional-signature-and-current-smart-card-digital-certificate-signature.pdf
[3]. https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html#:~:text=Differences%20between%20digital%20and%20handwritten%20signatures%20include%3A&text=A%20handwritten%20signature%20is%20biologically,implemented%20by%20a%20Certification%20Authority.