Digital Data Transmission – Security & Safeguards

by
Knud E. Hermansen[†] & Carlton Brown[††]

There are few surveying and engineering firms that have not had to transmit or been asked to transfer surveying and engineering data in electronic format. The requests for electronic surveying documents rather than paper documents are expected to grow.

Many procedures employed by a firm to insure data accuracy and integrity using paper documents are now outdated in the digital age. In this age of data transmission, illicit data swapping, data alteration, and even entire counterfeit digital documents can be produced without easy detection. Image-editing tools can make pixel by pixel changes that alter the font, color, intensity, size, shape, and placement information without visual recognition. Accordingly, new procedures must be considered and employed.

Any procedure for the transmittal of digital data should address four aspects: 1) authentication, 2) data integrity, and 3) end-to-end accountability, and 2) fraud prevention or detection of fraud.

Authentication addresses whether the document is genuine. Previously, the use of a watermark on paper, seal, signature, etc. was used to authenticate the document issued by the surveyor or engineer (though not necessarily the contents of the document). Thus a plan that contained a seal and signature of the professional issued in the stream of commerce could be relied upon. The presence of the seal and signature provided authentication to the reliant party that the source of the plan was a professional.

While a seal and signature can be used to authenticate a document's source, the seal and signature does not address data integrity. Data integrity deals with the validity of the data within the document. For example, were the format, color, lines or words within the document added or altered after leaving the creator's possession but before being used by a reliant party (e.g., public). In the past, the difficulty of alteration without removing or defacing the signature and seal made authenticity and data integrity almost synonymous. This is not true anymore.

End-to-end accountability addresses the ability of both the sender and user to guard against unauthorized modifications or additions to the digital data. In the past, end-to-end accountability was assuaged by use of the United States Postal Service. While there are numerous examples of postal service misfeasance, the number of problems were so low as to give both the sender and receiver considerable comfort. Now, data is sent through numerous routers and third parties. Data corruption occurs along with viruses, worms, and trojan horses that can attach to the file and infect computers and systems. Fortunately, this problem is being addressed by inexpensive anti-virus software, firewalls, etc.

Finally, fraud detection or prevention deals with both making it difficult to perpetuate fraud on the one hand, and easing its detection if fraud is present on the other hand. In the past, the high cost of printing or skill of the forger made undetectable fraud unlikely. Now, the availability of inexpensive software that does pixel by pixel changes has made undetectable fraud likely.

Accordingly, a procedure for the transmittal of digital data should address three concerns (assuming the professional and user have anti-virus software and firewalls): 1) assurance of the unaltered substance of the document; 2) the authenticity of the sender; and 3) the inability or impracticability of falsifying or altering the contents without detection.

There are several procedures and techniques that are available to the surveyor and engineer to deal with one or more of these concerns.

Imbedded Information – Historically a watermark, seal, or signature was used to authenticate a document. Only the sender had the paper, seal, or unique signature. (For a watermark detection, a reader would hold the paper up to a light source to view the watermark in order to authenticate the document.)

Rather than imbed a logo in the paper fabric, digital imbedding places security identifiers in the data that are unique to the sender and vary with the digital document (i.e., digital watermarking). Digital watermarking injects information within the transferred document that is read by security software. The digital watermarking often consists of imperceptible or unnoticeable vectors within the digital elements found throughout the document or sometimes concentrated within a decorative

motif. In other words, it may be in the form of pseudo-random digital noise in the data or part of a decorative element. In any event the code, wherever found can only be detected and decoded by special software. The content of the motif or the aggregate of the imperceptible changes can only be detected and read by the receiver's software. The software will verify the authenticity of the document and identity of the sender, thereby making alterations detectible to the user. Even if a forger is aware that imbedded information exists, there is little likelihood the forger can identify the code or how to vary the code to match the changes that have been made by illicit actions. Using a simplified example, an imbedded digital code attached within this article may contain the word or letter count for the entire document. If the end user's count of the words or letters in the document they have received does not match the word or letter count within the imbedded code, the user can presume alterations have been made.

Imbedded digital codes have the advantage of allowing the receiver to authenticate the document, provide a forensic analysis if the document has been altered, and determine the identity of the issuer by the contents within the imbedded information. The disadvantage of imbedded information is that the sender and receiver must have the appropriate hardware and software to make and interpret the imbedded information. For additional information about imbedded digital information, the reader can view websites of some of the companies that use this technology: www.digimarc.com, http://www.enseal.co.uk, http://www.mediasec.com,

Digital Signatures – Digital signatures are a form of cryptography (transforming messages into seemingly random forms of data and back to the original form again). Digital signatures have two different keys: 1) private and 2) public. The private key is generated by software in the possession of the sender. The public key is used in software in the possession of the receiver that interprets the encrypted message. The private key turns the data into seemingly unintelligible form during transmission, while the public key turns the unintelligible form back into readable form. The public key can be sent to the end user or published on an on-line repository usually maintained by a trustworthy third party. A simplistic example would be for the sender's private key to be a series of numbers or code that generate the number 13. The public key would be

the number 13. If the sender's document did not generate the number 13, it could not have been sent by the proper party.

Fixed Format – Probably the most common manner of secure digital transmission is done by fixing the form of the data into a proprietary format. Adobe Acrobat is probably the most widely recognized proprietary format for transmission of digital data. In the case of Adobe Acrobat, fixing the format of the data requires the purchase of proprietary software. On the other hand, reading the proprietary format is done by a free reader available to anyone for downloading.

Summary – Surveyors and engineers that are sending digital information should consider adopting some of the software safeguards outlined in this article. Commercial software is available that not only fixes the format but provides digital signatures and other security measures that can be employed in digital document transfer.

† Knud E. Hermansen is a professional land surveyor, professional engineer, and attorney at law. He is a professor in the College of Engineering at the University of Maine.

†† Carlton Brown is a professional land surveyor and professional engineer. He is an assistant professor in the College of Engineering at the University of Maine.