Report on forms of non-repudiation are important to information assurance

Law, Evidence

Non-repudiation applied in digital security has cryptological implications. It is basically a service seeking to prove the originality and integrity of data. With a high assurance of data, it can be asserted that the said data is genuine. Asymmetric cryptography allows for proof of the said data without the verification or the consent of the original author. This report explains why the forms of non repudiation are important to information assurance. It also identifies and describes the trust or security domain boundaries that may apply to a personal computer in a business environment.

There are two forms of non repudiation: non repudiation with proof of delivery and non repudiation with proof of origin. The latter provides the information recent with the proof or assurance of the sender's identity; meaning that the sender does not have to verify the information sent since the non repudiation services will identify the origin of the data. The other form of non repudiation, the sender is provided with proof or assurance of message delivery. The sender will be able to know that the recipient has received and recognized receipt of the message. This form of non repudiation also entails recognition of the message content by the recipient.

Cryptography provides secrecy, non repudiation, integrity, and authentication. All these four provide secure code, data, and access. In a business environment, people generally like privacy and confidentiality however the activities of attackers can put sensitive information belonging to an individual or an organization at great risk. If a business establishment comes up with a new product or business strategy, this information may be stored in a computer. The business will therefore have to ensure that the computer is protected and secure from the activities of attackers. The

channels for data communication and networks are usually insecure and any information transmitted through these channels is subjected to threats. The attacker can either intercept the transmission process to view the information or intercepting the process to modify the information. With cryptographic services such as non repudiation, the information can be protected from any form of security threat.

Non reputation in the business environment

In the electronic business environment, non repudiation shifts the burden of proof from the recipient of a message to the sender or the signatory. At the same time it can deny the signatory the right to repudiate a signature in digital form. This means that once a digital signature has been verified the burden of proof rests upon the signatory or the owner of the signature to prove that the digital signature is not his or hers.

The most common way of ensuring that information is from a particular author is through the use of digital certificates. All digital signatures belong to some form of public key infrastructures which are referred to as the digital certificates. These certificates can serve the function of encrypting information sensitive to an individual or an organization, for instance signatures. The signatory or the digital origin of a signed data is the individual possessing the private that corresponds to the public key within the digital certificate. This means that if a signatory fails to properly safeguard his or her private key, chances are high for attackers to engage in activities such as digital forgery.

Applying the security domains in the business environment is aimed at

preventing any unauthorized activity. A trusted system of computing can easily be trusted to ensure security of information sent through the network channels and channels for data communication. TTP is one of the security domains that can be used to protect digital signatures in a business environment. TTP stands for trusted third parties. The trustworthiness of a signature can be questioned based on the way in which a party may try to repudiate a signature. Therefore, a standard way in which these risks can be prevented is through engaging a trusted third party. TTP establishes digital certificates repository that embodies keys used in digital signatures. For instance, the digital certificates work by ensuring there is a correspondence of private keys to public keys within the certificates.

Notaries and forensic analysts are the most common trusted third parties that can be used for secure computing within a business environment. A forensic analyst can easily detect forged and valid signatures by looking at it. They also have the potential of making a reasonable assessment of a signature’s legitimacy. For notaries, they have the potential of establishing the identity of a party based on what they claim to be. They achieve this through providing transaction logs of the signing parties.

However, when strictly dealing with digital signatures, the only trusted third parties is the digital certificates that has the repository for public keys. When verifying a digital signature, it is not proof enough to simply determine that the alleged sender affixed the digital signature. The process of verification establishes one thing; that there is a correspondence of the private keys with the public keys which embody the private keys.

Conclusion

In conclusion, with regard to digital security non-repudiation purposes to provide proof data originality and integrity. It utilizes asymmetric cryptography in providing data verification essential in both personal and business contexts. In the business contexts, security domains mainly purpose in preventing unauthorized activity. Information is sent through trusted systems of computing, which ensures security of information communicated in the business environment. Forensic analysts can assess legitimacy, and this justifies their increased use as trusted parties in securing computing in the business envrionement. On the contrary, digital certificates with repository for public keys are the only trusted parties.

Dylan, B. (2000). Non repudiation in the digital environment. First monday: peer-reviewed journal on the internet, 5(8): 1-5.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms and source code in C. New York: Wiley.