Global Information Assurance Certification Paper

Non-repudiation – Simple to understand, Difficult to implement

Keith Ainsworth
November 8, 2000

"It is estimated that $2.9 TRILLION dollars worth of electronic business transactions will be conducted over the Internet by 2004 according to Forrester Research"[1]. With that much money floating around in cyberspace there will be arguments that touch upon the legitimacy of a transaction. People will commit acts of fraud; people will also be victims of those acts. Information security professionals will play a major role in helping businesses protect themselves and consumers against false claims or repudiation of transactions.

Repudiation is defined as "the rejection or refusal of a duty, relation, right or privilege"[2]. If an electronic transaction is viewed as a binding contract between two parties, a repudiation of the transaction means that one of the parties' refuse to honor their obligation to the other as dictated by the contract. Thus non-repudiation can be defined as the ability to deny a false rejection or refusal of an obligation with irrefutable evidence.

The International Organization for Standardization (ISO) provides the main standards for electronic non-repudiation in the *Open Distributed Processing Reference Model*, the X.400 and X.800 series of standards. ISO/IEC 13888-1 maintains, "Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment" [3]. An important piece of information security in the digital economy is providing a mechanism for the non-repudiation function. The information security professional must help provide that mechanism by collecting and protecting the irrefutable evidence needed as defined within the transactional envelope.

"ISO provides for a series of non-repudiation services for conformance with ISO/IEC 13888-1, -2 and -3:"[4]

- Non-repudiation of Origin: This service will verify a signed message's originator and content through a data validity check.
- Non-repudiation of Delivery: This service will digitally sign an X.400 proof of delivery message.
- Non-repudiation of Submission: This service will digitally sign an X.400 proof of submission message.
- Non-repudiation of Transport: This service will provide proof that a delivery authority has delivered the message to the intended recipient.

Within a Public Key Infrastructure (PKI) environment, digital certificates can be used to generate a digital signature. This digital signature creates non-repudiation tokens that are used to provide evidence in the origin and delivery services transparently to the user. The only way to provide the submission and transport services is through the use of a Trusted Third Party (TTP).

A perfect example of a non-repudiation of submission is the service that the USPS provides when you send a registered letter. You are given a receipt that contains an

identification number for that piece of mail. If the recipient never receives the mail and claims that you have not sent it, the receipt is the proof that provides the non-repudiation of submission. If the USPS has the receipt of delivery that contains the recipient's signature, they have provided the proof for the non-repudiation of delivery service. The USPS provides the non-repudiation of transport service by acting as the TTP in the transaction.

While non-repudiation seems simple to explain and understand, in reality providing a full and complete non-repudiation service is a complex and difficult undertaking even for the most seasoned security professional. Full non-repudiation is a two-way street, although one-way non-repudiation is also possible. Both parties in the transaction must be protected by the non-repudiation services. "In order for full non-repudiation for both parties, the following steps must be taken:

- All parties must be identified and authenticated
- All parties must be authorized to perform the functions required
- The integrity of the transaction content must be intact throughout the entire process
- Certain transaction information needs to be confidential for authorized users only
- All transactions must be fully audited"[5]

Lets' extend the registered letter metaphor by changing the delivery mechanism to email and use the above steps to see how non-repudiation services are provided.

You access the corporate email system and use your userid and password to authenticate. You write an email to the VP of Human Resources requesting an out of band raise for one of your employees. You use your private key to sign the message and encrypt the message with the VP's public key because it contains sensitive salary information. The VP reads your email by decrypting the email using their private key and verifies the digital signature by using your public key certificate. The VP responds with an approval message that is also signed, using their private key, and encrypted using your public key. You first verify the signature with the VP's public key certificate then read that message by using your private key to decrypt the content. You complete the form for payroll to process the raise and when it gets to the VP of Human Resources to approve, they deny having previously approved the raise via email. You can use the following non-repudiation path to settle the dispute.

Your company has provided all employees with corporate digital certificates after extensive background checks analogous to the Verisign class A digital certificate issuance process in accordance with it's well defined security policies. They have verified identities by using the information provided in the US I-9 form that all employees are required to complete and issued and distributed digital certificates via the Corporate Certificate Authority, which acts as the TTP in this scenario. They have also created a process for the email server that automatically sends updates of generated public key certificates to all users. A unique userid for every employee is created at the same time the digital certificate is generated and assigned accordingly. The corporate security policy dictates the use of strong passwords and enforcement of this policy is performed via a special program. All of the above elements combined with the authentication mechanism

used to access the email system satisfy the requirement of all parties being identified and authenticated. The authentication mechanism can be improved via the use of a strong two-factor authentication mechanism but that is a topic for another discussion.

By gaining access to the corporate email system using the unique userid and strong password and their job descriptions allows authorized corporate managers to request and approve out of band pay raises for employees. These elements of the email transaction satisfy the requirement that both parties are authorized to perform the function.

Content integrity has been maintained via a message digest that is encrypted with the signer's private key to create the digital signature. By using a strong message digest function and creating an encryption of the resulting digest, the recipient of the message is able to guarantee that the contents have not been manipulated prior to delivery. By encrypting the digest strong integrity assurance is provided because the contents of the digest cannot be altered without breaking its encryption. The corporate email server acts as the TTP to ensure the non-repudiation of transport service. These elements combined ensure that the requirement for transactional content integrity has been met.

The private key of each user is kept confidential, according to corporate security policy, so that only the intended recipient could possibly decrypt the contents of the message. This meets the requirement that certain transaction information be kept confidential and only available to authorized users.

Since corporate policy states that all email is archived on the corporate email servers, an audit trail has been maintained. Your own personal security policy should provide for archiving and retrieval of sensitive data in case of emergency. This satisfies the requirement that the transaction be auditable.

When the VP objects to approving the raise, you can use the above techniques to produce the proof needed to provide non-repudiation. While this overview is very simplistic and does not delve into the technical details of how digital signatures are created and used, it is a valid example of how security functions are used in the business environment to provide a mechanism for non-repudiation.

In conclusion, while non-repudiation is always complex and sometimes difficult to implement, it is a clearly needed business function. By understanding the requirements of non-repudiation as it applies to the specific application, technology can be applied within the confines of the application to achieve your desired results. Using a combination of a clearly defined security policy and commonly available security tools and techniques, the information security professional can greatly enhance the non-repudiation process.

---

[1] Watson, Judy. "Wake-up Call", E-security,
URL:http://www.fortune.com/fortune/sections/esecurity/esecurity.htm
[2] West's Encyclopedia of American Law, Volume 9, page 4, Copyright © 1998 by WEST GROUP
[3] Information Technology – Security Techniques – Non-repudiation – Part 1: General. ISO/IEC 13888-1, 1997
[4] A McCullagh and W Caelli, "Non-Repudiation in the Digital Environment",
URL:http://www.firstmonday.dk/issues5_8/mccullagh

[5] Author unknown, "Sixth Security Building Block…Non-Repudiation" URL:http://www.amsinc.com/Amscat/SecurityBldgBlock6.htm