Vulnerabilities

Technology, Information Technology

Full Paper Vulnerabilities Electronic mail is the most common way of communicating messages to the sender. However, there are many associated threats and vulnerabilities that may breach any one of the three security fundamentals i. e. confidentiality, integrity and availability. Accordingly, during transit, if the message is modified, integrity and confidentiality will be breached. Similarly, non-repudiation issues will also occur, if there is no Public Key Infrastructure (PKI) that is operated by separate third parties. Likewise, the PKI is associated with digital certificates issued from a corporate authority i. e. Certificate Authority (CA) and is considered to be the most efficient control in terms of email security (Ellison & Schneier, 2000).

In case of secure email, one has to make sure about the sender possessing the key is the one who is the authentic sender. Likewise, when signed email is verified, one of the checks includes the source of the email i. e. the sender. However, if encryption is applied to the public key infrastructure, there is a requirement of identifying people possessing the relevant key to decrypt the message (Ellison & Schneier, 2000). This is the point where email certificates starts to operate, as the certificate ID is a digitally signed message from the CA that is transmitted to the user linked with the public key. However, the (PKI) possess many risks that may lead to vulnerabilities and in the end threats. One of the risks incorporates a breach of keys associated with the signer via unauthorized access or by any other means (Ellison & Schneier, 2000). However, efficient Certificate Authorities can mitigate risks by en effective physical security, personnel security and secure network. Pretty Good Privacy ‘ PGP’ counters these issues as well by

incorporating ‘ Web of Trust’ including self-governing signatures linked with the single certificate (Ellison & Schneier, 2000). Moreover, for addressing internal security, monitoring of employee emails is a regulatory requirement. However, there are many procedures, tasks and functions associated with it. The requirements can be met by utilizing tools from outlook express that are capable of retrieving certain keywords used in the email. For example, the keyword ‘ account’ can retrieve all emails including this specific word. (Bhatnagar, 2012). However, these outlook tools only work individually on each workstation and can be solved by incorporating Microsoft Exchange server. As the server will retrieve all emails of all employees containing the specific keyword, however, technical excellence is required in this regard. The second risk can be associated with the signer who does not know whether the information is certified or not. PGP addresses this issue as well by providing efficient key signers who are aware of the person whose key is in process of sign. Moreover, one more CA was initiated by the credit bureau by utilizing the legacy data maintained in the database for authenticating emails online. However, this mechanism requires a shared secret data and credit bureau that does not have data associated with it, as data is available for sale (Ellison & Schneier, 2000). Consequently, it is a weak point or a vulnerability, as a hacker only requires an identity theft for gaining the certificate.

References

Bhatnagar, A. (2012). Is your email secure? Journal of Financial Planning, 25(3), 42-43.

Ellison, C., & Schneier, B. (2000). Risks of PKI: Secure email. Communications of the ACM, 43(1), 160-160.