Local and distributed trust management: essay

Business, E-Commerce

Running Head: Local and Distributed Trust Management: Discuss the enabling Role and Challenges of local and distributed trust based management of intra enterprise applications for on-line banking from the perspective of a security manager: Discuss the enabling Role and Challenges of local and distributed trust based management of intra enterprise applications for on-line banking from the perspective of a security manager: In today's world of electronic commerce of online buying and selling, security is a top concern to the vast majority of security managers entrusted with the responsibility of securing the commercial sites and the transactions that are undertaken online (Bussler, 2002). These sites include money bookers, e bay, pay pal and Wells-Fargo. It would be worth to note that numerous hardware and software solutions have been developed to secure communication both on local platforms and distributed platforms. Such Solutions incorporate firewalls, VPN (Virtual Private Network) solutions, IPSEC (IP Security) protocol, SSL (Secure Socket Layer) protocol, HTTPS (Secure Hypertext Transfer Protocol), PKI (Public key Infrastructure), NAS (Network Admission server) and cryptography (Falcone, 2005). These platforms are run on trust amongst the different modules in the communication system, such that the modules of the system check and verify requests from a principal by an authentication process done by a different module in the system (Chen, 2004).

Notwithstanding the accessibility of the aforementioned solutions, challenges persist in privacy, security and reliability. The methodology of trust management between the involved parties is often undefined (Medhi et al, 2007). Thus, a thoroughly planned, robust and comprehensible infrastructure

must be adopted by the parties to facilitate authentication of requests and authorization of access to resources within the intra enterprise (Bussler, 2002). It is further recommended for purposes of review of the systems versatility, that log files for auditing purposes be kept. It is on this strength that trust based management systems were developed to enhance intra enterprise applications. Depending on the physical size of organisation, either a local trust based system or a distributed trust system can be implemented. These systems are support scalability, ease management, and enforce policy and large-scale implementation (Stølen, 2006).

Local trust based management: In a local trust based system, the system designers would decide whether to restrict access to organisational resources using just single password authentication methods, or through the use of smart cards, or biometric access, or single root PKI (public key infrastructure) (Bussler, 2002). Single user password authentication methods are easy to implement and resilient to brute force attacks specifically where users are urged to use strong passwords that are enforced using local security policy settings or group policy objects. Its shortcomings are that users' passwords can fall into wrong hands more so when handled carelessly.

A number of users prefer to apply easily memorable but nonetheless weak passwords that are defenceless in the face of brute force attacks (Chen, 2004). Application of smarts cards make available a better means of authentication for the reason that the individual user credentials are hard wired into a in a chip (Bussler, 2002). Properly handled smarts cards have

proved impossible to crack because they are able to present a more detailed data set that is easily portable. A common challenge of smart card usage is that smart cards are easily stolen consequently compromising the security of the entire system (Falcone, 2005). Biometric systems enable the use of indelible physical body features to provide access to resources (Chen, 2004). These include voice recognition software, fingerprint readers, and eye scanners. Biometrics has so far promised a stronger level of security for the reason that it solely accepts user input that is natural and hard to fake (Stølen, 2006). The down side comes with fact that biometric is not mature as a technology and exploratory researches are still being carried out to find ways of overcoming the challenges associated with it (Medhi et al.

, 2007). Furthermore, biometric systems are too costly to install and maintain as they require a huge initial capital outlay and specialised skill to run. This has held back their wide spread use and accessibility (Bussler, 2002). In a single/simple roots public key infrastructure, there is a trusted single root CA (Certificate Authority) that issues Public keys to users (Falcone, 2005). These keys are only valid if signed by the issuing Certificate authority (Chen, 2004). The signing binds individual public keys to their respective users (Chen, 2004). The advantages of a single root PKI is that has a centralised trust decision point hence making available a centralised point of administration. The challenge is that it provides for a single point of failure in the event that the certificate authority suffers technical hitches.

This kind of setup is not scalable in a wide spanning environment. To conclude, as there is only one private key used for signing, compromise of

this key automatically cripples the system in its entirety since the CA is not any more trusted as a unique signer (Bussler, 2002). Distributed trust based management: Distributed trust based management is implemented due to the massive scale of the enterprise either spanning different geographical regions or by the sheer huge numbers of entities accessing resources (Medhi et al., 2007). This follows that different physical or logical systems are used to provide access (Chen, 2004). The most notable methods for providing trust include the use of Radius Server and hierarchical Certificate Authorities (Falcone, 2005). In hierarchical CAs, the Root CA delegates and distributes trust to subordinate CAs (Stølen, 2006).

These subordinate CAs in turn issues certificates to end users or even other sub CAs depending on the size of the hierarchy which largely depends on the design implemented (Chen, 2004). Depending on the complexity of the design, we can have cross-certified CAs for reliability. This distributed type of design provides for a better infrastructure since if one CA is compromised, its certificates can be revoked and its users redirected to other CAs (Bussler, 2002). The disadvantage of this kind of trust based management is that the hierarchy gets too complicated such that tracing the certification path is impractical. Implementation and maintenance of this design requires a dedicated team and in cases where the root CA private key is compromised, the whole system will crumble (Medhi et al., 2007).

RADIUS (Remote Authentication Dial-in User Service) Proxy Server can be used to control access to a group of various individual RADIUS servers (Chen, 2004). Each division in the organisation is responsible for creation and

maintenance of its own database of users. The advantage of this structure is that the proxy radius can determine which server to query for information and it can implement load balancing to avoid traffic congestion (Falcone, 2005). References: Bussler C., (2002) Web Services, E-Business, and the Semantic Web: CAiSE 2002 international workshop, WES 2002, Toronto, Canada, May 27-28, 2002: revised papers, Springer, p 32-48Chen H., (2004) Intelligence and security informatics: Second Symposium on Intelligence and Security Informatics, ISI 2004, Tucson, AZ, USA, June 10-11, 2004; proceedings, Springer, p71-89Falcone R., (2005) Trusting agents for trusting electronic societies: theory and applications in HCI and E-commerce, Birkhäuser, p28-34Medhi D., Nogueira M J., Pfeifer T., (2007) IP operations and management: 7th IEEE international workshop, IPOM 2007 San José, USA, October 31-November 2, 2007: proceedings, Springer, p 39-41Stølen K., (2006) Trust management: 4th international conference, iTrust 2006, Pisa, Italy, May 16-19, 2006: proceedings, Springer, p59-61.