Network security research

Finance

Full Paper Authentication Protocols The Challenge handshake authentication protocol is used to vali the identity of a computer, connection or a request on the network. The validation process takes place in the initial stages, when connection ‘ A’ request to the connection ‘ B’ for establishing a communication channel. When the link is established between the two connections, connection A sends a message named a ‘ challenge’ to the connection ‘ B’. Connection ‘ B’ replies to the request by calculating a value with ‘ one-way hash’ utility. It is important for both connections that the hash value connection should be the required one; otherwise, the connection will be terminated. Moreover, these authentication procedures initialize at random intervals (CHAP, challenge handshake authentication protocol). Extensible Markup Protocol is more advanced as compare to CHAP as it supports multiple authentication methods. One more significant advantage EAP has that it executes on the link layer without IP address. Consequently, it is designed to support its own operations for retransmission of authentication request and order delivery. Moreover, the mechanism of EAP is based on lock step protocol concluding that it will support only a single packet in flight. This directs towards a negative factor for EAP that is not suitable for corporate networks having bulk data transmission (EAP, extensible authentication protocol). Password Authentication Protocol initially sends a LCP packet in order to create communication on a point-to-point connectivity over the network during link establishment. After the establishment of the link, PAP or PPP provides an authentication mechanism, which is optional. The optional authentication mechanism is provided prior to the network layer protocol stage. Previous two protocols do not have an optional authentication mechanism. Virtual Private Networks and Remote

Access Secure Socket Layer secures online transactions and develops trust for websites consisting of integrated electronic commerce services. SSL functions in three vital stages. The first stage involves an SSL certificate that activates encryption of confidential data that is transmitted during online transactions. The second stage involves an allocated view for each SSL certificate along with unique credentials that identifies the certificate owner. Lastly, the third step includes a certificate authority that authenticates the identification of the certificate owner prior to the issuance (Secure sockets layer (SSL): How it works - SSL Encryption/https from VeriSign, inc.). Internet Protocol Security is " a security protocol from the IETF that provides authentication and encryption over the Internet. Unlike SSL, which provides services at layer 4 and secures two applications, IPsec works at layer 3 and secures everything in the network. Also unlike SSL, which is typically built into the Web browser, IPsec requires a client installation. IPsec can access both Web and non-Web applications, whereas SSL requires workarounds for non-Web access such as file sharing and backup" (IPsec definition from PC magazine encyclopedia). Layer2 Tunneling Protocol (L2TP) as defined by the RFC 2661 was designed to facilitate dynamic tunneling on layer 2 within the packet data switching networks. L2TP illustrates a standard method for tunneling that enables connections similar to circuit to travel on one or multiple layers. Moreover, layer three operates on point to point and point to multipoint connectivity channels between locations of customers. L2TP also supports data encapsulation for multiplexing and de-multiplexing data transmission channels via nodes on the network (L2TP (layer 2 tunneling protocol)). Remote access protocols facilitate people to access a computer remotely by viewing the Graphical user interface. Whereas, VPN protocols

provide security and encryption along with a dedicated communication channel. Risk Assessment & Analysis The first step will be to analyze borders of the network and information system resources and exchange of information within the enterprise network. The first step is to gather information, which lays the foundation for conducting risk analysis. The system related information includes hardware, software, data, IT support staff, processes performed on the network, mission critical systems, data sensitivity. The operational environment of the enterprise network includes network design and topology, security architecture, system users, functionality of the network, methodologies for protecting the data in parallel with availability, confidentiality and integrity, input and outputs of the network, management controls, security controls, physical security, and environmental security controls. The outputs for this stage are system boundaries, System functionality, Criticality of the system and data, Sensitivity of the system and data. The second step is to analyze any potential threats for the network. While analyzing threats, is it essential to consider all possible, potential threats and sources which may disrupt or harm the network and information systems. The common threats related to natural disasters are floods, tornadoes, earthquakes etc. The common threats related to human includes hacking, cyber crime, viruses, malicious software attack, un authorized access to organization’s critical data, and deliberate actions. The environmental threats include substantial power failure, any chemical leakage, liquid spilled on any computing component etc. The output of this step is the identification of potential threats, which may disrupt the network and information systems in the future. The third step is to analyze any possible vulnerability within the network. This step

concludes the weaknesses and flaws, which are currently present in the network security architecture. The assessment of possible vulnerabilities is not an easy task as some previous history is required to perform vulnerability assessment. If the network is operational, a thorough analysis of the network security features and controls is conducted. It will also include technical and procedural elements for protecting the network. The previous reports of risk assessment, audit reports, system anomaly reports, network evaluation reports, network testing reports are considered. Some support is also considered from the vendor advisories, vulnerability bulletins from military networks and also by reviewing the history of previous security breaches within the network. Other methods are also used to breach the security infrastructure including penetration testing, which is an attempt to breach the network compromising the current security infrastructure. The method is used to test the current security measured for any possible vulnerability. References CHAP, challenge handshake authentication protocol Retrieved 4/22/2011, 2011, from http://www. networksorcery. com/enp/protocol/chap. htm EAP, extensible authentication protocol Retrieved 4/22/2011, 2011, from http://www. networksorcery. com/enp/protocol/eap. htm IPsec definition from PC magazine encyclopedia Retrieved 4/22/2011, 2011, from http://www. pcmag. com/encyclopedia_term/0, 2542, t= IPsec&i= 45408, 00. asp Secure sockets layer (SSL): How it works - SSL Encryption/https from VeriSign, inc. Retrieved 4/22/2011, 2011, from http://www. verisign. com/ssl/ssl-information-center/how-ssl-security-works/ L2TP (layer 2 tunneling protocol) Retrieved 4/22/2011, 2011, from http://www. networkworld. com/details/511. html