Essay

Table of Contents

INTRODUCTION

The research is going to explain the concept of internal information security; threats involve in data transfer and proposed techniques to resist the system from attackers. Insider attacks are more vulnerable than outsiders, every organisation under does such attacks. There are some security credentials which are described by the report. The report is also going to discuss the challenges and their solutions of asymmetric cryptography. There many threats while exchange the public key between numbers of people. The report includes the research about Digital signature, it is a mechanism to authentic the sender via un-trusted network and number of public key consumers. The report will discuss threats associated with 802.11 wireless networks. The threats are MITM attack and evil twin access point. The report provides the complete information like- functions, advantages, and disadvantages of four popular firewalls

TOPIC 1-INFORMATION SECURITY

Information security is a concept of confidentiality from data is being used by unauthorised access. It prevents the chances of data enclosure and data disruption. It provides a self-guard to the transmitted data. This concept is managed by Cyber security system, which contains the IT technology components. Generally, the attacker exploits the transmissions frames which are going from sender to receiver in analogue or digital form. Some hacker can miss direct the data or he/she may change some data and send it back to the actual receiver. This is more vulnerable and creates a drastic effect on the whole organisation and firms which are interact with the organisation. Malicious external threats are unintentional passive attacks (Sarkar, 2010). The organisation mainly focuses on such outsider attacks. This hacktivism is generally defended by IT technology which is also known as cyber security. But it is analysed that insider attacks are more catastrophic than outsider attacks. These attacks are less noticeable than outsider attacks, but in the present scenario, insider attacks are most commonly facing by each enterprise. Organisation needs to take both the threats seriously.

External cyber securities strategies provide defend from external threats only. It is commonly installed at each organisation. It gives negotiable assurance from internal hacking. IT professional are the bigger attacker than outsiders. Let it understand by an example- an angry

employee of the company who have the entire secret file and important documents of the company may expose these things to the rivals. IT workers of the company have a complete idea about cyber security credential. A malicious insider like IT administrators can easily steal the information. These insiders are exploited by the external rival organisation. Some careless insiders can apply wrong cryptography key or this resultant loss or modification of sensitive information of the company. Such threats are a disaster for the companies. Insider attackers have more potential than external. Insider IT attackers contain more powerful administrative tools and equipment. This increases the virtualization inside a company (Mathew.et.al, 2010). The virtualization means the controlling, monitoring and managing the data by virtual machines. Any one of the IT employees can cut, copy, modify or delete numbers of sensitive documents. It takes very few times to click by the mouse. Hence, the damage is very simpler and faster than outsider attacks. Insider attacker is very difficult to detect. Insider cyber criminals can sabotage the whole system of the enterprise. According to PwC Global State of Information Security Survey, 2005 most common cyber criminals are belong from company's employee.

IT technologies are continuously focused on the modifying privilege of security credentials. To minimise the risks the company should find their important assets and its location. If the company is most dealing with money then money is need to be protected by strong physical location. If the assets are data then the company should store it by applying username, password, Key and cryptographic technique. This will create a firewall on the important data. Apart from this, organisation have to observe suspicious behaviour or out of character behaviour. The staff should be a boast to investing data leakage by their colleague (Stolfo.et.al, 2012). The security is more adaptable at a higher level of the hierarchy of the organisation i.e. owner and information custodians. It is needed to take security training for information custodians so that they can restrict the access of information. This training will give some schemes for lower the privilege of resource access. This principle defined the roles and responsibility of each employee, so that gives restriction at technical and physical level (Coles-kemp & Keromytis, 2012). In future, it is necessary to implement a strong database and implement its backup which is must be managed by advanced IT security tools. This will mitigate the insider attacks and secure backup is used for recovery purpose if the documents are disrupted by criminals.

Research also suggests that minimise the criminal getting- into the firms by implementing policies and procedures. These policies are must be more powerful to ensure the strong commitment to complete security of the network. Procedures must trap the consequences which leak the information of the company and it works as a victim to catch the attacker inside the organisation.

TOPIC 2-CRYPTOGRAPHY

Public key Cryptography is also defined as asymmetric Cryptography. In this Cryptography technique system uses two keys- one is private and another one is public. Any people who have public key may encrypt the message but decrypt only by private key or encrypt by single private key but decrypt by a number of public keys. The complete cryptosystem contains key exchange algorithm, secure transport layer, encryption and decryption key methods and digital signatures.

Major challenges which are found in the asymmetric key is that it require more secure channels to exchange a number of public keys and the receiver is also using different transport channel. In this method, there are more chances of a man-in-middle attack. It can be happening due to decryption occurs at many parties so attackers have many chances to observe decryption at many systems. When the hacker traps the public key, he/she may take a data or encrypt it from his/her public key and send to the network transport layer. On the receiver it will create suspicion. To identify these attacks is very difficult because transmission includes wireless media or some other public transport channel (Raw.et.al, 2013). In order to overcome such problem, a third trusted party must be involved in the system. Only the trusted party system can allocate digital certificate to a person, organisation or an entity. The certificate includes digital sign which indicates that public key belongs to which person. It is needed that sender has to send data with his/her digital signature. In this way, it is authenticated and more secure.

Another way to overcome such problem is to use RSA algorithm for key exchange. This provides a secure key exchange algorithm which is not easily hacked by attackers. RSA algorithm is invented by Rivest, Shamir, Adleman in 1977 in order to credential key exchange process. RSA algorithm is very strong which is proven to computationally undetermined method. This algorithm is used basically 4 keys- one is for encryption, another one for decryption and

two other public register and private register key which need to be kept secure. Such algorithms are necessary to implement at server or client site(Agudo.et.al.,2011). It provides complete authentication as well as credentials and it reduces the chances of spoof between transmissions from a sender to receiver.

Digital signature gives assurance on the receiver that the document is legal or not. The method is used to provide authentication. In public cryptography system, there is a number of the entity that has public key. The difficulty is raised that how the receiver will know the information about the sender. There is a possibility that attacker may hack the public key and send unauthorised data. To overcome such issues digital signatures tend to use. Each entity needs to authenticate itself by a digital signature. This technique is used to provide confidentiality on unsecured channels (Kotz, 2011). In future if the receiver wants to claim something then he/she can easily claim on sender with proof of valid digital signature, it is also known as non-repudiation. Digital signature is equally validated like handwritten signatures. But the digital signature is more securable than hand written signature. Hand written signature can be copied by professionals. This cannot happen for digital signature. Digital signature software generates a hash code by sender's own private key. The hash code is valid for one time only. This hash code is applied for complete documents to valid each transmitting frames. The speed of hashing is faster than handwritten sign on a number of the documents which is to be sent. Every hash contains the unique value. If the cybercriminal alters or delete any letter from the transmitted frame, it is easily detected on receiver site and receiver will generate the new request to the server.

In the present scenario, the digital signature is now becoming a challenge for information technology. Papers documents are rapidly replaced by electronic documents. Enterprises are using a watermark and digital signature but it provides lack security. It's all depend on the digital signature process, suppose if the digital signature is not so much strong or if it uses a simple method that attackers will easily trap the signature or make fake signature resultant which drastically impact on the organisation(Skarmeta.et.al.,2011). Apart from this some digital signing process has limitation to generate hash code or sometimes the process takes the intensive amount of time. To respond such challenges some jurisdictions require like safeguard at digital signing

process, deploy to manage and must be one-time product for a particular organisation only, not to allocate it on another organisation.

TOPIC 3 - NETWORK SECURITY FUNDAMENTALS

802.11 is a wireless local area network technology it provides communication between network and base stations. This network is induced by media access control and physical network layer. It allows transmission between two wireless clients. It is basically a wireless network so that it cannot be physically secured (Von mulert.et.al, 2012). The attacker may attack this network by sitting at any place whether it office or a park or any street. Wireless network is less defending and it is very critical to defending them. It is mostly threatened by man-in-middle attack. In this attack, two parties are believed to communicate each other without knowing about the third person who is secretly altering the communication. Attacker built the independent connection with both the parties and grasps the data. Then he/she change the data and send to another party (Hiertz.et.al, 2010). The attackers generally impersonate themselves at each end point of the wireless network. It mostly happens that MITM (man in the middle) takes secret key at the start of the communication. Suppose one party wants to exchange the secreted key then the attacker will transfer the message without alteration to another party. After the complete process, the cyber criminal has both the security key. Now the attacker can do anything with the communicating message whether he/she trap the communication silently or alter the message at drastic level. MITM criminal mainly exploits real-time data transmission (Khan.et.al, 2010). In 802.11, WLAN data packets are travel all over the network openly so the attacks are more vulnerable.

EVIL TWIN ACCESS POINT

Evil Twin is defined as a rogue wireless access point which offers as valid and legal access to the network but actually it secretly access the private data. It eavesdrop the communication without interrupting the communicating parties. Wireless users are making fool by attackers which are professed them as legitimate network providers. Such criminals steal password and all the security credentials at just the one time access of users. Evil Twin Access Points are easily set as it only requires a laptop or a smart phone and a wireless network card which purport itself as an access point. These fraud access points are very hard to trace because

at any time they shut down their connection (Song.et.al, 2010). Sometimes the attacker positions himself with victims so that victim is trapped by tempting on a high-speed network and starts to use it. The computer of the attacker automatically chooses an end user and hack his/her security credential with interrupting the network access. It was also known by honey pots or base station clones. To overcome this VPN becomes a safety guard for the wireless users. VPN works as a tunnel between the network and the user. This network encrypts the data send to the network so it reduces the chances of being a trap to the network. The wireless users should only use public authenticated network, they should carefully access online shopping or banking site.

When legitimate credentials are sent to legitimate access points then there are still chances of threats. The attackers can hack the data while transmission and easily grab the information at endpoints of network. Legitimate credentials contain important and sensitive data. When these are sent on public authorised network, there are chances of man in middle attacks. According to the research the users need to include a security network to overcome such threats. The user can implement VPN network which works as a tunnel between communicating network and user. VPN network provides security by applying algorithm of encryption and decryption. Encryption is a technique which converts plain text into cipher text and this cipher text is sent to the receiver via a legitimate network (Noubir.et.al, 2011). The encryption process is implemented by using the private key. At the receiver end, cipher text is converted into plain text, this process is known as decryption of message. Decryption process occurs. This technique is known as Cryptography. Legitimate credentials are needed to be secured by such techniques. In legitimate channels, it provides the resistant from data overhearing but it does not have control on data tampering. This research proposed that strong protocol is needed to exchange secret information. To exchange the key, it has been suggested to using a strong mechanism like- RSA algorithm or Diffie–Hellman problem. These algorithm are very hard to solve or computationally infeasible. Such eavesdropping schemes are impossible to hack the information of secret key.

TOPIC 4 – FIREWALLS

Firewall is a kind of network security mechanism, which prevents unauthorised and illegal access of data packets. An ideal firewall resists the access of both hardware and software. In this way, it provides security both at network and computers. Firewall act as a barrier between

transfers of incoming and outgoing data packet. Hardware firewalls are installed on the host; it is a layer of software. It resists the data traffic on a single machine and resists the data going on outside the machine without user permission. The technology is most important for the consumers because their hardware machine contains hidden malware or viruses which may send credential information. The host firewall acts as a barrier in such cases.

Popular Firewalls

1) *Circuit level gateways*

Circuit level gateways observe the network and bounded the unrequested data packets coming from the host. In OSI model, it is implemented at the session layer. It handles the excessive data traffic by data filtration schemes based on port and IP address associated with packets. It controls on TCP three ways handshaking status of connection from start to end. If the connections have time out then the firewall will not allow the transmission of data packets (Zuk.et.al, 2013). Circuit level gateways optimise the connection, whether it is legitimate or not. This deployed model coming into the when connection is established on the first time. A device transfers the information outside the network. It helps at initial screening process.

Advantage:

Circuit level gateways are cost efficient and comparatively inexpensive. It also provides vagueness on private network from the outsiders.

Disadvantage:

Circuit level gateways do not filter packets individually. After completing the screening process and establish the connection, the outside attacker can take advantage of it.

2) *Packet Filtering firewalls*

Packet Filtering Firewalls are generally implemented at the routers. Routers connect the host network to the internet. In OSI (open system interconnection) model, packet filtering firewalls are deployed on Network layer. Such firewalls control the access according to its configured list. It observes all the packets which are coming from the network. It screens all the packets according to defined rules. These rules are configured by Network Administrator. If in case, a data packet does not meet the defined criteria then it drops the packet and updates the

information of dropped packet (Trabelsi & Zeidan, 2012). Network Administrator defined the access control list (ACL) by protocols, IP address and attributes of the data packets.

Advantage:

Packet Filtering Firewall is best suited for small level network. It uses very few resources so it is very cost efficient.

Disadvantage:

Packet Filtering Firewall are only preferred for small network but not so much efficient for complex rule based models. It works only at the network layer so there are still chances of spoofing.

3) *Application level gateways firewalls*

Application level gateways firewalls are normally deployed on the application layer of OSI (open systems interconnection) model. It acts as an intermediate medium between one network to another specified network (Krueger.et.al, 2010). In this way, it prevents the direct connection. The most common example of such firewall is Proxy server. It protects from a threat on application layer by defined application protocols. Some other application level gateways are HTTP and POP3 protocols. It may block or allow the traffic based on set rules.

Advantage:

The biggest advantage is that it prevents the direct attacks on VPN (virtual private network) and it resists unwanted traffic due.

Disadvantage:

Proxy firewalls like HTTP or SMTP each requires a new proxy agent. It is very difficult to manage new proxy agent for each firewall. Sometimes it is incompatible with installed proxy firewall. The configuration of the proxy is difficult as compared to other firewalls. VPN network does not work properly with proxy firewalls as it modifies the IP address of the host. It would lose the data packets. It is also flexible only for high bandwidth network due to additional processing is required.

4) *Stateful Multilayer Inspection Firewall*

Stateful Multilayer Inspection Firewall is the combination of all above discussed firewalls. It filter the coming data packet on Network layer according to ACL, contol on the data packets at Application layer, legitimate the packets on the gateways (Stouffer.et.al.,2011). It adapts the technology of above three firewalls and provides flexibility.

Advantage:

It provides direct communication between client and the server. It implement by complex security models and strong algorithm.

Disadvantage:

The biggest disadvantage of stateful multilayer inspection firewall is that it is very difficult and complex to configure the settings. It does not examine the complete packet. Thus, it provides low level protection.

CONCLUSION

The report concluded that insider attacks are more frequent and it impacts drastically on the organisation. It has been suggested that owner of the organisation should change the policy of security credential of the company. Administrative tools are necessary to implement in the company. The IT security tools will monitor, control and manage data on virtual machines and it also provides privilege of sensitive data access. The report concluded the attacks on wireless network 802.11 that is a third person may alter the information because the data packets are freely transferred in the network. The report included the control on the flow of data packets by firewalls that are- circuit level gateways, packet filtering firewall, state-full multiple layer firewalls, application-level firewall.

REFERENCES

Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P. and Lambrinoudakis, C., 2011. Cryptography goes to the cloud. In *Secure and Trust Computing, Data Management, and Applications* (pp. 190-197). Springer Berlin Heidelberg.

Coles-Kemp, L. and Theoharidou, M., 2010. Insider threat and information security management. In *Insider threats in cyber security* (pp. 45-71). Springer US.

Hiertz, G.R., Denteneer, D., Stibor, P.L., Zang, Y., Costa, X.P. and Walke, B., 2010. The IEEE 802.11 universe. *Communications Magazine, IEEE*,*48*(1), pp.62-70.

Khan, S., Loo, K.K. and Din, Z.U., 2010. Framework for intrusion detection in IEEE 802.11 wireless mesh networks. *Int. Arab J. Inf. Technol.*, *7*(4), pp.435-440.

Khan, S., Loo, K.K., Mast, N. and Naeem, T., 2010. SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks.*Journal of Network and Systems Management*, *18*(2), pp.190-209.

Kotz, D., 2011, January. A threat taxonomy for mHealth privacy. In*COMSNETS* (pp. 1-6).

Krueger, T., Gehl, C., Rieck, K. and Laskov, P., 2010, March. TokDoc: A self-healing web application firewall. In *Proceedings of the 2010 ACM Symposium on Applied Computing* (pp. 1846-1853). ACM.

Mathew, S., Petropoulos, M., Ngo, H.Q. and Upadhyaya, S., 2010, September. A data-centric approach to insider attack detection in database systems. In *Recent advances in intrusion detection* (pp. 382-401). Springer Berlin Heidelberg.

Noubir, G., Rajaraman, R., Sheng, B. and Thapa, B., 2011, June. On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming. In *Proceedings of the fourth ACM conference on Wireless network security* (pp. 97-108). ACM.

Raw, R.S., Kumar, M. and Singh, N., 2013. Security challenges, issues and their solutions for VANET. *International Journal of Network Security & Its Applications*, *5*(5), p.95.

Sarkar, K.R., 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), pp.112-133.

Skarmeta, A.F., Hernandez-Ramos, J.L. and Moreno, M., 2014, March. A decentralized approach for security and privacy challenges in the internet of things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (pp. 67-72). IEEE.

Song, Y., Yang, C. and Gu, G., 2010, June. Who is peeping at your passwords at Starbucks? â?? To catch an evil twin access point. In *2010 IEEE/IFIP International Conference on Dependable Systems&Networks (DSN)* (pp. 323-332). IEEE.

Stolfo, S.J., Salem, M.B. and Keromytis, A.D., 2012, May. Fog computing: Mitigating insider data theft attacks in the cloud. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on* (pp. 125-128). IEEE.

Stouffer, K., Falco, J. and Scarfone, K., 2011. Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), pp.16-16.

Trabelsi, Z. and Zeidan, S., 2012, June. Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement. In *Communications (ICC), 2012 IEEE International Conference on* (pp. 1074-1078). IEEE.

Von Mulert, J., Welch, I. and Seah, W.K., 2012. Security threats and solutions in MANETs: A case study using AODV and SAODV. *Journal of network and computer applications*, *35*(4), pp.1249-1259.

Zuk, N. and Guruswamy, K., Juniper Networks, Inc., 2013. *Multi-method gateway-based network security systems and methods*. U.S. Patent 8,370,936.