UNC CHARLOTTE

College of Computing and Informatics

Department of Software and Information Systems

Enterprise and Infrastructure Protection
ITIS 6230

MIDTERM PROJECT

PKI LAB

SAHIL BHIRUD - 801138029

This lab was designed to provide hands-on experience on Public Key Infrastructure (PKI) and also for better understanding of the same.

From this lab, I have concluded that the functioning of PKI is completely based on Digital Certificates. A digital certificate is a form of electronic identification for websites. Secure connections are established between two parties because the identities can be verified by the use of certificates. If the Certification Authority (CA) is compromised by the attacker, then he/she can attack all the users using that CA. I also observed that PKI prompts and tries to warn the users about the malicious website they are about to visit. Other procedures which I learnt are how to establish a Certification Authority (CA), issue certificates to website, create a Web Server and host a website on it and how a Man-In-The-Middle attack occurs.

In future, I will be meticulously scanning for all the signs my web browser is trying to give me of a malicious website. In my professional career, I will also be able to enlighten my colleagues about how PKI tries to safeguard the users from accessing malicious websites over the Web and protect them from attacks like Phishing, Man-In-The-Middle, etc.

I would prefer Attribute-Based-Encryption (ABE) over Public Key Infrastructure since ABE provides security and access control to the user. It is a Public Key based one to many encryption that allows users to encrypt and decrypt data based on attributes. Encryption and decryption can be done only if the number of matching attributes is at least of a threshold value [1]. Moreover, Chase and Chow [2], provide a solution which removes the trusted central authority and protect the users' privacy from the trusted third party vendors and hence, making ABE more usable in practice. They present a multi-authority ABE with user-privacy and without the trusted authority. Their system uses anonymous key issuing protocol which allows multi-authority ABE with enhanced user privacy i.e. they allow users to communicate with Attribute-Authorities (AA) via pseudonyms instead of having to provide their GIDs and they also prevent the AAs from pooling their data and linking multiple attribute sets belonging to the same user. Some of the advantages of ABE are data confidentiality, secured access control, scalability, user accountability and user revocation [1].

Downside of PKI is that various vendors sell different solutions of PKI and if the vendor goes bankrupt then, it will be very hard to obtain the same service. Also, fraudulently issued certificates with malware is another disadvantage. The companies which issue certificates are under the

misconception that they are secured from all the threats. If a company which issues certificates is breached, then all the users fall victim to the attackers [3]. There are also chances of MITM attacks when it comes to PKI. If the attacker gets control of the certificate authority, then he/she will be able to compromise all the users which are using certificates issued by that certificate authority.

Sieve is modern platform which uses ABE while sharing information with a web service over an untrusted cloud. This platform has proved to be efficient and secure. In this system, only the user has access to all the decryption keys. Using ABE, Sieve allows user to define access policies which are cryptographically enforceable. Sieve implements cryptographically strong access controls using ABE. ABE uses a master secret key to generate decryption keys which is in possession of the user since Sieve is a user centric system [4].

REFERENCES:

[1] R.Nitya Lakshmi, R.Laavanya, M.Meenakshi and Dr.C.Suresh Gana Dhas, “Analysis of Attribute Based Encryption Schemes,” *International Journal of Computer Science and Engineering Communications Vol.3, Issue 3, 2015, Page.1076-1081 ISSN: 2347–8586*

[2] M.Chase and S.S.M. Chow “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” *Proceedings of the 16th ACM conference on Computer and communications security, November 2009, Pages 121–130*

[3] V.Lozupone “Analyze encryption and public key infrastructure (PKI),” *International Journal of Information Management, 38(1), 42–44*

[4] F.Wang, J.Mickens, N.Zeldovich and V.Vaikuntanathan “Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds,” *13th USENIX Symposium on Networked Systems Design and Implementation 2016, 978-1-931971-29-4, Santa Clara, CA, pages 611--626*