Volume 6, Issue 8, August 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication Against Man-in-The Middle Attack & Honey Encryption

Mohit Koul
Department of Computer Engineering, SKN Sinhgad Institute of Technology & Science,
Lonavala, SPPU, Pune, Maharashtra, India

Abstract— Mobile Authentication is the verification of a user's identity through the use of a mobile device. It can be tampered using malicious attacks & attacks done on client machine. In this paper, we present a survey on the network attack in wireless environment .we will discuss vulnerabilities ,security in Man-in-Middle attack & security at the access point where the attack is imminent. The ASMiTM attack vulnerability exploits the WPA2 encrypted Wi-Fi-Networks protocol &is responsible for injecting malwares & sniffing private data of users. Human interaction is the only way security is exploited. The Mobile Protocol will be an alternative to prevent MITM & security at access point can be increased by using Honey Encryption techniques.

Keywords— Authentication, access point, ASMiTM attack, MITM-Man in the Middle Attack, Honey Encryption, WPA2

I. INTRODUCTION

Authentication using only passwords has become Obsolete and is no longer considered safe. Even a phishing attack executed remotely can cause password theft. Due to this online banking services have switched to a more secure authentication alternative. This includes two factor authentications, which requires OTP to be sent on phone which makes authentication to be depended on something you have, not on something you know. Wi-Fi networks are also prone to attacks. Advanced Stealth Man-in-the-Middle (AsMiTM) that is a combination of SMiTM (Stealth Man-in-the-Middle) And WDoS(wireless Denial of Service),both exploit the hole 196 vulnerability and causing malicious insiders to inject spoofed frames using group transient key whose access was given to access points(APs) according to802.11 standard. The ASMiTM is an improved version and its attacks are difficult to detect, has increased attacking duration and higher stealthiness wrt MiTM and DoS.The security at the access point can increased by using Honey Encryption which creates a cipher-text that, which when decrypted with false password generates a false but correct looking message which confuses the hacker whether he was successful in decryption or not.

II. PAGE LAYOUT

Some digital certificates are defined for user authentication via mobile defined by ETSI standard. Currently solutions for EAL4+ certified sim cards which get activated over the air when user subscribes for the service.

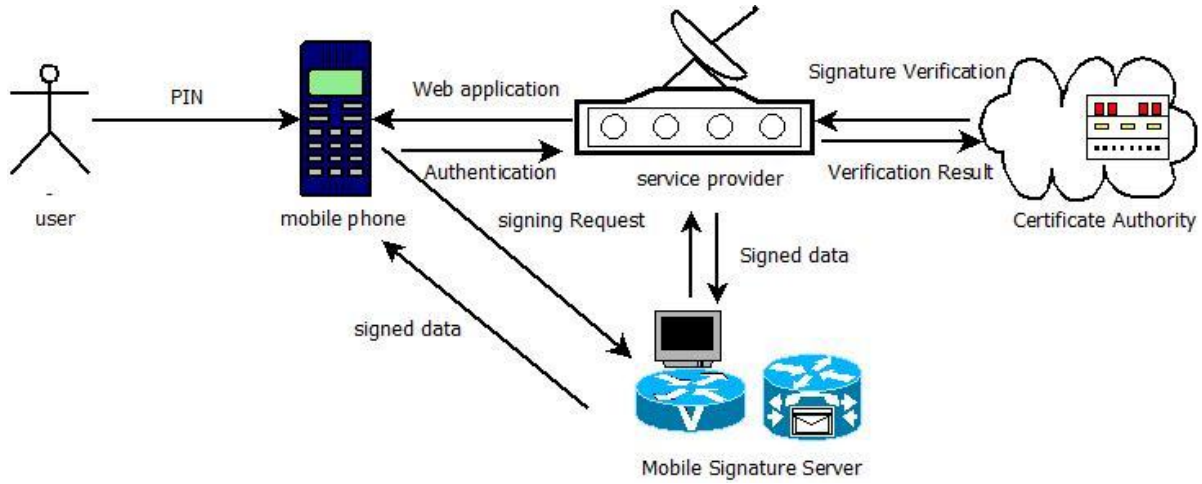

Fig.1 The solution of currently available mobile solution

Keys are generated for each certificate. sim cards store private key. Public key is stored in a directory.

When user requests a service, authenticating service automatically pops up on the phone requesting the signature. However MITM attack can be occurred by stealing the credentials stored by the above system on sdcard.

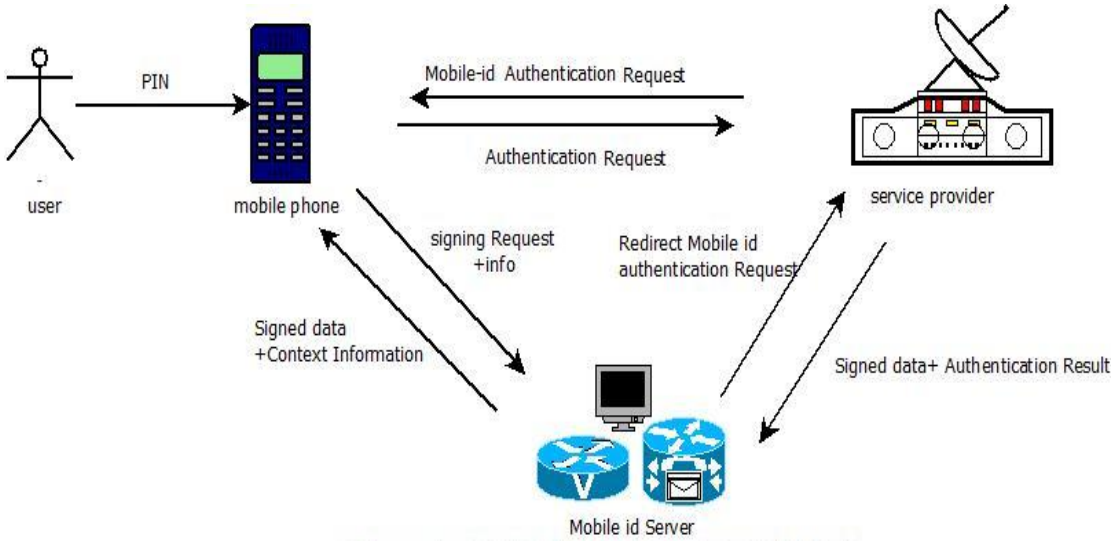

Fig.2 operation of mobile id protocol secure against MiTM attack

To overcome this mobile id secure protocol is used that uses a single sign on solution.

The user inserts sim in the phone and public-private key in the sim card gets certified automatically. The browser inbuilt in phone communicates with the server. As soon as user inputs the url to site he wants to navigate to, a connection is established between browser and service provider. The service provider establishes a secure TLS/SSL connection and user can login using mobileid credentials.

The main advantage is that the mobile id server can differentiate between the legitimate user and hacker and therefore break the connection.For better understanding here is an example:Suppose Alice receives a phishing email that pretends to be her bank gbank.com but contains a link to the bogus site ggank.com.With her mobile device, she clicks on the link and opens ggank.comWhile thinking she is visiting gbank.com. The bogus site immediately opens a session on the real bank website gbank.com to impersonate Alice and commit a fraud. Since Alice chooses to use Mobile-ID, the bogus site has no choice but to mimic it on the real site. Then, the real bank web site establishes a secure connection to MIS to authenticate Alice.MIS obtains a signed message from Alice's machine which contains the information that Alice is connected to ggank.comMIS notices the mismatch between the real and bogus web sites and informs gbank.com for this incident. As a result, a real-time phishing attack is prevented. The signing capability of Sim card called the Secure Element we can have communication in two ways:

Remote communication with SE

The mobile operator establishes a communication with secure element(sim card) remotely using encrypted SMS messages. Bypassing mobile terminal. The main advantage is that it is immune to malware.

Local communication with SE

The other approach requires accessing SE from a local application providing a protocol against MiTM attack.

The former approach has a disadvantage that malicious software may run on client machine generating fake transaction keys .the late approach has a disadvantage that mobile id protocol will only work if the user is accessing the service from his own device registered not any anonymous machine.

III. HOLE196 VULNERABILITIES, SMITM, AND WDOS ATTACKS

The Hole196 Vulnerability exposes the WPA2 protected Wi-Fi networks. Only access points are allowed to use the group transient key for broadcasting frames to the client. But malicious hackers can spoof as access Points (APs) & inject modified frames that affect the connected device.

A. SMiTM ATTACK

SMiTM attack usually involves poisoning the Address Resolution Protocol (ARP) cache of the client to intercept the client's traffic. This attack is however short lived as ARP gets refreshed ARP cache entries gets replaced with genuine ones.

B. WDoS ATTACK

WLANs remain very vulnerable to Denial of Service attacks. While you may not be able to prevent DoS attacks, a WIDS can help you detect when DoS attacks occur and where they come from, so that you can track the intruder down and bring him to justice -- or at least scare him away.

C. ASMiTM ATTACK

It is a combination of both the attacks with increased efficiency and tougher detection.The attacker terminal is loaded with backtrack os and drivers such as MadWifi drivers and wpa_supplicant .the attacker spoofs as AP &uses the group

transient key for encryption .wpa_supplicant is used to obtain the most recently group transient keys used by clients..MadWifi drivers helps the attacker to use the group transient key for encryption .Once setup with all these attacker converts the ToDS frame to a FromDS frame .this is where the attacker gets in the network .

In SMiTM attack ,the attack is nullified by refreshing the fresh ARP updates which clears the false IP:MAC mapping.However,in ASMiTM ARP refresh cannot nullify the effect .Even if ARP refresh clears the false IP:MAC mapping the geuine mapping cannot be obtained immediately as inflated packet number delays the ARP frames coming from the target. the attacker can remain in the number by choosing an appropriate inflated value of the packet number.

IV. HONEY ENCRYPTION

To increase the security at the access point, we will use honey encryption technique .Hacking tools such as John Ripper (www.openwall.com/john) enable to easily crack the hashes when passwords inside them are weak.

Many users store there password in apps like DashLane, Last pass or Apple iCloud KeyChain. They store passwords not their hashes in a database and encrypt it under a master password .However these password managers are vulnerable to brute force attack. But at the lager end they are safer and can be applied at the access point.

So when the attacker actually exploits the hole 196 vulnerability and tries to get the group transient key used at the access point, decrypts it ,will get correct password looking key which is actually a cipher text confusing the hacker that whether the key obtained is correct or not. Thus, enabling security and reducing the attack probability.

V. PROPOSED WORK

Mobile-id protocol has reduced the Man-in-Middle attack but hole 196 vulnerability needs to be work upon for which honey encryption can be proposed as technique to stop the infiltration of the attackers.

VI. CONCLUSIONS

Thus we conclude that the malicious software can break user authentication but by using mobile-id protocol and can avoid man in middle attack. however the main solution for MiTM attack rely on user's awareness because human error is the main source of security failures . Also the hole 196 vulnerability causes attacks such as WDoS, MiTM and ASMiTm attack however using Honey encryption at the access point can avoid these attacks and secure the network.

REFERENCES

[1] Mobile Authentication Secure against Man-in-the-Middle Attacks *K. Bicakci ; TOBB Univ. of Econ. & Technol., Ankara, Turkey ; D. Unal ; N. Ascioglu ; O. Adalier*

[2] Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks *M. Agarwal ; Dept. of Comput. Sci. & Eng., Indian Inst. of Technol. Guwahati, Guwahati, India ; S. Biswas ; S. Nandi*

[3] Honey Encryption: Security Beyond the Brute Force Bound Ari Juels, Thomas Ristenpart-University of Wisconsin.

