Reliance on Untethering : A new way to remote attacks in wireless

Nitesh Chouhan*, Hemant Kumar Saini**

*Assistant Professor, at MLV Government Textile & Engineering College, Bhilwara (Rajasthan).

**MITRC, Department of Computer Science& Engineering, Alwar,Rajasthan

Today with the emerging technology remote computers in the every world becomes a wide wireless spectrum. But this widening wireless technology unfortunately becomes the platform for malicious practitioners to play new dangerous attacks. With such a skill where Untethering which seems to be the most popular secure way for communication, one cannot imagine that it might become a door for attack.

Untethering

Most times when the people is seen using Smartphone, laptops for the surfing the web. They usually make data connection either via Bluetooth, Wi-Fi or connect PC through Smartphone. Some are using USB air cards to connect. This type of plugging devices to use data is known as tethering. And when the data usage or surfing is over the devices being disconnected it resembles the Untethering or we can say that device work as stanalone or in a peer to peer network. Or it can be said untethered means a portable system that relies on a wireless connection to other computers.

Analysis for attack

It is necessary to identify the security barriers and mechanisms in the communications to defeat the attacks. That's why a hypothetical model attack graph can be assembled which exploits essential factors to penetrate defenses as shown in Fig 1. This graph reveals the security defenses which help in overwhelming them.Not only this but the model predicts substitution paths with the preliminary access to demanding goal, all this make attacks more complex than a single remote root exploit.

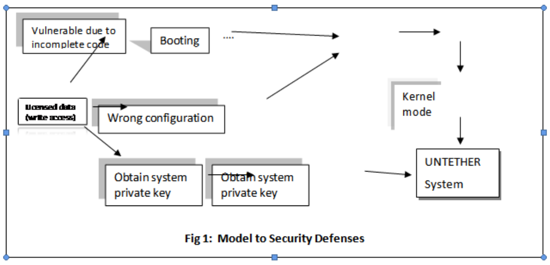
Vulnerable due to incomplete code
Booting
....
licensed data (write access)
Wrong configuration
Kernel mode
Obtain system private key
Obtain system private key
UNTETHER System

Fig 1: Model to Security Defenses

Comprisingsecurity

The key generated is kept within the data or the system in untethered mode as seen in Fig. 1 and hence vulnerable to break or tamper the key. Since the key is placed with document so that it is convenient to access data without network connection and client protected key. But this would be less secure and the devices can be taken for reverse engineered which is much handy as the hardware's can be easily re-engineered and the key can be easily revoked.

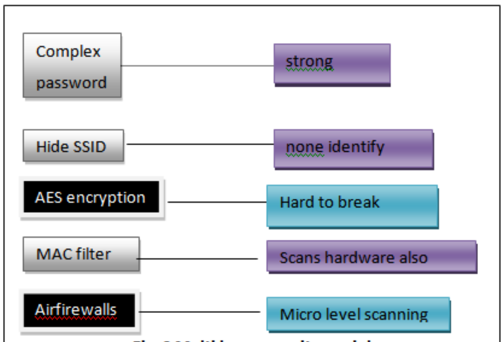

Fig. 2 Multi layer security model

Protection measures

Although the intruders keep on finding the new ways to attack the WLAN, still some measures can be taken with the multilayer security which is of paramount significance as shown in Fig. 2. Those key measures are as:

- ✓ Choose Strong and complex passwords that could not be easily guessable.
- ✓ Hide service set identifier (SSID).
- ✓ Authenticate the access points based on IEEE 802.1x standards and encryption by IEEE 802.11i (WPA2) that uses the advance encryption standard(AES) algorithms with 128 bit key.
- ✓ Timingly scans by enabling media access control (MAC)filtering.
- ✓ Disable remote administration.
- ✓ Implement Airfirewalls thwarting the attempted intrusions or snooping.

Conclusion

As the Untethering mode rely their security on the obscurity which is again a proprietary “scrambling” algorithm which can be breached. Not only this , in untethered mode end users may be the attackers itself which seems to be connect in the group to get key or might connect to store the key into its device which would be later reverse engineered .And when the key isoncebreak, it can be easily run everywhere. This is a serious concern in the wireless spectrum which should be taken into account in the secure wireless spectrum. However the multilayer security model has been discussed to prevent at some extent but still it finds the topic of future research.

References

[1] Choosing an Enterprise Rights Management System: Architectural Approaches ,http://www.infosecwriters.com/text_resources/pdf/ERM_AVOCO.pdf

[2] Secure untethered, IP-enabled devices, http://embedded.communities.intel.com/community/en/software/blog/2010/01/14/secure-untethered-ip-enabled-devices.

[3] http://untetheredoffice.com/tether-or-not-tether-your-smart-phone/

[4] RSA 2014: Experts discuss the most dangerous new attack techniques,http://www.scmagazine.com/rsa-2014-experts discuss-the-most-dangerous-new-attack-techniques/article/335815/