WIRELESS SECURITY AND ROAMING OVERVIEW

Nidal Aboudagga,Jean-Jacques Quisquater
UCL Crypto Group - Place du levant,3 - 1348 Louvain-la-Neuve Belgium
aboudagg@dice.ucl.ac.be,quisquater@dice.ucl.ac.be

Companies and persons request omnipresent connectivity with high confidentiality. For this reason the progress in wireless network is growing very fast.

SECURITY

WEP [2] was a protocol based on the symmetric algorithm RC4 and used problematic static 40-bit or 104-bit key, but failed to ensure confidentiality, integrity and authenticity in wireless communication. It was subject of many attacks, IV collision, authentication spoofing, replay attacks, etc. The 802.1x Standard [4] was adapted to Wireless LAN as basis for access control, authentication and key management. The 802.1x standard combines a 128-bit WEP key and the Extensible Authentication Protocol (EAP), which allows the use of various methods of authentication such as certificate, smartcards, one time passwords, public keys etc.

The WI-FI Protected Access (WPA)[1] is an interim solution based on earlier Work of the IEEE 802.11i group, working on security. WPA supports mixed environment (WPA/WEP). WPA uses 802.1x and EAP-TLS to authenticate users and addressed WEP vulnerabilities with the Temporal Key Integrity Protocol (TKIP), which is composed of 4 algorithms. WPA defeat forgery, prevents replay attacks and uses a re-keying mechanism, but WPA is based on RC4 with known weaknesses, and the use of AES is optional.

In addition to the WPA features, the 802.11i IEEE standard makes use of AES in CCM mode, which is a combination of counter mode and CBC-MAC mode. The same key, of at least 128 bits, serves for the AES counter mode for encryption and the AES CBC-MAC mode for authentification. The 802.11i standard supports also Quality of service.

ROAMING

The 802.11i [4] standard introduced some solutions for roaming. A first solution allows that when a station roams to a new access point, it can create a

new association and authenticate via 802.1x/EAP or with PSK (pre-shared key). Nevertheless, this solution is very slow and doesn't ensure Continued connectivity.

Another solution is that the station and the Access Point keep the Pairwise Master key (PMK), negotiated in an older association, in the cash. When the station comes back to this Access Point, it re-uses the PMK and skips the Authentication steps, starting directly the negotiation of the session keys(unicast and multicast) via key management protocol (4 way handshakes, Group key handshake) which reduces the time of re-association. The time of authentication and association with a new Access Point will stay long. But the question was how many (PMK) an AP, with limited resource, can store and how long?

The third solution enhances both roaming and fast roaming. This solution consists in a pre-authentication which means that the station negotiates authentication with new access points before leaving the current one, without association. The station stores the negotiated PMKs and will use one of them when roaming to a new access point. Once the current access point left, the station will use, to go to a next access point, the stored PMK related to this new access point and negotiated before. Then they negotiate the session keys (4 way handshake and group key Handshake protocols) and associate. The time needed for this negotiation can be shortened to allow roaming of voice and video application. The 802.11r working group has already made some success in this direction. But many Network operators think that pre-authentication involves a waste of RADIUS resources and bandwidth. Even inside the 11i group pre-authentication is criticized. The combination of all these solutions with the work of the 802.11K working group, will enable the client a better choice of access point roaming destination 802.11i standard wait his maturation.

REFERENCES

[1] WPA Wi-Fi Protected Access Specification Documentation

[2] IEEE Std 802.11b-1999 and IEEE Std 802.11b-1999-Cor1-2001, Amendment to IEEE Std 802.11-1999 Edition.

[3] IEEE P802.11i/D9.0, March 2004, Amendment to ANSI/IEEE Std 802.11-1999 Edition as amended by IEEE Std 802.11g-2003 and IEEE Std 802.11h-2003.

[4] Port-Based Network Access Control, IEEE Std 802.1X, 2001 Edition.