Security architecture in a multi-hop mesh network[1]

Omar Cheikhrouhou[α], Maryline Laurent-Maknavicius[β],Hakima Chaouchi[β]

[α]*Unité de recherche ReDCAD,Ecole Nationale d'Ingénieurs de Sfax, BP W 3038 Sfax,Tunisie.*
E-Mail: enis01amor@yahoo.fr
[β]*CNRS Samovar UMR 5157, GET/INT/LOR, 9 rue Charles Fourier, 91011 Evry, France*
E-Mail:{Maryline.Maknavicius, Hakima.Chaouchi}@int-evry.fr

IT infrastructure is one of the important pillars of any country development. Emerging wireless technologies are offering new opportunities to develop very quickly IT infrastructures in order to deploy immediately important and useful community services. One big challenge is to provide a possibility to build a network that can grow in term of coverage to offer service access such as internet access for a large number of people with different needs from the network.

In this context, we propose to analyse a wireless mesh network extended by an ad hoc network capable to grow in an ad hoc way by using ad hoc routing capabilities. The technical challenges are related first to the authentication architecture, and second to the data confidentiality. More precisely, EAP-TLS over PANA is proposed and discussed in a multi-hop mesh network, and a security analysis is provided.

Keywords: mesh network, ad-hoc network, authentication, EAP-TLS, PANA

1. Introduction

Securing access network is the first protection against fraudulent access to network services. Authentication mechanism is essential for securing the access to the network. This mechanism is as much vulnerable as the media communication is eavesdropping sensitive. In fact in a wireless network and in particular in an ad hoc network, the authentication mechanism has to be strengthen in order to ensure that only authorized users are getting access to the network services.

In the context of emerging wireless technologies, different access network architectures are possible. Infrastructure, ad hoc, mesh or hybrid wireless access networks can be used for different environments and applications. One of the very promising architectures is the extension of a wireless mesh network by an ad hoc network, this will allow a rapid coverage extension in order to offer access for different services located in the wired part of the network. This architecture is very encouraged by wireless operators that own the mesh network part. We are interested in this paper by this mixed ad hoc-mesh network named multi-hop mesh network and illustrated in Figure 1.

This architecture is composed of a set of Access Points (e.g. Wimax) interconnected as a mesh network. Ad hoc network will be used to extend the coverage of the mesh network. Mobile terminals will use the ad hoc network to get access to the internet or to any server behind the operator's mesh network. The biggest problem is the authentication of the mobile node.

[1] Article issu de O. Cheikhrouhou, M. Laurent-Maknavicius, H. Chaouchi, " Security architecture in a multi-hop mesh network ", 5ème conférence sur la Sécurité et Architectures Réseaux SAR 2006, Seignosse, Landes, France, juin 2006.

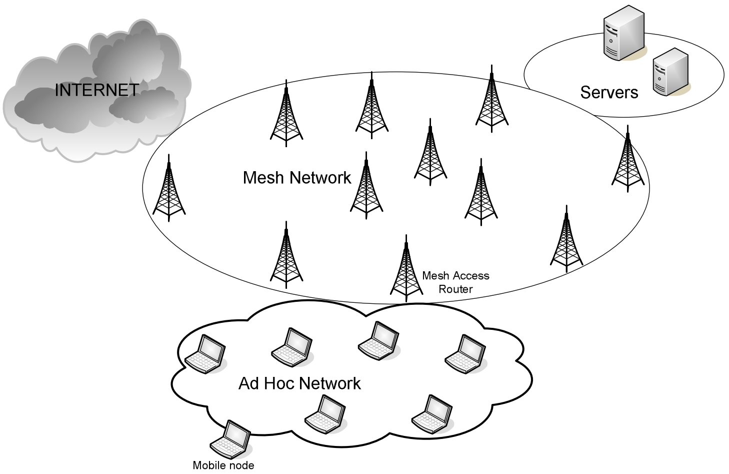


Figure 1. The multi-hop mesh network

2. Problematic

The architecture in Figure 1 considers that a mesh network under the control of an operator is extended by an ad-hoc network. Therefore this architecture inherits from the security problems met in ad-hoc networks, mesh networks and the access control enforced by operators to protect their network from intruders and illegal use.

Due to its features of open medium, and infrastructureless, ad-hoc networks are vulnerable to passive eavesdropping, message replaying, message distorsion and active impersonation that may be performed from the external perimeter of the company or the campus where the communications take place. Ad-hoc networks are also highly vulnerable to Denial of Service (DoS) attacks as any ad-hoc devices are solicited for routing purpose, and users may deny forwarding packets from one node to another for battery savings, so too poor available network resources lead to low quality connections or even disconnections. The ad-hoc routing may be disrupted by users shortening or lengthening routes by removing or injecting extra nodes on the path between two nodes.

Additionally, in mesh networks, Access Points (APs) are very sensitive points as fake APs may abuse users so their traffic is directed to these APs, and APs are then able to perform traffic eavesdropping, tampering, or DoS attacks. In that latter case, DoS attacks may result from the APs denying forwarding the traffic.

For operators to grant accesss to their network resources to legitimate users only, a very strict control should be enforced by operators. First users should be authenticated, and then authorized by the operator. The authentication should be as simple as possible for any users to authenticate easily (e.g. login / password) and robust against intruders attempting to crack the authentication method to get an illegitimate access (e.g. token ID).

Moreover, for a higher access service quality, the operators may provide users with a secure solution to protect data exchanges over the radio link against eavesdropping and tampering. Security services to be considered are data confidentiality, integrity, and origin authentication.

This article mainly addresses the security interactions between the operator and the users in a multi-hop mesh network environment. This includes mutual authentication between users and operator's access networks and data exchange protection over the radio link.

3. State of the art and related works

As far as we know, all the security problems described in section 2 are studied separately from each other. Therefore this section gives a snapshot of current research works done in ad-hoc networks security and also for operator to control users' access in mobile environments.

3.1. Ad-hoc network security

Although our work is not about securing ad-hoc network, we briefly describe the state of the art of this research area in order to provide a large view of security solutions in ad-hoc networks. These solutions might be combined with our architecture in order to minimize malicious nodes acting in the ad-hoc part.

Ad-hoc network security is addressed today in a pure ad-hoc context and covers secure routing, key establishment, authentication and certification/revocation services. Secure routing is an essential security component which permits detecting and eliminating malicious nodes disrupting the network, e.g. by advertising false routing information. Designed security protocols include ARAN [2], Ariadne [3], SAODV [4] which all consider a very constrained prerequisite that nodes are configured with appropriate pre-shared key or public/private keys to support origin authentication.

As such, a number of works were conducted towards adapting certification and revocation services to ad-hoc networks, and most of them identified the threshold cryptography [5][6] as a possible solution where k-out-of-n nodes collaboratively provide a certification service for other nodes in the network. The revocation service is operated when a minimum number of k nodes are accusing a node of misbehaving, and sometimes the action is balanced with the reputation of each accusing node.

Therefore, the threshold cryptography is adapted to ad-hoc networks to establish keys that may be used next to secure the routing, authenticate nodes and exchange encrypted data. Another solution is the ID-based cryptography [7] where the node's identifier is part of its public key, so a public key is naturally bound to the node. Another solution [8] considers both cryptography, the threshold one to initialize a private-key generation server for ID-based cryptography support.

3.2. Users' access to wireless networks

In the past few years, access to IEEE 802.11 networks strongly evolved to integrate more robust security mechanisms to support user authentication, key establishment and data protection. Today IEEE 802.1X standard [9] defines a mechanism for port-based network access control to prevent access to a LAN port until the authentication and authorization succeed. It carries EAP (Extensible Authentication Protocol) [10] messages between the user and the AP of attachment which relays EAP messages to the authentication server (usually an AAA server like RADIUS or Diameter) under EAP over RADIUS or EAP over Diameter protocol. After a successful authentication, the mobile is registered as a MAC address authorized to access to the LAN, and the AP is registered as a MAC address in the mobile. Moreover, the AP exchanges keys with the mobile, and the 4-way handshake method for key establishment is defined in the 802.11i standard [11].

Since 2001, the IETF (Internet Engineering Task Force) is defining a medium independent solution that enables EAP messages to be carried over IP within a PANA (Protocol for Carrying Authentication and Network Access) protocol [12]. This protocol is further detailed in section 4.1 as our solution is based on it, and has similar scheme than 802.1X defining a PANA client hosted into the mobile, and a PANA Agent (PAA) located into the operator's network within a router.

Once authenticated, data exchange may be protected between the PANA/802.1X client and server using the key obtained from the 4-way handshake method. A recent idea is that EAP may also serve itself to establish a common secret between the PANA client and authentication server. The secret may be communicated to the PANA Agent, so then an IKE/IPsec [13] tunnel is setup for instance between the PANA Agent and client and data exchange over the link layer is secured.

4. Proposed security architecture

A very first idea for securing access to mesh networks is to adapt IEEE 802.1X so that mobiles may be authenticated by the mesh access router (hosting an AP). However, as explained in section 3.2, authentication is done at layer 2; the association between mobiles and mesh access routers relates to MAC addresses. As such, the mobile is assumed to be directly (and physically) attached to the mesh routers in IEEE 802.1X, and no simple adaptation to multi-hop context is possible.

Therefore, PANA (Protocol for carrying Authentication for Network Access) [12] appears as a manifest solution to overcome the authentication concern as PANA is designed to enable customers to authenticate to the access network using the IP protocol. Thus PANA is independent of the underlying access technologies and is applicable to any network topology.

Moreover PANA is an EAP lower-layer and as such any EAP method is suitable for customer's authentication.

Section 4 is organized so first PANA framework is described, second the full architecture is presented with the selection of EAP-TLS over PANA and IPsec/IKE, and finally, a security analysis of the solution is discussed.

4.1. PANA framework

An access control framework using PANA defines the four following functional entities:

- **PANA Client (PaC):** The PaC resides in the mobile wishing to gain access to the network. The PaC is responsible for requesting authentication to the PANA Authentication Agent and providing the credentials to prove its identity.
- **PANA Authentication Agent (PAA):** The PAA within the access network interacts with the authentication server to determine the access control state and then communicates this state to the Enforcement Point.
- **Enforcement Point (EP):** The EP controls access to the network. It blocks data traffic of a new node until it is successfully authenticated. Only configuration flows and authentication data are permitted to go freely through the EP such as PANA, DHCP, PAA discovery, etc. The EP receives the attributes of the authorized clients from the PAA either through an API (if both EP and PAA are co-located on an Access Router AR) or the SNMP protocol for instance (if they are remotely located).
- **Authentication server (AS):** The AS is asked by the PAA to verify the credentials of a node requiring access to the network. The AS and PAA can be co-located in the same node so a simple API is sufficient for their communications; otherwise communications are supported by an AAA protocol like Diameter or RADIUS.

4.2. Technical description

As depicted in Figure 2, when a new mobile joins the network, first it gets an IP address called pre-PANA address from the local DHCP server, and then it initiates PANA protocol to discover the PAA (located on the AR - Access Router) and to authenticate itself. Note that the mesh router and intermediate nodes are configured to permit some IP flows including DHCP, neighbour discovery, and PANA for unauthenticated users. Once successfully authenticated, the client initiates the IKE protocol with the mesh router in order to establish a security association. Then the IPsec tunnel ensures data protection over the radio link and an inherent data access control by the mesh router.

For discovering PAA, the PaC broadcasts PANA-PAA-Discover message. By default the first PAA responding with the PANA-Start-Request message is selected by the PaC, and the PaC replies with the PANA-Start-Answer message in order to enter to the authentication phase. Mechanisms to mitigate DoS attacks happening during the discovery phases are described in section 4.3.

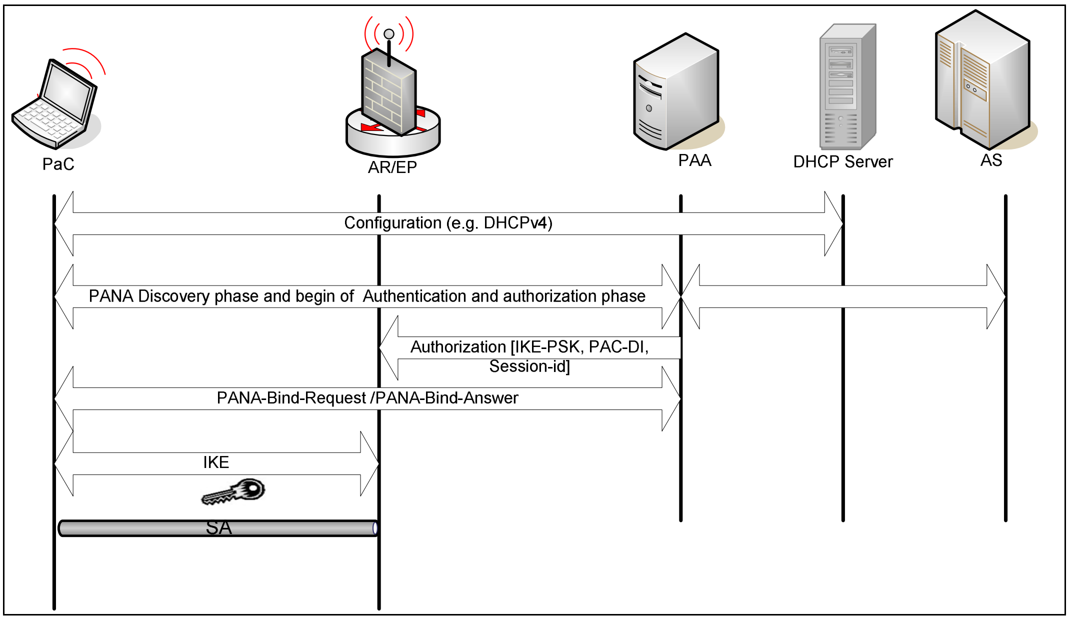
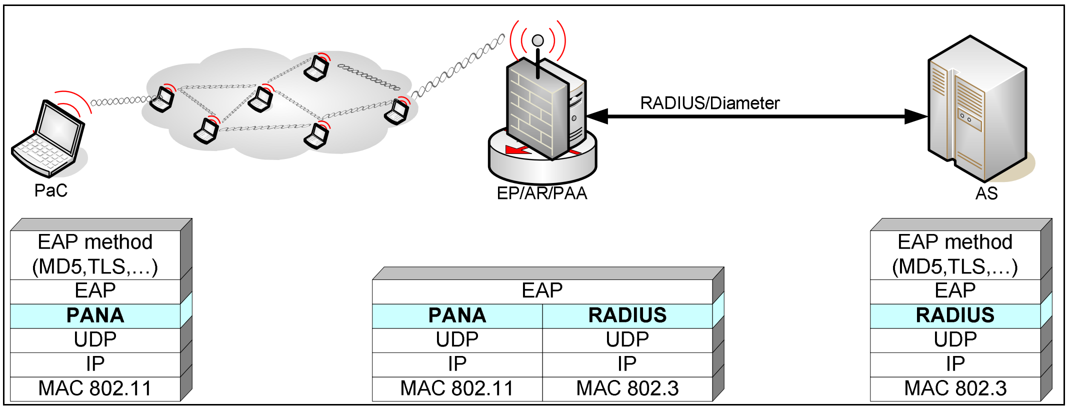

PaC
AR/EP
PAA
DHCP Server
AS
Configuration (e.g. DHCPv4)
PANA Discovery phase and begin of Authentication and authorization phase
Authorization [IKE-PSK, PAC-DI, Session-id]
PANA-Bind-Request /PANA-Bind-Answer
IKE
SA

Figure 2. Chronological phases (AR/EP and PAA separated)



PaC
EAP method (MD5,TLS,…)
EAP
PANA
UDP
IP
MAC 802.11

EP/AR/PAA	
EAP	
PANA	**RADIUS**
UDP	UDP
IP	IP
MAC 802.11	MAC 802.3

AS
EAP method (MD5,TLS,…)
EAP
RADIUS
UDP
IP
MAC 802.3

Figure 3. Encapsulation of EAP packets during PANA authentication (AR/EP and PAA co-located)

During the authentication and authorization phases, PANA supports EAP messages exchanged between the PaC and the PAA, and the PAA relays EAP messages to the AS for instance using EAP over RADIUS (cf. Figure 3). The choice of the EAP method depends on the credentials used by the PaC and the AS. For operator's management efficiency, the EAP-MD5 method based on a login / password would be a good choice, but it suffers from known vulnerabilities (dictionary and brute-force attacks), and does not support mutual authentication.

Therefore, we selected EAP-TLS [14] which offer the following advantages:

- It is proved to be secure and robust against attacks (under some conditions like mutual authentication selection);

- Mutual authentication is supported based on public key certificates and detects rogue mesh access routers;
- Derivation of keying material is possible to protect network access by providing an IKE pre-shared key (IKE-PSK) to PaC and EP. More precisely, after EAP-TLS authentication, PaC and AS share a common key called MSK for Master Session Key; thanks to MSK, an AAA-Key may be derived on both PaC and AS; AAA-Key is securely communicated by AS to PAA and serves to derive two other keys, one (PANA-MAC-Key) to protect PANA messages between PaC and PAA, and the IKE-PSK which is configured by PAA into EP (cf. Figure 2). In case of moves, a new IKE-PSK is put in place between PaC and the new EP.

Upon exchanging messages PANA-Bind-Request and PANA-Bind-Answer, the authentication phase is completed, and thanks to their IKE pre-shared key, PaC and EP are able to initiate IKE exchanges [13] to mount an IPsec tunnel.

PANA/EAP-TLS authentication procedure

The sequence of messages exchanged during a successful authentication process is shown in Figure 3. The mesh access router sends an EAP-Request/Identity message encapsulated in PANA-Auth-Request message to the PaC. This message starts the process of authentication and then the authentication proceeds as follows:

1. Upon receiving the EAP-Request/Identity message, the PaC sent back his identity (e.g. username, hostname …) in an EAP-Response/Identity message encapsulated into a PANA-Auth-Answer message.
2. Once having received the PaC's identity, the mesh router forwards this message to the AS. From this point, the mesh router acts as a pass-through (Figure 3) between PaC and AS.
3. The AS then sends an EAP-TLS/Start packet to start the EAP-TLS conversation with the PaC.
4. The PaC responds by sending a TLS client_hello handshake message which contains the TLS version number, a TLS session Id, a random number, and a set of supported cipher suites (encryption algorithms).
5. The AS then sends an EAP-Request packet containing a TLS server_hello handshake message followed by a TLS certificate, server_key_exchange, certificate_request and server_hello_done. The server_hello handshake message contains the AS's TLS version number, another random number, a sessionId, and the selected cipher suite.
6. The PaC sends an EAP-Response packet containing his certificate, client_key_exchange which determines with the server_key_exchange the session key (Master Session Key), certificate_verify which is a digital signature of the authentication response.
7. Upon receiving this EAP-Response packet, the AS proceeds by verifying the PaC's certificate and the digital signature. If the test succeeds, it sends an EAP-Request packet containing TLS change_cipher_spec and finished handshake messages which includes a keyed hash over the message. By verifying the keyed hash, the PaC can authenticate the AS (EAP server).

If the authentication is successful, the PaC and AS exchange EAP-Response and EAP-Success messages. Note that PANA messages PANA-Bind-Request and PANA-Bind-Answer are protected with a keyed hash (MAC – Message Authentication Code) generated with the PANA-MAC-Key shared between PAA and PaC.

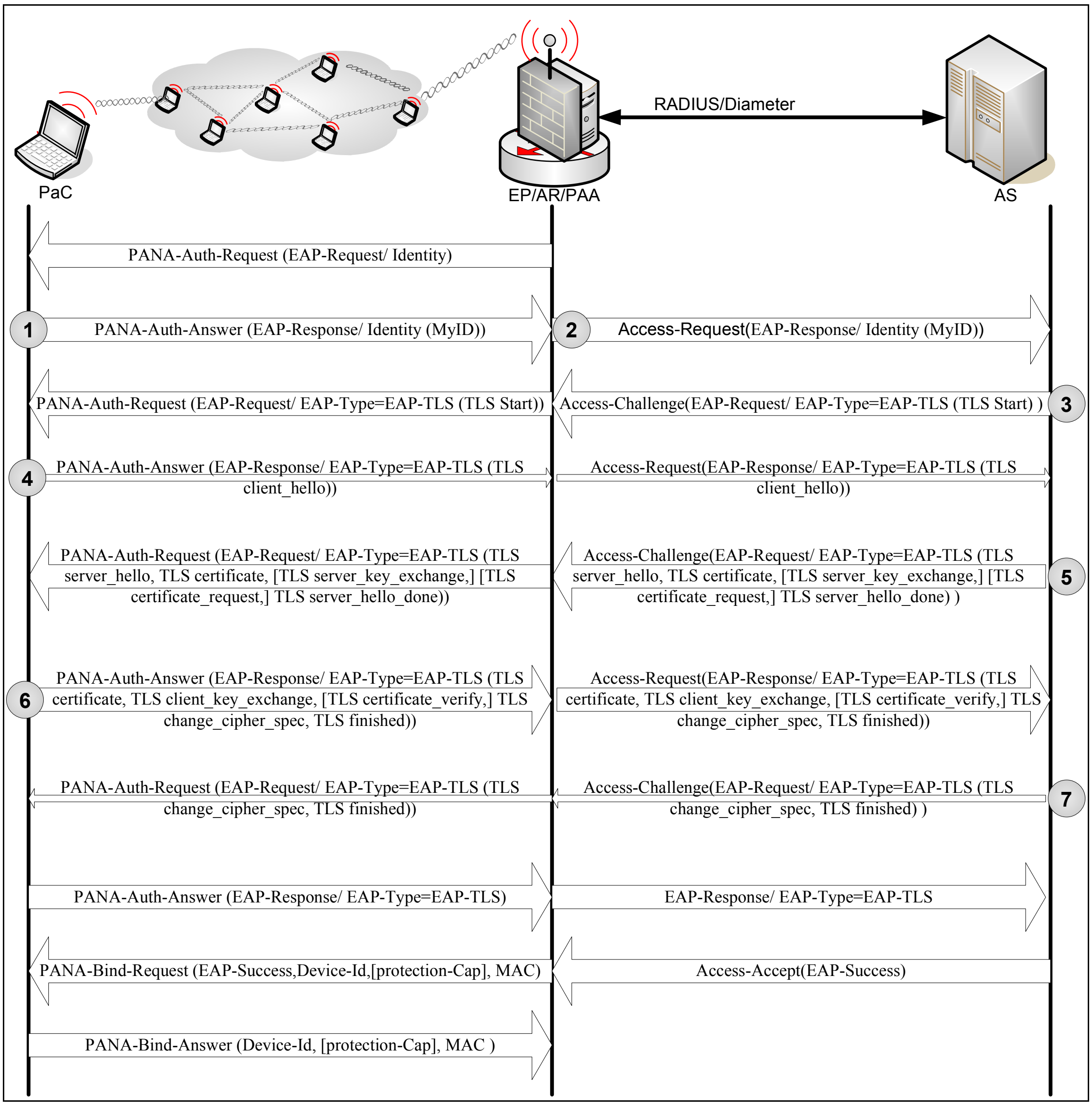

RADIUS/Diameter
PaC
EP/AR/PAA
AS
PANA-Auth-Request (EAP-Request/ Identity)
1
PANA-Auth-Answer (EAP-Response/ Identity (MyID))
2
Access-Request(EAP-Response/ Identity (MyID))
PANA-Auth-Request (EAP-Request/ EAP-Type=EAP-TLS (TLS Start))
Access-Challenge(EAP-Request/ EAP-Type=EAP-TLS (TLS Start))
3
4
PANA-Auth-Answer (EAP-Response/ EAP-Type=EAP-TLS (TLS client_hello))
Access-Request(EAP-Response/ EAP-Type=EAP-TLS (TLS client_hello))
PANA-Auth-Request (EAP-Request/ EAP-Type=EAP-TLS (TLS server_hello, TLS certificate, [TLS server_key_exchange,] [TLS certificate_request,] TLS server_hello_done))
Access-Challenge(EAP-Request/ EAP-Type=EAP-TLS (TLS server_hello, TLS certificate, [TLS server_key_exchange,] [TLS certificate_request,] TLS server_hello_done))
5
6
PANA-Auth-Answer (EAP-Response/ EAP-Type=EAP-TLS (TLS certificate, TLS client_key_exchange, [TLS certificate_verify,] TLS change_cipher_spec, TLS finished))
Access-Request(EAP-Response/ EAP-Type=EAP-TLS (TLS certificate, TLS client_key_exchange, [TLS certificate_verify,] TLS change_cipher_spec, TLS finished))
PANA-Auth-Request (EAP-Request/ EAP-Type=EAP-TLS (TLS change_cipher_spec, TLS finished))
Access-Challenge(EAP-Request/ EAP-Type=EAP-TLS (TLS change_cipher_spec, TLS finished))
7
PANA-Auth-Answer (EAP-Response/ EAP-Type=EAP-TLS)
EAP-Response/ EAP-Type=EAP-TLS
PANA-Bind-Request (EAP-Success,Device-Id,[protection-Cap], MAC)
Access-Accept(EAP-Success)
PANA-Bind-Answer (Device-Id, [protection-Cap], MAC)

Figure 4. Authentication procedure by EAP-TLS over PANA

IPsec/IKE protection

Once the client is successfully authenticated with PANA, the mesh access router then limits access to network only to authorized clients. With the multi-hop environment, the access control needs to operate at the netork layer or upper layers, and as such the IPsec protocol suite is suitable in the multi-hop mesh network. First, it supports strong access control with the possibility to authenticate packets' origin. Second, it provides data encryption when using ESP (Encapsulating Security Payload) [14], and as such, helps mitigating eavesdropping over the radio link.

In order to setup an IPsec security association, the mobile and the mesh access router need to initiate IKE exchanges and first authenticate to each other. To take benefit of the first authentication done by PAA, the PAA is required to simultaneously provide the mesh router with an access authorization for that mobile, and the IKE-PSK key.

4.3. Security analysis of the solution

The obtained security solution verifies the security requirements defined in [12] to support authentication. Hereafter, we present some of the potential attacks and give recommendations for mitigation.

Protection against replay attacks

PANA messages carry sequence numbers, which are monotonically incremented by 1 with every new request message. These numbers are randomly initialized at the beginning of the session, and verified against expected numbers upon receipt. A message whose sequence number is different than the expected one is silently discarded.

In addition to accomplishing orderly delivery of EAP messages and duplicate elimination, this scheme also helps preventing an adversary from spoofing messages to disturb ongoing PANA and EAP sessions unless it can also eavesdrop to synchronize on the expected sequence number.

Protection against PaC DoS attacks

The authentication results (EAP success or failure) transmitted by the PAA to the PaC at the end of the authentication process is protected by a MAC. This prevents attackers from launching DoS attacks against the PaC by sending a spoofed EAP failure message.

A spoofed PANA-Termination-Request message may be sent by malicious nodes, however MAC protection prevents this type of malicious attack.

Providing message integrity

The PANA security association created at the end of a successful authentication provides message integrity and particularly protects the PaC's identifier and therefore prevents the service theft attack described in [12].

Spoofing PAA message

As there is no trust relationship between PaC and PAA during the discovery phase, an attacker can spoof PAA messages like the PANA-Start-Request one.

If this message contains information (such as supported authentication methods) other than the discovery of the PAA itself, a malicious node can launch a binding down attack as it can send a spoofed advertisement with capabilities that indicate authentication methods less secure than those supported by the real PAA, thereby fooling the PaC into negotiating an authentication method less secure than would otherwise be available.

For this reason, it is recommended to negotiate parameters like protection capability and encryption algorithm after the establishment of PANA security association for example in PANA-Bind-Request message.

PAA DoS attack

As discussed above an attacker can overload the PAA with PANA-PAA-Discover messages in order to make the PAA out of service. One solution to mitigate this misbehaviour is to add a cookie to the PANA-Start-Request message. The cookie is generally computed based on the PaC's device identity such as an IP address to guarantee a PaC is available at the claimed address as it is able to return the same cookie in its PANA-Start-Answer message. Thus the cookie mechanism proves that the claimed IP address is not a randomly generated IP address and hence the PAA can avoid a per-PaC state creation.

DHCP DoS attack

PANA assumes that the PaC acquires an IP address before running PANA. When the IP addresses are assigned before the client authenticates, DoS attacks are possible in which unauthenticated malicious nodes can deplete the IP address space by acquiring multiple IP addresses.

Other possible attacks

As stated in section 2, ad-hoc and mesh networks are vulnerable to passive eavesdropping, message replaying, message distorsion, easy man-in-the-middle, active impersonation, and DoS. Such attacks are easily achievable in ad-hoc networks due to simple nodes relaying traffic, and any nodes joining the group. In particular, eavesdropping is made easier since packets are visiting naturally all the nodes on the route selected by the ad-hoc routing.

IP spoofing is also made easier with the ad-hoc network, especially when a node leaves the ad-hoc group, another might use its IP address, however a man-in-the-middle is necessary to intercept and block PANA-Termination-Request message so that the session will remain alive. However, as PANA architecture uses periodic reauthentication, the IP spoofing is effective only for a small duration.

Apart from the worst DoS (packets voluntarily not relayed, battery down), some cryptographic technics (IPsec) can be used to prevent eavesdropping, message distorsion, and active impersonation.

The mesh networks might suffer also from similar attacks as the ad-hoc networks, but the worst DoS is not possible since mesh routers are under the administration of the network operator. Therefore, mesh routers interconnection should be secured using access control, and cryptographic technics.

5. Future works

The proposed architecture combines PANA with EAP-TLS in a multi-hop mesh network. EAP-TLS provides mutual authentication and strong robustness against attacks, but the use of asymmetric cryptography has the disadvantages of heavy treatment (incompatible with light ad-hoc networks) and the need of establishing and managing a PKI (Public Key Infrastructure). An alternative would be EAP-MD5 which is simpler, however it is vulnerable to eavesdropping attacks, as we pointed earlier, worsen by the ad-hoc environment. For this purpose, we are working on a new scheme that will ideally combine the simplicity of EAP-MD5 and the robustness of EAP-TLS.

Compared to IEEE 802.1X, PANA requires allocation of an IP address before authenticating, and this exposes to IP address starvation in IPv4. This opens new research direction for adapting IEEE 802.1X to multi-hop mesh networks.

6. Conclusions

Wireless networks are promising a large, easy and rapid IT services deployment. Different architectures are possible depending on the applications, and the environment such as infrastructure-based, ad-hoc, or mesh networks. In this context of emerging wireless technologies, security is vital for a successful deployment of services over these new networks. In this paper, we address access network security including access control, and data protection in a multi-hop mesh network.

IEEE 802.1X standard could obviously be extended to support authentication in multi-hop mesh networks, but this is not that easy in practice because it implies modifying the standard. A combination of EAP-TLS over PANA and IPsec has been proposed, described, and analyzed.This architecture is a promising one since it is independent of the wireless media, and this is very appropriate for the emerging heterogeneous 4G wireless networks. However, contrary to 802.1X, PANA is relying on the availability of IP addresses to avoid the rejection of new coming mobiles not authenticated yet due to the lack of IP addresses. This problem can hopefully be solved in IPv4 by allocating temporary private addresses, and in IPv6 thanks to the large space address.

Acknowledgements

Our sincere acknowledgements go to GET financing EcoMesh project, Mr Maher Ben Jemaa (ENIS, Tunisie), Julien Bournelle and Chakib Bekara (GET/INT, France) for their time and support.

Acronyms

AR – Access Router
AS - Authentication Server
EP – Enforcement Point
IKE – Internet Key Exchange
PAA - PANA Agent
PaC – PANA Client

References

[1] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E. M.Belding-Royer: “A secure routing protocol for Ad Hoc networks”, Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[2] Y. C. Hu, A. Perrig, D. B. Johnson: “Ariadne: A secure on-demand routing protocol for Ad Hoc networks”, Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

[3] M. Guerrero Zapata: “Secure Ad hoc On-Demand Distance Vector Routing,”ACM Mobile Computing and Communications Review (MC2R), vol. 6, no. 3, pp. 106–107, July 2002

[4] H. Luo, P. Zerfos, J. Kong, S. Lu, L. Zhang: “Self-securing Ad Hoc Wireless Networks”, Seventh IEEE Symposium on Computers and Communications (ISCC’02), 2002.

[5] S. YI, R. Kravets: “MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks”. 2nd Annual PKI Research Workshop. April 2003, Gaithersburg MD, USA.

[6] D. Boneh, M. Franklin: “Identity-Based Encryption from the Weil Pairing”. In J. Killian, editor, Advances in Cryptology, CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213-229. Springer Verlag, August 2001.

[7] A. Khalili, J. Katz, W.A. Arbaugh, “Towards secure key distribution in truly ad-hoc networks”, IEEE Workshop on Security and Assurance in Ad-hoc Networks, 2003.

[8] IEEE Standard 802.1X-2004: “Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control”, December 2004.

[9] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz: "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[10] IEEE Standard 802.11i-2004: “Standard for Information technology - Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements”, July 2004.

[11] M. Parthasarathy: "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", RFC 4016, March 2005.

[12] C. Kaufman: “Internet Key Exchange (IKEv2) Protocol”, draft-ietf-ipsec-ikev2-17, September 2004.

[13] B. Aboba, D. Simon: “PPP EAP TLS Authentication Protocol”, RFC 2716, October 1999.

[14] S. Kent, R. Atkinson: “IP Encapsulating Security Payload (ESP)”, RFC 2406, November 1998.