Int. J. Communications, Network and System Sciences, 2014, 7, 175-180
Published Online June 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.76019

Scientific Research

Creation of Virtual Wi-Fi Access Point and Secured Wi-Fi Pairing, through NFC

Oussama Stiti[1,2], Othmen Braham[2], Guy Pujolle[1]

[1]Sorbonne Universities, UPMC Univ. Paris 06, UMR 7606, Paris, France
[2]VirtuOR, Paris, France
Email: oussama.stiti@virtuor.fr, othmen.braham@virtuor.fr, guy.pujolle@lip6.fr

Received 16 April 2014; revised 16 May 2014; accepted 30 May 2014

Abstract

The growing ubiquity of Wi-Fi networks combined with the integration of low-cost Wi-Fi chipsets in all devices makes Wi-Fi as the wireless technology the most used for accessing to internet [1]. This means that the development of a Wi-Fi strategy has become an imperative for almost all operators worldwide. In this context, APs (Access Points) have to become as secure as cellular networks. Furthermore, authentication process between a mobile device and an access point has to be automated, without user constraining configuration. For reaching this purpose, client must have different credentials depending on authentication method. Our goal is to create an architecture that is both ergonomic and flexible in order to meet the need for connection and client mobility. We use NFC technology as a radio channel for starting communication with the network. The communication initiation will instantiate a virtual Wi-Fi AP and distribute all policies and access certificates for an authentication based on EAP-TLS (it could be extended to any EAP method for 802.1X standard). The end result of our new topology is to allow access to services through a virtual Wi-Fi AP with an enterprise-grade in a public hotspot.

Keywords

Wi-Fi, NFC, Virtual Access Point, Pairing, Automation

1. Introduction

Data mobile traffic is climbing at dizzying speeds. The number of tablets and smart phones sales has grown up rapidly and is requiring ubiquitous internet access. Customers need to be connected everywhere, anytime. Different actors involved in Cloud Computing are rising the mobile traffic significantly [2] [3] by developing services requiring very high bandwidth and availability without thinking of how users will access to these services.

How to cite this paper: Stiti, O., Braham, O. and Pujolle, G. (2014) Creation of Virtual Wi-Fi Access Point and Secured Wi-Fi Pairing, through NFC. *Int. J. Communications, Network and System Sciences*, **7**, 175-180.
http://dx.doi.org/10.4236/ijcns.2014.76019

MNOs (Mobile Network Operators) have difficulty to keep up the pace, and end up with saturated cellular networks [4].

Mobile data offloading traffic over Wi-Fi emerged as a good solution to decongest cellular networks. The most important aspect is to find a way connecting seamlessly without human configuration to a public Wi-Fi access point and maintaining a high level of security encountered in cellular networks. In traditional Wi-Fi networks, users must search for and choose a network, request the connection to the access point (AP) each time, and in many cases, must re-enter their authentication credentials. The challenging issue is to enable a seamless connection between hotspot networks and mobile devices, and to deliver the highest WPA2-enterprise security.

One of the most secured authentication methods in wireless networks is EAP-TLS [5], which use two certificates (one on server-side and the other on client-side) for the creation of a secure tunnel which then allow identification.

To initiate at the beginning a seamless connection between hotspot and mobile devices, we need both client and authentication server to have certificates for two-way authentication. Certificates provisioning for devices using Wi-Fi is still an open issue.

We propose to distribute certificates with NFC terminals. The client with its mobile device has to touch or bring into proximity of the NFC terminal. Client sends personal informations to NFC terminal that forward it to the RADIUS server in the operator network for generating certificates. RADIUS server sends back: client certificate, certificate authority, PMK (Pairwise Master Key) to the client via the NFC terminal. Once client credentials sent by operator network, the NFC terminal forwards it to the client, and on the same time, send order to the Wi-Fi AP to create a new virtual AP fitting with the credentials. In this way, client can connect on the virtual Wi-Fi AP provided in the area by its own operator.

2. Virtual Wi-Fi Access Point

A virtual Wi-Fi AP is a virtual machine running on a physical AP and fitted with virtual interfaces allowing it to communicate with the physical interfaces on purpose to broadcast its SSID for allowing wireless devices to communicate with it. Virtual Wi-Fi APs that we have developed allow complete isolation between virtual instances: each one is operating independently and running on the same Wi-Fi card.

Resources pooling of the physical infrastructure of Wi-Fi hotspots among different service providers and MNOs would allow a better service availability, network architecture flexibility, as well as a wider coverage area [6].

Virtual access points extend services of different virtual networks to cover users around a physical Wi-Fi access. The objective of this method is to create and study the advantages of a virtualized access point. Pooling resources in a Wi-Fi access point allows to introduce more flexibility, isolation and security, and extend network coverage. The idea is to optimize the use of physical resources used by a single access point. Thus, a physical machine used as the access point is shared between several virtual access points. We will describe four examples of use cases highlighting the benefits of this solution in the following.

2.1. Resources Pooling of a Physical Wi-Fi AP between Several Operators

In the first use case, this type of access point can be used by several operators at the same time in areas where installing multiple physical access points is not acceptable, as airports. Furthermore, multiple physical access points may be uneconomic in cases where the number of customers varies significantly depending on time, as in public parks, libraries, etc. The virtual access points seek to optimize physical resources that are generally not used optimally and to share the costs of deployment. Thereafter, an operator can install a Wi-Fi network in a cell covered by a virtualized access, it only has to instantiate virtual access based on physical resources.

2.2. Several Virtual Wi-Fi AP for Dedicated Networks

In the second use case, this type of access points can be used by a single operator to deploy multiple networks dedicated to flows intrinsically different. These networks must be installed on the same physical access point with total isolation between the different flows. This is the case for example of a company that wants to create a wireless network for VoIP, a second network for video streaming, a third network to implement a highly secured stack protocol and a fourth open network for web browsing. Changing the configuration of virtual access points according to the type of flow is very advantageous in terms of performance. Indeed, some protocol stacks and

routing algorithms are better suited to network services than others.

2.3. Migration of Virtual Wi-Fi AP

In a third use case, this type of access points can be useful for security purposes. In the case of an attack, a virtual access point can be migrated to another physical machine and the access point attacked destroyed without interruption of service. The migration of an access point is very simple because it requires to instantiate another virtual access point with the same configuration files than the attacked one, or perform a conventional migration with tools provided by virtualization.

2.4. Dynamicity of Virtual Wi-Fi AP Enabling Innovation and Research

In a fourth case, the use of this type of access point as a test platform can support innovation and research for Wi-Fi networks. Indeed, the implementation of new protocols and performance studies of different types of flows are possible. The created virtual networks are logically isolated by virtualization and must share bandwidth available depending on priority and scheduling. In a more general way, dynamic cohabitation of Wi-Fi networks allowed with virtualization appears to be a promising solution to decouple physical infrastructure and services.

3. Distribution of Client Policies and Certificates through NFC

We have seen some of the numerous benefits of virtual Wi-Fi AP. The main idea of our approach is to find a mechanism that induces the creation of a virtual Wi-Fi AP and at the same time gives to the client all policies to connect to his AP without human configuration. As mentioned above, the virtual created AP has to include a high security level by implementing WPA2-Entreprise (that use 802.1X standard and 802.11i encryption). For 802.1X authentication method we chose to focus on EAP-TLS that is considered one of the most secure EAP standards available because of digital certificates.

For a secure network, the communicating parties must obviously trust each other. A method for building trust goes through a trusted third party, for example, a PKI (Public Key Infrastructure) certification authority (CA). In practice, with EAP-TLS we need to configure certificates for the server and the client, to ensure mutual authentication. These certificates must be signed by a certificate authority (AAA server).

The developed solution complies with the 802.1X protocol, in order to allow physical access to the network only after authentication. This tripartite architecture involves the device to authenticate (supplicant or client), the access point and the AAA server. As it is not authenticated, the client cannot access to the network, only authentication exchanges process are relayed to the authentication server by the access point. Once the client is authenticated, he is authorized to access to his service through the AP. The standard EAP-TLS uses two certificates for the creation of a secure tunnel which then allow identification. This means that even if the password is discovered, it will be of no use without the client certificate.

3.1. Certificate Distribution for EAP-TLS

Like other protocols (SMTP-TLS, IMAP-TLS, HTTPS, etc.) EAP relies on TLS to provide secure authentication. The use of certificates has advantages and disadvantages. They are often considered more secure than passwords, however management operations that they cause can be tedious (creation, deletion, certificate revocation list etc.) and a Public Key Infrastructure (PKI) is required. The distribution of certificates to clients is a constraint that should not be neglected.

We have to make sure the certificate is securely sent. If a non-secure protocol such as e-mail, HTTP, or FTP is used to send the file over the Internet, the certificate's security can be compromised. The secure way to distribute a certificate at the present time requires HTTPS, SSH or hardware (USB flash drive, external hard drive, etc.). There is no particular technique to distribute a certificate. More than ever, this issue will be a critical point for deploying Wi-Fi APs using certificates. Operators, Internet Service Providers (ISPs) and all actors providing Wi-Fi access will face the massive task of distributing credentials to their subscribers.

3.2. Advantage of NFC for Certificate Provisioning

When using NFC, we can distribute certificates to the client and also install it in the secure element inside the

mobile device. Acquisition of access rights is done in a single phase, no need to download and then install the certificates manually.

Possible transfer rate with NFC technology is 424 Kb/s operating at 13.56MHz with a range of 10 cm [7]. However, the ease of operation fits perfectly with the philosophy of smartphones mobility. The goal is not to compete with Bluetooth or Wi-Fi, but to give a simple functionality to smartphones for accessing to their services with required credentials.

3.3. NFC Security Issues

The very short range of NFC already provides an important security aspect. But NFC technology is not immunized against attacks such as eavesdropping, corruption and data handling and interceptions [8]. Encryption is not mandatory in the NFC standard (it was intentional to ensure that the technology was compatible with previous implementations of RFID), but AES standard encryption could be used. Although attacks on NFC are rare and require sophisticated equipment, but they exist. Such a security aspect must be treated with the greatest attention for distributing certificates, without which the whole chain security (WPA2-Enterprise) established may be corrupted upstream. An exchange of data between a mobile device and an NFC terminal to initiate communication based on EAP-TLS with a Wi-Fi AP, should be secured by TLS.

LLCPS is an IETF's TLS working group draft that describes implementation of TLS protocol over LLCP layer on NFC. LLCPS will provide an enhanced security for the NFC P2P communication. LLCPS will provide to NFC an appropriate security level for exchanging personal data and network access certificates [9] [10].

3.4. Topology and Mechanism

As shown in **Figure 1**, a customer device wanting access for the first time to virtual Wi-Fi access point provided by its operator must obtain a client certificate for authenticating. NFC terminal belonging to the operator, can produce the certificate automatically without any manipulation of the customer. Steps in Fig. are as follows:

1: Device sends customer informations e.g. IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Station Integrated Services Digital Network Number), or any other information to uniquely identify the customer to NFC terminal through LLCPS.

2: NFC terminal sends user appliance for a certificate at a registration authority (RA).

3: Depending on client identity confirmed by RA, certification authority (CA) issues the certificates and sends it back to NFC terminal.

4: NFC terminal sends to mobile device all the necessary credentials with LLCPS.

4': NFC terminal sends informations to physical AP about the virtual AP fitting with client credentials (SSID, passwords, EAP method…).

5: The virtual Wi-Fi AP is created, and begins to send beacon frames to announce its presence.

3.5. Connecting to Virtual AP Based on EAP-TLS Authentication

In **Figure 2** the client has certificates, and Wi-Fi network access policy, he could access to its services through the virtual AP.

1: Client get associated with AP but is not permitted to send any data at this point and sends an authentication request.

2: AP send client authentication request with its certificate (EAP-TLS) to AAA server to check if the user is a legitimate one. The server presents its certificate to the client as well for a two-way authentication.

3: Both of server and client were authenticated and a PMK (Pairwise Master Key) is shared between client and AP.

4: A new encryption key is dynamically derived from the master secret during a four-way handshake: PTK (Pairwise Transient Key).

5: Data exchanges are now encrypted between mobile device and AP.

6: Virtual Wi-Fi AP forwards frames to the mobile device.

4. Conclusions

Wi-Fi AP virtualization can help make the Internet more scalable and support new innovations. More than ever

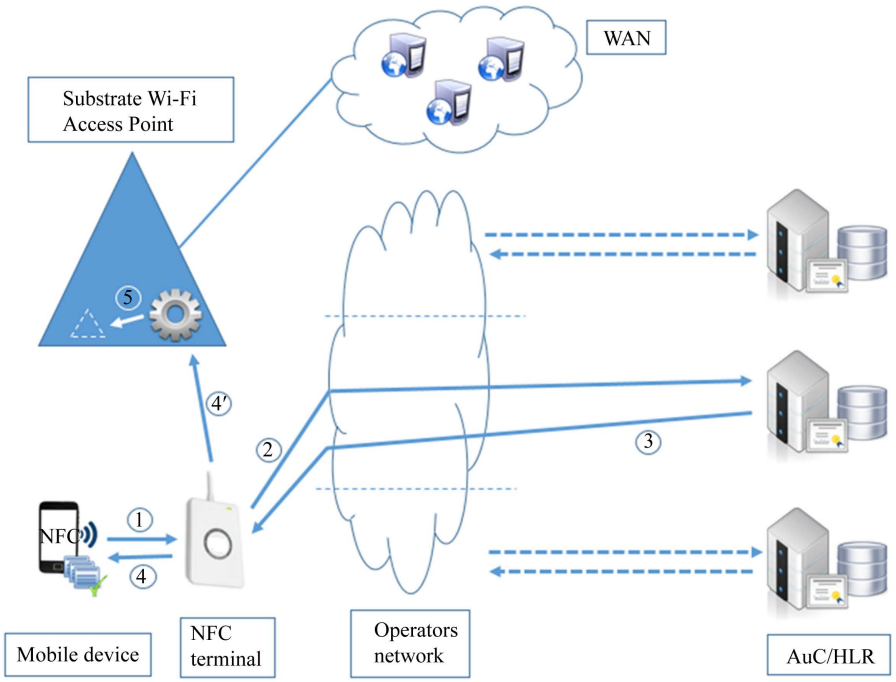

Figure 1. Certificates distribution and virtual Wi-Fi AP creation.

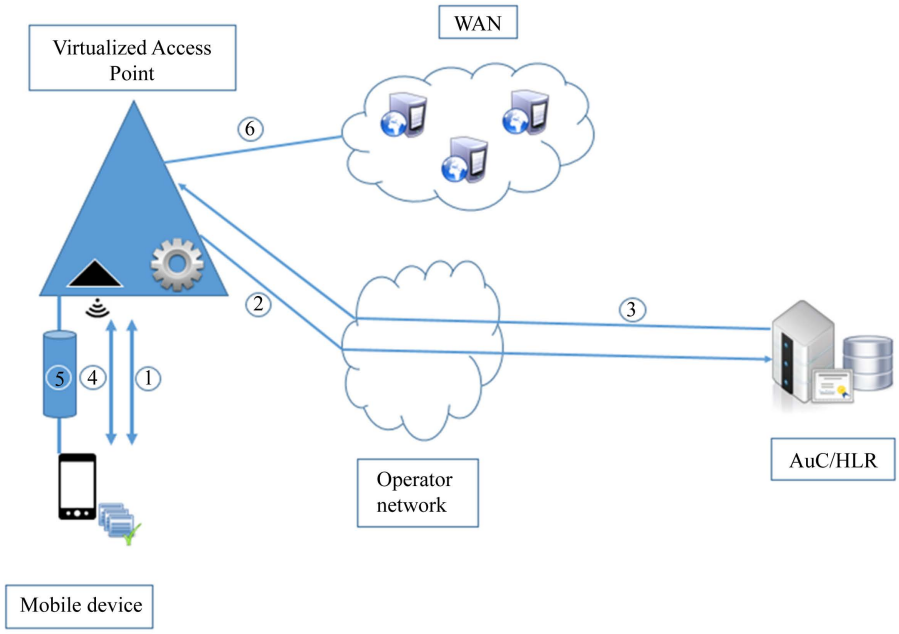

Figure 2. Client accessing to internet with EAP-TLS authentication through the virtual Wi-Fi AP.

wireless access is designing network architectures. With the increased mobility of clients, access becomes a service. The access point must follow the customer everywhere. Advances in virtualization technologies have created new opportunity for network operators to take advantage of network resources. In our approach we try to adapt virtualization concepts to satisfy many of today's network telecommunication challenges. The major problem is the limited bandwidth allowed with Wi-Fi, which fades more and more thanks to the high speeds of new wireless standards. More than ever, the need to connect seamlessly with a high level of security became a

hot topic. The standard Hotspot 2.0 under development by the Wi-Fi Alliance, is trying to respond to this problem, but will be faced to an incompatibility of old mobile devices.

NFC technology turns out to be an effective way to distribute certificates to clients, and allow any legitimate customer to access to a Wi-Fi AP created on demand. Other short range technologies could be used as a radio channel for starting communication with the network for creating a virtual Wi-Fi AP, and should be discussed in a future work.

Acknowledgements

We would like to acknowledge VirtuOR to help us to develop our architecture and validate it on real virtualization platform. We are studying an optimization of these new architectures and techniques. Experimentations are still ongoing.

References

[1] Wireless Broadband Alliance, Global Developments in Public Wi-Fi, WBA Report Industry 2011. http://www.wballiance.com/wba/wpcontent/uploads/downloads/2012/07/16_WBA-Industry-Report-2011-_Global-Developments-in-Public-Wi-Fi-1.00.pdf

[2] Stiti, O. and Braham, O. (2014) 802.1X-EAP-TLS Certificates Provisioning with NFC Terminals for Accessing to Wi-Fi CERTIFIED Passpoint. *MobiSecNFC* 2014: 1*st Workshop of Mobile Applications, Secure Elements and Near Field Communication*, Gainesville Florida, 21-22 February 2014,

[3] Cisco (2014) Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

[4] Cisco (2010) Evolution of the Mobile Network. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-624446.pdf

[5] IETF RFC-5216 (2008) The EAP TLS Authentication Protocol.

[6] Braham, O. and Pujolle, G. (2012) Virtual Access Point to the Cloud. *Cloud Networking* (*CLOUDNET*). 2012 *IEEE* 1*st International Conference on Cloud Networking*, Paris, 28-30 November 2012, 206-208.

[7] NFC Forum Specifications. http://www.nfc-forum.org/specs/

[8] Security Risks of Near Field Communication. http://www.nearfieldcommunication.org/nfc-security-risks.html

[9] LLCPS, draft-urien-tls-llcp-00.txt, IETF Draft, 2012.

[10] Urien, P. (2013) LLCPS, A New Security Framework Based on TLS for NFC P2P Applications in the Internet of Things. *Consumer Communications and Networking Conference* (*CCNC*), 2013 *IEEE*, Las Vegas, 11-14 January 2013, 845-846.