ENHANCING PUBLIC WIFI SECURITY

A Technical Paper prepared for SCTE/ISBE by

Ivan Ong
Principal Engineer
Comcast
1701 John F Kennedy Blvd
Philadelphia, PA 19103
215-286-2493
Ivan_Ong@comcast.com

Table of Contents

1. Abstract

Approximately 15 million Xfinity WiFi public hotspots are available today domestically, the total tonnage or usage for the month of Jan 2017 was 174 Petabytes and there were 1.79 billion sessions. More than 7 million apps were downloaded on the network in that month. Ensuring the security of the users on public hotspots will minimize threats and provide an overall improved user experience. This paper will explore EAP-TLS mechanism and its implementation approach on public WiFi.

2. Overview

At a minimum, a typical hotspot broadcasts an open and secure SSID today, with EAP-TTLS and EAP-GTC mechanisms to ensure service compatibility primarily for Android and iOS systems. A user has the option of associating their mobile client to either SSID, however, a profile is generated for secure SSID association as it offers some advantages over a non-secure SSID. A mobile client associating to a secure SSID today will have the ability to generate and download a profile that will ensure connectivity to a valid trusted service provider hotspot due to the server authentication that occurs in the EAP inner mechanism that is employed.

The majority of Android mobile clients are accommodated by the EAP-TTLS method which performs a two-phase authentication: the outer authentication, from server to client, mandates the client to authenticate the server certificate. Once validated, a TLS tunnel is established; the inner authentication, from client to server, will then exchange encrypted information typically based on a simple non-TLS authentication method. In the case of Xfinity WiFi, username and password credentials are exchanged.

The majority of iOS mobile clients are accommodated by the EAP-GTC method, a basic EAP standard that utilizes token management for authentication. This method was employed due to the fact that iOS requires an Apple based application to generate a profile; without relying on the user to download an application that may seem intrusive to the inherent connection manager, this method was the most viable approach. This is used as a stepping stone to generating the profile remotely and subsequent associations will leverage the EAP-TTLS mechanisms. EAP-GTC does not protect the authentication data, both text challenge and reply are sent as clear text.

Combine with EAP-PEAP, MSCHAP, for windows mobile clients, EAP-TTLS and EAP-GTC mechanisms do offer some form of security assurance, however, the path to improve user experience led us towards the employment of EAP-TLS which offers improvements over these EAP methods. EAP-TLS mandates server and client certificate based authentication. In brief, certificates are used instead of a subscriber's username and password as credentials. The content within the certificate typically consists of various attributes that are encrypted, the subscribers username and password are typically not included within. While this requirement makes it more secure than most other EAP methods, it is more challenging to deploy as it requires certificates to be generated and there is additional cost incurred in using a trusted

Certificate Authority (CA) to produce these certificates. There are benefits of using a trusted Certificate Authority as most of the Global Certs are already embedded within various devices operating systems and applications. This enables the client to server/AP authentication to occur seamlessly and to ensure the subscriber is associated with a trusted AP and not a rogue AP.

To understand the improvements that are proposed, let's explore the specifics around EAP and IEEE 802.1x.

3. EAP Primer

EAP, Extensible Authentication Protocol, is an authentication framework developed to function at the link layer. It is defined in RFC 3748 and updated in RFC 5247. There are many authentication mechanisms that functions within the EAP framework, they were developed by various vendors to accommodate different operating systems.

EAP is designed to function within the link layer, negotiation occurs between the supplicant (end user mobile client) and the Authentication Server (typically a RADIUS server) via an Authenticator (typically an Access Point with RADIUS client). RADIUS attributes are required to be supported for each new authentication mechanism that is developed. Figure 1 depicts the high-level flow of an EAP transaction

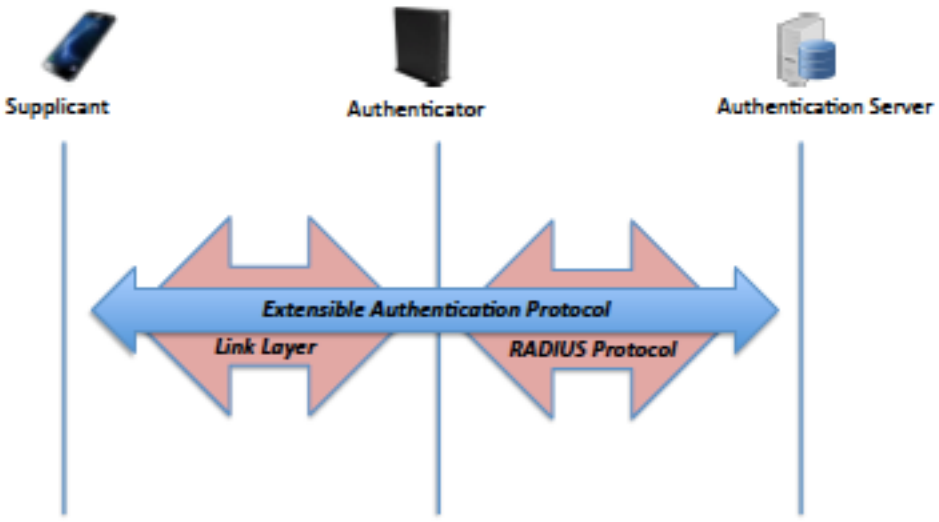

Figure 1 - High Level EAP exchange between Supplicant and Authentication Server via Authenticator

4. IEEE 802.1x and EAPOL

The IEEE 802.1x standard and EAP over LAN (EAPOL) are typically coined as the same term, they referenced one another within the standard. IEEE 802.1x is found within the 802.11i standards where security attributes such as WPA2 (WiFi Protected Access version 2), TKIP and AES are derivatives.

IEEE 802.1x is an IEEE standard for port based Network Access Control, what this translates to is access managed by means of a port. Until authentication is validated, access is blocked by the port to a LAN or WLAN. It does so by encapsulating EAP protocol over IEEE 802, also known as EAPOL.

Figure 2 depicts the EAPOL frame and Figure 3 the EAPOL high level flow, as mentioned previously, the EAPOL frame contains destination and source MAC address but no network frame blocks as it functions on the Link Layer

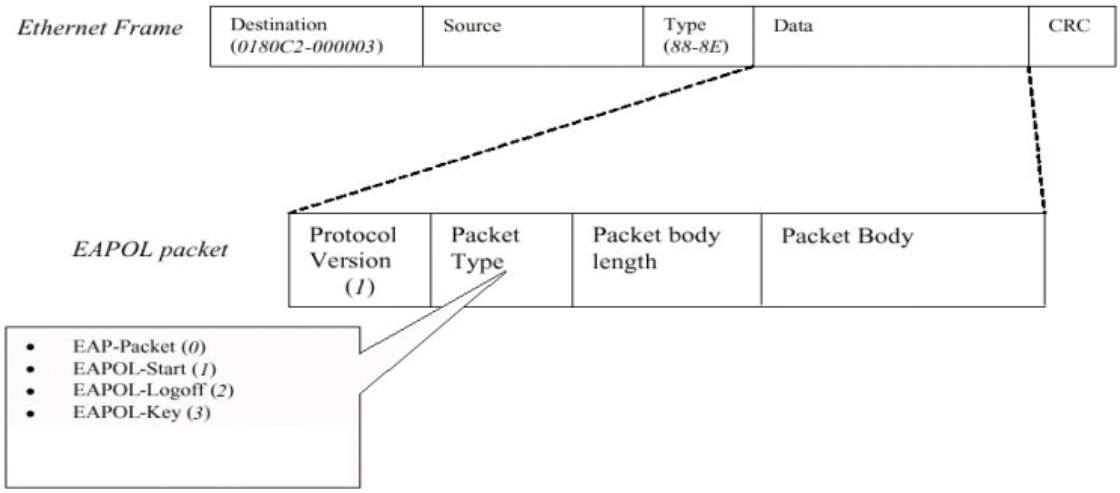

Figure 2 - EAPOL Frame structure

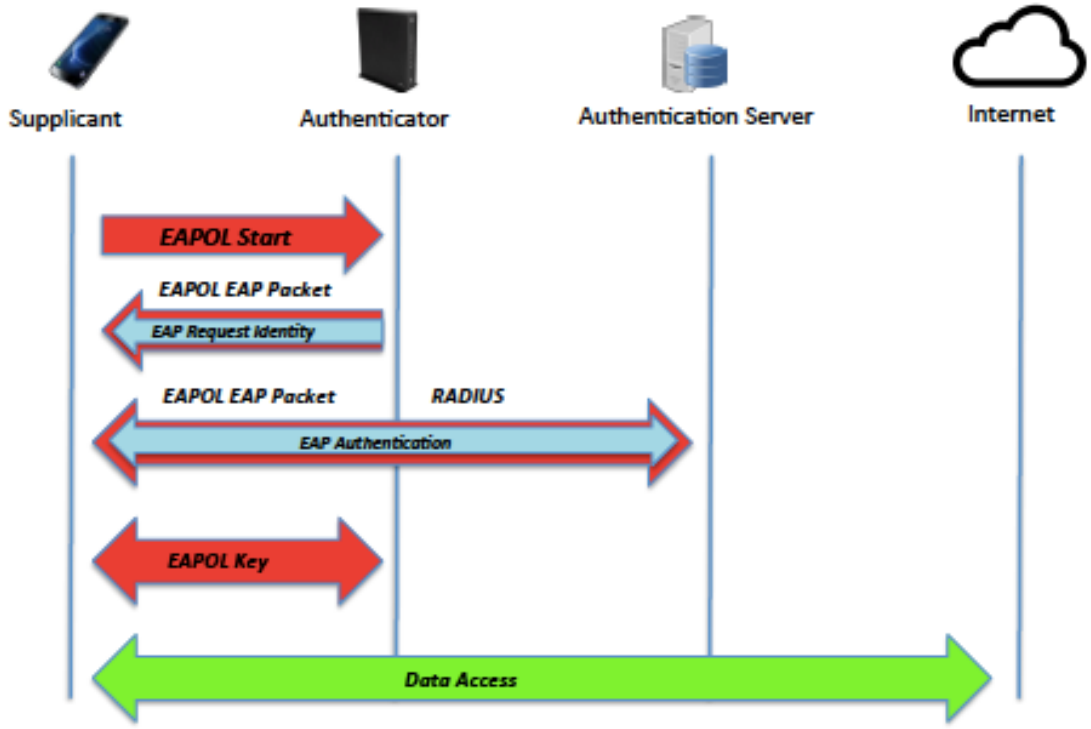

Figure 3 - EAPOL High Level Flow

5. EAP-TLS Primer

EAP-Transport Layer Security (TLS) is the authentication mechanism selected to provide a secure experience. EAP-TLS, as defined in RFC 5216, is an IETF open standard that requires the use of both client and server certificates, preferably from a trusted Certificate Authority (CA). This is known as mutual authentication where certificates from both entities are validated prior to enabling access. Certificates adhere to the x.509 standard where the process of invoking a certificate is defined clearly with specific attributes such as encryption type, method, organization name, expiration date, extensions, among others are supported by most Certificate Authorities in their Public Key Infrastructure specifications. Please refer to Figure 4 for the structure of an x.509 certificate:

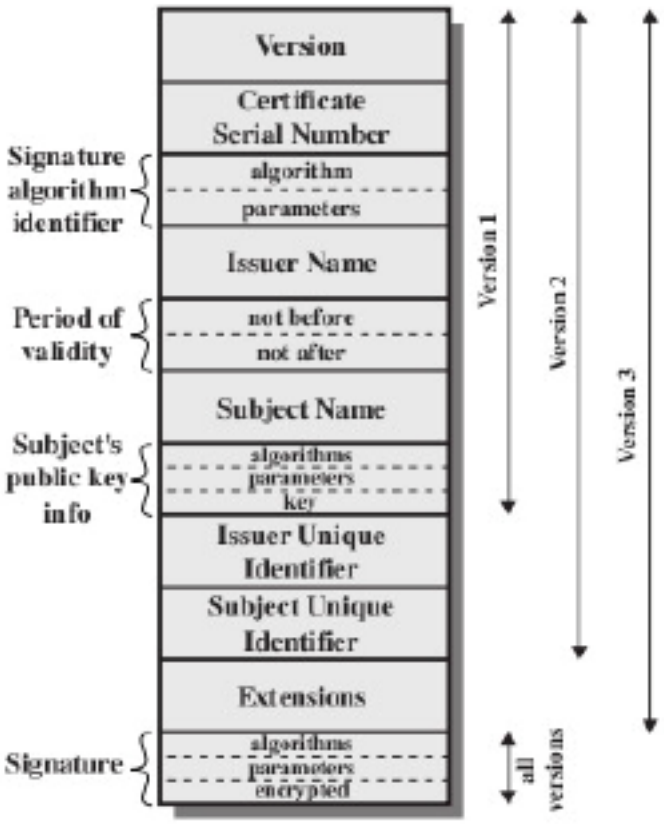

Figure 4 - x.509 Certificate Structure

Attributes within the certificate are defined by the organization and issued by the Certificate Authority. A public and private key is established as part of the certificate generation process, the certificate(s) are then chained to a trusted root certificate of the CA. The server and client certificate will contain the private keys that are only known to itself and the CA, it is used to decrypt the public key that are then distributed to other devices/applications. An analogy would be a user accessing their banking website today, the mobile device employs the use of a browser that contains certain certificates (private key) that are inherently trusted and embedded. When the banking website is accessed, the SSL transaction would be called upon and check the certificate (public key) of the website to ensure it is a legitimate website. With EAP-TLS, the exchange occurs on both ends with the client and the server validating both certificates. If the server certificate is not who they claimed to be, then the authentication fails, this would be akin to preventing connectivity to a rogue AP with the added benefit of validating the client as well. It the server certificate passes but the client certificate fails, that could be translated as a user who is no longer a valid subscriber due to a number of reasons.

Figure 5 depicts the EAP-TLS flow, it is based off the EAPOL message flow if compared with Figure 3. Digital certificates are used in place of username and password as credentials. Mutual authentication exchange certain RADIUS attributes between the mobile client (supplicant) and the Authentication Server (RADIUS server) via the AP (NAS). A series of RADIUS messages are exchanged after the initial EAPOL transaction is initiated, a RADIUS Access-Request will be invoked as a result of an EAP-Response/Identity call. Common RADIUS attributes in this flow include NAS-Id, NAS-Port, Calling-Station-Id. The RADIUS server in turn will send a RADIUS Access-Challenge message to the AP which produces an EAP-Request message to the mobile client. Common RADIUS attributes in this flow includes Session-Timeout, Service-Type. The mobile client then responds with an EAP-Response [containing the certificate] to the AP which will produce a RADIUS-Access-Request message where AAA will then validate the certificate. If certificate is valid, AAA will return a RADIUS-Access-Accept message and the session keys to the AP, and in turn an EAP success.

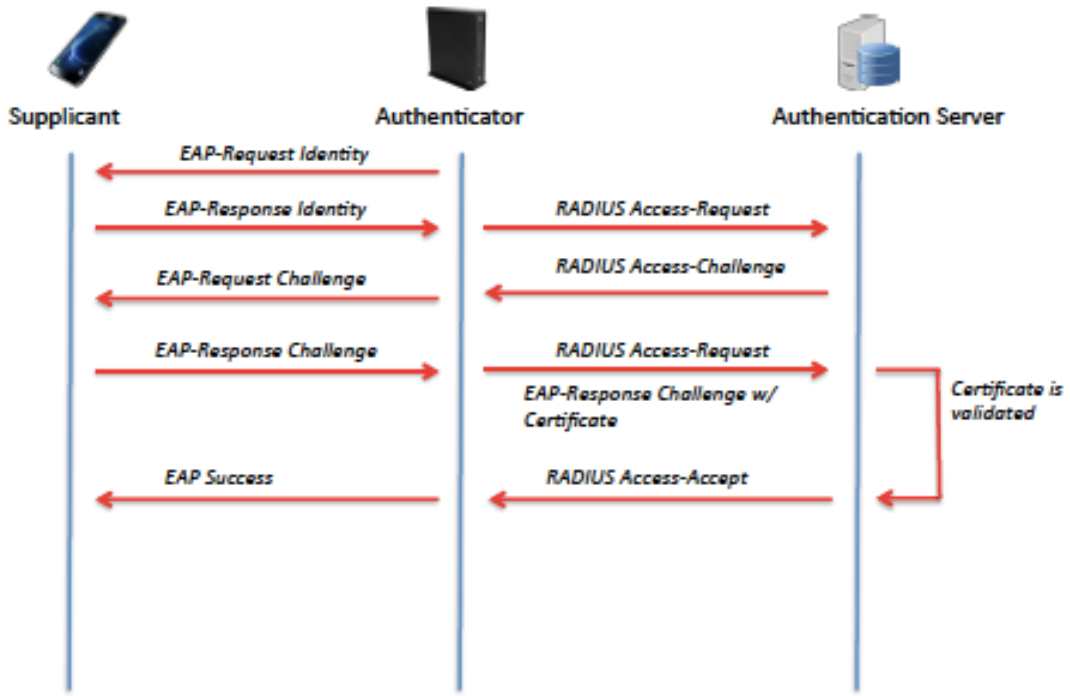

Figure 5 - EAP-TLS message flow

6. Certificates

Essentially, two forms of authentication will occur in EAP-TLS: network will be authenticated against client, then client will be authenticated against network. Instead of using username and password, certificates are the common elements involved. On the network side, the certificate may reside on the AAA or any component playing the role of the AAA server. Figure 6 displays a sample certificate on the network side:

Figure 6 - Server Certificate

Some of the common attributes defined within a server cert are the Country, State, Locality, Subject, Organization, Organizational Unit, Common Name. The certificate encryption may be RSA or ECC based, typically with a 2048 modulus bit encryption applied. Ultimately, the server cert is chained to the trusted CA Root Cert that is prevalent on most device operating systems root store.

Figure 7 displays a sample certificate on the client side which is generated based on certain user attributes. Ultimately, the certificate is chained to a trusted Root CA.

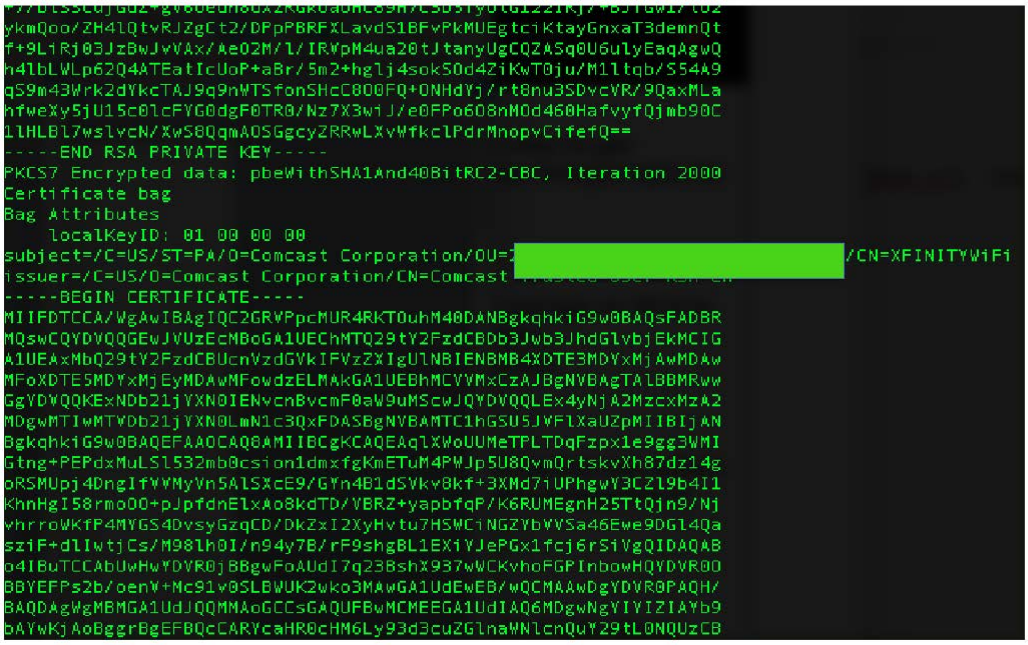

Figure 7 - Client Certificate

7. Implementation

The benefits of employing certificates mutually between server and client and vice versa ensures a secure and seamless on-boarding experience for the user. To achieve this, many factors come into play such as certificates from trusted Certificate Authorities, core network infrastructure upgrades (such as captive portal development), policy changes (primarily to AAA), AP security features support (to support EAP mechanisms), and app development for various client operating systems (to provide an intuitive user interface)

The user interface will essentially redirect a user to a captive portal to assist in generating and installation of a client certificate based on certain required parameters. This is the initial encounter which will not be repeated unless in the event of an expired certificate or when deemed necessary to reissue a new certificate. Subsequent client associations will not require any user input, the EAP-TLS exchange would ensure a transparent, secure connectivity between the client and AP. Even in a roaming scenario between APs, the certificates exchange would occur in the background and help authenticate and validate the mobile client on their respective service provider public WiFi network.

8. Looking Forward

The security implementation of EAP-TLS will help ensure the proper framework is in place to accommodate other EAP mechanism as additional services are offered that may take advantage of the public WiFi network such as cellular service. The underlying foundation are in place to also support other industry standard specifications such as Hotspot 2.0. As the implementation help evolve the public WiFi network to a carrier grade level, the users will only stand to benefit from these changes.

9. Abbreviations

Acronyms	Description
AAA	Authentication, Authorization and Accounting
AP	Access Point
CA	Certificate Authority
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
GTC	Generic Token Card
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network

10. Bibliography & References

802.11 Wireless Networks: The Definitive Guide, 2005, O'Reilly, Matthew Gast

R10.0 WiFi Authentication with EAP. LCW442H-V3.0-SG Edition 1, NokiaEDU

Figure 2: http://www.zyxeltech.de/SNoteZW5_362/app/8021x.htm

Figure 4: https://www.slideshare.net/koolkampus/chapter-ns4

