Poster: Trust-based Light-weight Association Protocol for 802.11 Networks

Vineeta Jain
MNIT Jaipur, India
2015rcp9051@mnit.ac.in

Vijay Laxmi
MNIT Jaipur, India
vlaxmi@mnit.ac.in

Manoj Singh Gaur
IIT Jammu, India
director@iitjammu.ac.in

Mohamed Mosbah
LaBRI, University of Bordeaux, France
mohamed.mosbah@labri.fr

***Abstract*—We present a light-weighted trust based low bandwidth association protocol named ETAnalyst for 802.11 networks that would empower clients to assess the legitimacy of access points (APs) and detect Evil Twins (ETs) before associating with them. An ET can be defined as a rogue AP created by hackers to resemble the authentic AP in a network zone. ETs are easy to launch and can be extremely fatal as they can execute attacks such as spoofing, Man-in-the-middle (MITM) attack, etc., which may lead to information loss, financial loss, remote control, etc. The existing IEEE 802.1X protocol is considered robust against ET attacks, but the deployment is expensive and non-trivial as it requires meticulous setup for initial handshake and X.509 public key certificate issued by a trusted certification authority (CA). It puts an additional cost on network operators, particularly existing ones, who have no incentive to provide this facility. ETAnalyst operates by padding surplus information named as trust bytes in 802.11 management frames. These bytes are evaluated by clients to judge the genuineness of APs. ETAnalyst abides by the existing 802.11 standards by not appending information greater than the permissible management frame size. The approach is light-weight considering it does not employ any encryption. The approach does not use any pre-shared keys or strings; thus it is scalable. No additional hardware and certificates are required, making ETAnalyst a low-cost technique. Since it abides by existing 802.11 standards, a minor adaptation at driver level of AP and client is needed to implement in real networks; thus ensure negligible overhead.**

I. Introduction

Today, users want a seamless Internet connection on their mobile devices. They are least concerned regarding the authenticity of the APs. The attackers exploit this fact by introducing ETs in the network through a laptop or smartphone in a public Wi-Fi area, eg. Airports by simply spoofing SSIDs (Service Set Identifier). It is more challenging to evade ETs in Smart city models as every device is connected to the Internet. With voice and data offloading to wi-fi networks for saving spectrum in 4G networks, the attack vector shall get further expanded.

A lot of work has been conducted in the direction of ET detection. We categorize the existing solutions into two categories - post-association and pre-association. The post-association techniques identify an AP as an ET after associating with it. However, they are incapable of preventing phishing attacks, as they analyze APs after the relay of Internet traffic through them. The pre-association techniques disclose an AP as an ET before associating with it. Bratus et. Al [1] creates fingerprints of 802.11 MAC responses from routers. Although, this approach cannot detect an ET launched using mobile phones or software. Tang et al [2] utilize received signal strength indicators (RSSI) to catch an ET. However, this approach is only for stabilized APs and cannot detect an ET from software or mobile devices. Travis [3] proposed a certificate based technique to detect ETs. However, certificate distribution and management is not a trivial task and hence, not feasible to implement in a real scenario. Unfortunately, no such technique exists which can effectively and efficiently detect an AP as an ET (launched either through hardware, software or mobile phone) before associating with it.

We propose ETAnalyst, an association protocol for ET detection in the network. ETAnalyst works by stuffing additional **trust bytes** in the **management frames**[1] **(beacon/probe response)**, which are evaluated by clients to detect the genuineness of APs. The motivation being, the management frame is the only frame received by clients before associating with the APs. ETAnalyst offers the following advantages:

- **Light-weight**: ETAnalyst does not make use of any encryption or certificate based methods.
- **Trust based**: A trust is shared between clients and APs. Trust implies to a pre-shared trust bytes creation methodology, utilizing a password which gets updated periodically. Thus, it is resistant to dictionary attacks.
- **Low-Bandwidth**: The size of a management frame body is 2320 bytes. We are overloading these frames by not increasing the size more than 2320 bytes. Since we are not increasing the frequency of management frames; thus the bandwidth consumption is optimal.
- **Low-Cost**: No additional hardware is used.

II. Preliminaries

The structure of management frames is shown in Fig. 1. The vendor-specific (VS) element is 252 bytes long and always the last field in the frame. It can contain multiple VS elements. We propose to overload VS field by appending a new VS element containing the trust bytes.

[1]In this document, beacon frame and probe responses are referred to as management frames.

Network and Distributed Systems Security (NDSS) Symposium 2018
18-21 February 2018, San Diego, CA, USA
ISBN 1-1891562-49-5
http://dx.doi.org/10.14722/ndss.2018.23xxx
www.ndss-symposium.org

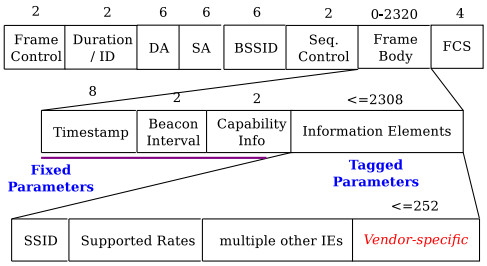


Fig. 1 – Structure of beacon frame

III. Trust Bytes

We define **Trust Bytes** as 16-byte hex information computed using Password-Based Key Derivation Function 2 (PBKDF2) hash function. PBKDF2 is used because it applies password iterations and thus, resistant to brute-force attacks [4]. Let the trust bytes be represented as T_o.

$$T_o = PBKDF2(PF, Pass, salt, c, dklen) \quad (1)$$

- PF = pseudorandom function for producing the hash. We use HMAC-SHA1.
- Pass = password. We use the date in six formats separated by a colon as a password (permutation of ddmmyy).
- salt = a nonce. We use a permutation of hours and minutes as a salt.
- c = number of iterations = 1000
- dklen = length of output = 16 bytes

The idea behind using date and time as password and salt respectively is that, in a day, the combination of hours and minutes is unique and, a date is unique for a year. Next year the year will change and thus the password keeps on updating. Thus, the T_o will be unique per minute. We assume that only the trusted APs and clients have access to the trust byte generation methodology. Since we use PBKDF2, attackers have extremely low chances of cracking the trust bytes.

IV. ETAnalyst

The workflow of ETAnalyst is depicted in Fig. 2. Firstly, the client sends out a probe request to the APs and calculates the trust bytes (T_o'') periodically every minute. The AP receives the probe request and prepares a probe response by appending an additional VS element containing the trust bytes (T_o) in the frame. The AP transmits the probe response to the client. The client, upon receiving the frame evaluates the trust. If both T_o and T_o'' are similar, the client sends an association request to the AP; else discards the frame.

To prevent replay attacks on management frames and avoid the matching overhead at the client side, the client stores the sequence number of management frames for every SSID with a window size of 100, i.e., for a management frame with the same SSID, if the sequence number lies in the window, client ignores the packet and updates the sequence number.

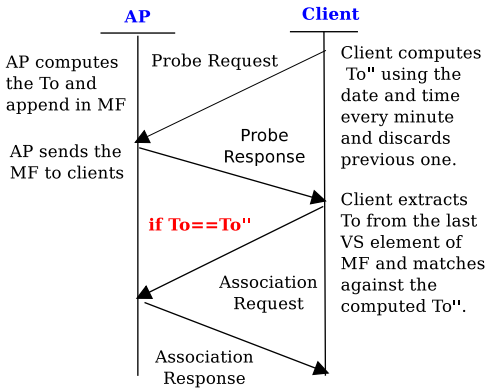


Fig. 2 – Workflow of ETAnalyst

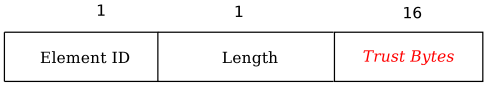


Fig. 3 – Structure of appended VS element

V. Design and Implementation

An additional VS element is appended to the management frame as shown in Fig. 3. Here, the Element Id for VS element is 221, length is 16, and the trust bytes contains 16 bytes of hashed hex data. This element is always the last of all VS elements present in the frame. The total length of management frame does not exceed the standard 802.11 frame size.

The implementation of ETAnalyst will be conducted on **hostapd** as AP and **wpa_supplicant** as client. The drivers responsible for sending and receiving management frames will be modified to incorporate the proposed protocol.

VI. Conclusion

ETAnalyst is an association protocol that works at link layer of the open source interconnect (OSI) model for ET detection. Thus, ETAnalyst empowers clients to detect ETs before association and relay of Internet traffic protecting their personal and financial information from attackers. Unlike 802.1X, ETAnalyst does not burden network administrators with additional certificate cost or installation. Hence, it can be easily deployed in public wi-fi networks.

Acknowledgment

The authors would like to thank Mojo Networks, Pune India for supporting an internship for proof testing the approach.

References

[1] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles, "Active behavioral fingerprinting of wireless devices," in *Proceedings of the first ACM conference on Wireless network security*, pp. 56–61, ACM, 2008.

[2] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, X. Gong, and Z. Wang, "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes," *Mobile Information Systems*, vol. 2017, 2017.

[3] T. S. Hendershot, "Towards using certificate-based authentication as a defense against evil twins in 802.11 networks," 2016.

[4] "PBKDF2." https://en.wikipedia.org/wiki/PBKDF2.

Trust based Light-weight Association Protocol for 802.11 Networks

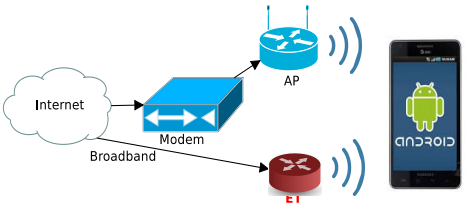
Vineeta Jain[1], Vijay Laxmi[2], Manoj Singh Gaur[3] and Mohamed Mosbah[4]

[1,2]Malaviya National Institute of Technology Jaipur India, [3]Indian Institute of Technology Jammu India and [4]LaBRI, CNRS, Bordeaux INP, University of Bordeaux, Talence, France

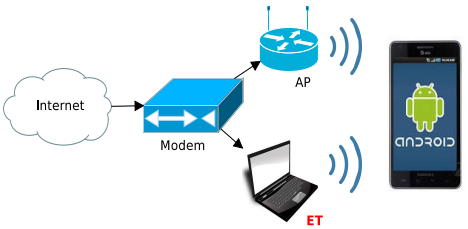
Overview

- We present a light-weight trust based low bandwidth association protocol named ETAnalyst for 802.11 networks that would empower clients to assess the legitimacy of access points (APs) before associating with them.
- It operates by stuffing additional **trust bytes** in the **management frames (beacon/probe response)**, which are evaluated by clients to detect ETs.
- It abides by the existing 802.11 standards by appending information not greater than the permissible management frame size.
- **Light-weight**: It does not make use of any encryption methods.
- **Trust based**: Trust here implies a pre-shared trust octet creation methodology, utilizing a password which gets updated with periodically.
- **Low-Bandwidth**: Since, we are not increasing the frequency of management frames, thus the bandwidth consumption is optimal.
- **Low-cost**: No expensive hardware is required.

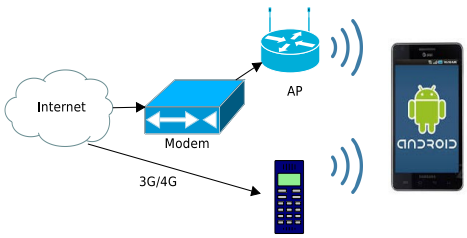
Launching ET Attacks



(a) ET is created using a hardware



(b) ET is created using software on laptop



(c) ET is created using hotspot on mobile phones

Trust Bytes

We define **Trust Bytes** as 16-byte hex information computed using Password-Based Key Derivation Function 2 (PBKDF2) hash function. Let the trust bytes be represented as T_o.

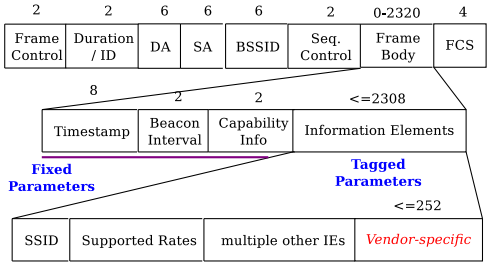
$$T_o = PBKDF2(PF, Pass, salt, c, dklen) \quad (1)$$

where,

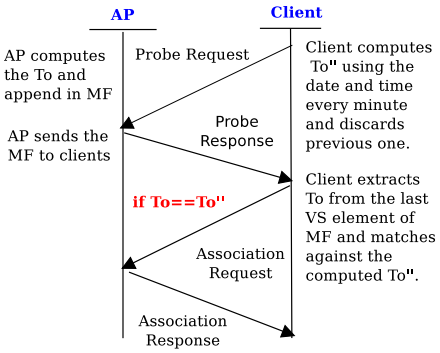
- PF = psuedorandom function for producing hash. We use HMAC-SHA1.
- Pass = password. We use date in six formats separated by colon as a password (permutation of ddmmyy).
- salt = a nonce. We use combination of hours and minutes as a salt.
- c = number of iterations = 1000
- dklen = length of output = 16 bytes

Methodology

We propose to overload VS field by appending a new VS element containing the trust bytes.

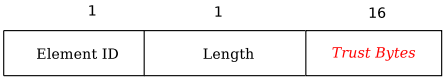


Workflow



Design and Implementation

An additional VS element is appended in the management frame as:



- the Element Id for VS element is 221,
- length is 16 and
- the trust bytes contains the 16 bytes of hashed hex data.

We are implementing the approach using **hostapd**[1] as the AP and **wpa_supplicant**[2] as the client.

Conclusion

ETAnalyst is an association protocol that works at link layer of the open source interconnect (OSI) model for ET detection. Thus, ETAnalyst empowers clients to detect ETs before association and relay of Internet traffic protecting their personal and financial information from attackers. It supplements an additional VS element in the management frame, which is computed to evaluate trust between AP and clients. Unlike 802.1X, ETAnalyst does not burden network administrators with additional certificate cost or installation.

References

[1] Linux Wireless. `https://wireless.wiki.kernel.org/en/users/documentation/hostapd`.

[2] wpa_supplicant-2.6. `http://www.linuxfromscratch.org/blfs/view/svn/basicnet/wpa_supplicant.html`.

[3] PBKDF2. `https://en.wikipedia.org/wiki/PBKDF2`.

Acknowledgment

The authors would like to thank Mojo Networks, Pune India for supporting an internship for proof testing the approach.

Contact Information

Email: 2015RCP9051@mnit.ac.in
Phone: +91 9521774641