User Study Report

In this report, we first explain the approach we have used to conduct this study. Then we present the results we obtained. Last, we include the full questionnaire that is used in this study

Approach of Our User Study

Goal of the study

Our user study aims to explore whether users' perception on the configuration options and response to the warnings could make them susceptible to the evil twin attack. In view of the practical and realistic factors such as discrepancies in the enterprise wireless network settings, devices together with installed OSes, and client awareness towards network security, we aim to further discover links between evil twin attacks and clients' detailed preferences when using enterprise Wi-Fi.

Study Setup

We target users who frequently access wireless networks secured by WPA Enterprise, such as employees in corporations and staff/students in educational institutes where Eduroam is deployed. Therefore, the participants have sufficient experience with laptops and/or smart phones by the time they take this questionnaire. To better understand the security risks associated with users, we group the participants according to their education levels and self-evaluated knowledge levels on network security.

Prior the questionnaire, we hide our real intention and inform the participants that this study is meant for evaluating the enterprise Wi-Fi user experience. We recommend them to select the answers that best suit their daily routine behavior. We have also obtained their acknowledgement and consent that the responses would be recorded and further applied in our analysis. Then each participant is presented with a set of same questions which we explain in the following section. We do not provide hints on the questions to ensure unbiased responses from the participants. After completing the questionnaire, we reveal our real purpose to the participants and provide feedbacks and recommendations to enhance their awareness towards wireless network security.

Results and Discussion

We have received 129 valid responses from WPA- Enterprise users with bachelor degrees and above. The majority of the participants have a computing/engineering-related major (over 87.6%) and have some knowledge regarding network security (over 77.8% chose 3 and above out of a range of 0-5, with 5 being the expert level of knowledge and vice versa).

We have observed that the participants, regardless which OSes they are using, are inclined to continue with the insecure connection option (i.e., to choose 'Connect' or 'Accept'), even when they are warned about the insecurity of the network. Despite this risky preference, around 70% of the participants still perceive that their credentials are secure to a reasonable extend. We also notice that a relevant education background (i.e., engineering and computing) does not improve the security awareness towards network security. We also observe that participants considering themselves more familiar with network security tend to have a higher chance of choosing the secure configuration. However, even for those who are security experts, the probability of a secure choice is still below 60%.

Even though the correct configuration of WPA-Enterprise serves as a crucial safeguard to the enterprise network security, we have found that only 24% of the participants are confident that they have received proper training and instructions on securely connecting to enterprise wireless network. The lack of security training has been reflected in the participants' WPA Enterprise configuration choices. For example, over 70% of the Android users chose default settings since they are uncertain about details regarding the supported authentication protocols.

Questionnaire:

This is a user preference study on WPA Enterprise. Please select the answers that best describe/represent your behavior when connecting to wireless networks authenticated by WPA Enterprise. Note that information from this questionnaire will be recorded for further analysis. By completing this questionnaire, you consent the usage of data provided hereby.

Section 1: Information about yourself

Q1: Highest Degree Obtained

(a) High School Diploma **(b)** Bachelor Degree **(c)** Graduate Degree **(d)** Others, please specify

Q2: Major (where applicable)

(a) Engineering **(b)** Computing **(c)** Others, please specify

Q3: How would you rate your knowledge level of network security? On scale of 1(no knowledge) to 5 (expert in network security).

(a) 1 **(b)** 2 **(c)** 3 **(d)** 4 **(e)** 5

Section 2: Information about your device

Q4: What is the type of device(s) you use to connect to wireless networks authenticated by WPA Enterprise?

(a) Laptop **(b)** Smart phone/tablet **(c)** Both, please answer questions regarding both laptop and phone

Q5: What is the OS run on your device (if multiple devices chosen, please complete the corresponding questions for each device)?

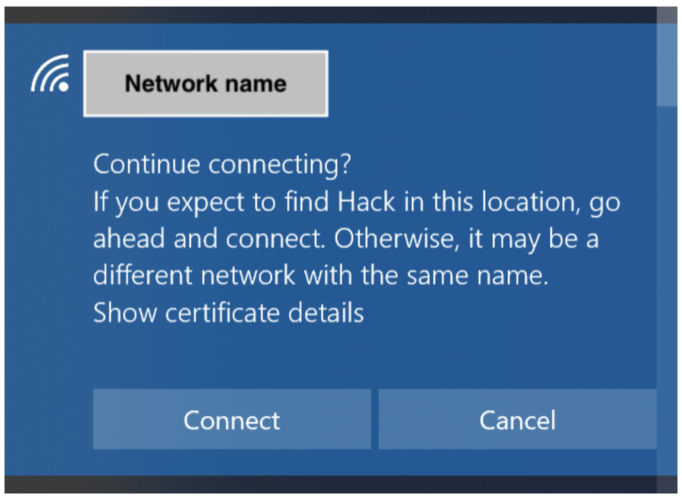
(a) Windows (Proceed to Q6) **(b)** MacOS (Proceed to Q7) **(c)** Android (Proceed to Q8) **(d)** iOS (Proceed to Q9)

Please specify the version of the device OS:

Section 3: WPA Enterprise Configuration User Interfaces

Section 3-1: Windows (Q6-Q7)

Q6: Suppose you have connected to the WPA Enterprise Wi-Fi signal, and keyed in your credentials. The following warnings (Figure 1) shows up. Which option best describes your behavior when choosing network authentication method (as highlighted in red rectangle)?



Network name

Continue connecting?
If you expect to find Hack in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details

Figure 1. Information prompted upon clicking on the SSID of target enterprise network in Windows.

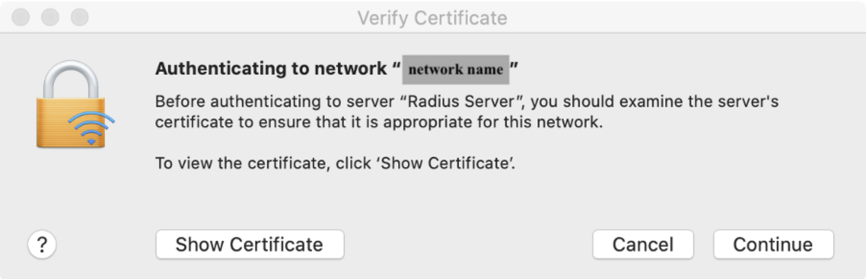
(a) Click 'Connect'

(b) Click 'Cancel'

(c) Click 'Show certificate details' and decide

Section 3-2: MacOS

Q7: Suppose the following information appears (Figure 3) during your Wi-Fi configuration or after getting connected, you would:



Verify Certificate

Authenticating to network " network name "

Before authenticating to server "Radius Server", you should examine the server's certificate to ensure that it is appropriate for this network.

To view the certificate, click 'Show Certificate'.

Figure 2. Information prompted upon clicking on the SSID of target enterprise network in MacOS.

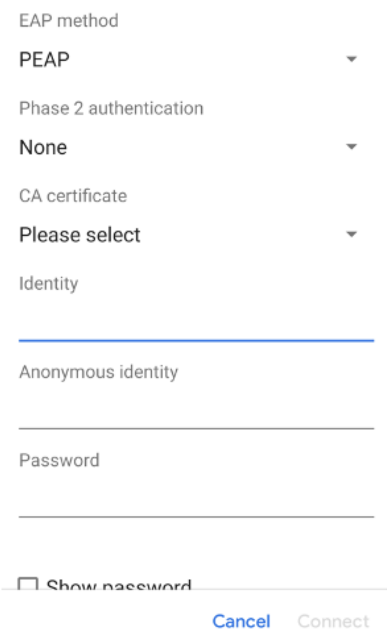
(a) Trust the certificate and click 'Continue'

(b) Doubt the validity of the certificate and click 'Cancel'

(c) Click 'Show certificate details' and decide

Section 3-3: Android

Q8: Suppose you have connected to the WPA Enterprise Wi-Fi signal, and the configuration UI (Figure 3) shows up. Which configurations will you select?



EAP method
PEAP

Phase 2 authentication
None

CA certificate
Please select

Identity

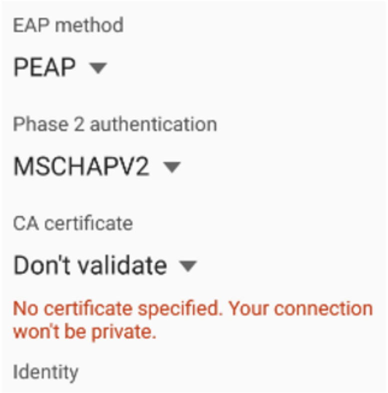
Anonymous identity

Password

□ Show password

Figure 3. WPA configuration UI in Android.

- **Q8-1:** EAP method: **(a)**TLS **(b)** TTLS **(c)** PEAP **(d)** Not sure, will just use default setting
- **Q8-2:** Select phase 2 authentication protocol (only for EAP-TTLS and PEAP): **(a)** PAP (TTLS) **(b)** MSCHAP/v2 (TTLS or PEAP) **(c)** GTC (TTLS or PEAP) **(d)** Use default or none
- **Q8-3:** CA Certificate: **(a)** Not specify **(b)** Specify a dedicated certificate **(c)** Specify any certificate **(d)** Not validate certificate **(e)** Not sure, will just use default setting
- **Q8-**4: If your answer to **Q8-3** is **(d)**, please answer this question. The following warning (Figure 5) will be shown. What will you do? **(a)** Still proceed to 'Connect' **(b)** Choose a random certificate **(c)** Choose a certificate from a trusted CA



EAP method
PEAP

Phase 2 authentication
MSCHAPV2

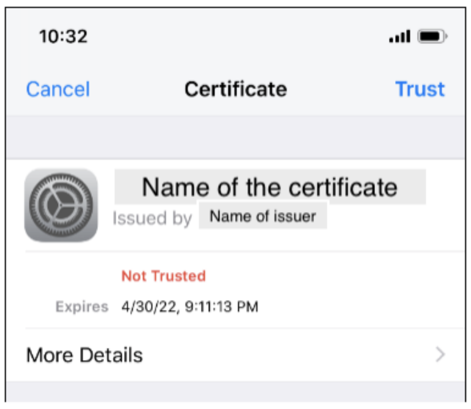
CA certificate
Don't validate
No certificate specified. Your connection won't be private.

Identity

Figure 5. Warning information during WPA enterprise configuration

Section 3-4: iOS

Q9: Suppose the following information appears (Figure 6) during your Wi-Fi configuration or after getting connected, you would:



10:32

Name of the certificate
Issued by Name of issuer

Not Trusted
Expires 4/30/22, 9:11:13 PM

Figure 6. Information prompted upon clicking on the SSID of target enterprise network in iOS.

(a) Trust the certificate and click 'Accept'

(b) Doubt the validity of the certificate and click ‘Cancel’

Section 4: Opinions towards Enterprise Wi-Fi Authentication

Q10: Does your company provide tutorial or specific instructions on the configuration of WPA Enterprise, especially on the certification verification?

(a) Yes

(b) No

(c) Not sure

Q11: What type of online services you would access, after getting authenticated and connected to the enterprise network (multiple choice)?

(a) Social networks

(b) Enterprise internal system

(c) Video streaming

(d) Financial services (e.g., ebanking)

(e) News

(f) Others, please specify:

Q12: On scale of 1 (extremely low) to 5 (extremely high), what is your confidence level regarding the security of your credentials if you configure enterprise Wi-Fi as you have described earlier?

(a) 1 **(b)** 2 **(c)** 3 **(d)** 4 **(e)** 5