An Empirical Study of WPA-Enterprise Misconfigurations

Stuart Minshull
ECE Department
Boston University
Boston MA,02215
minshull@bu.edu

David Starobinski
ECE Department
Boston University
Boston MA, 02215
staro@bu.edu

***Abstract*—we report the results of a survey of the configurations of WPA-Enterprise (IEEE 802.1X) networks at US universities, based on public information available from their web sites. We find that 77.8% of the networks are weakly configured, leaving them potentially vulnerable to severe attacks, such as man-in-the-middle and password cracking attacks.**

Keywords—Wi-Fi; security; authentication

I. Introduction

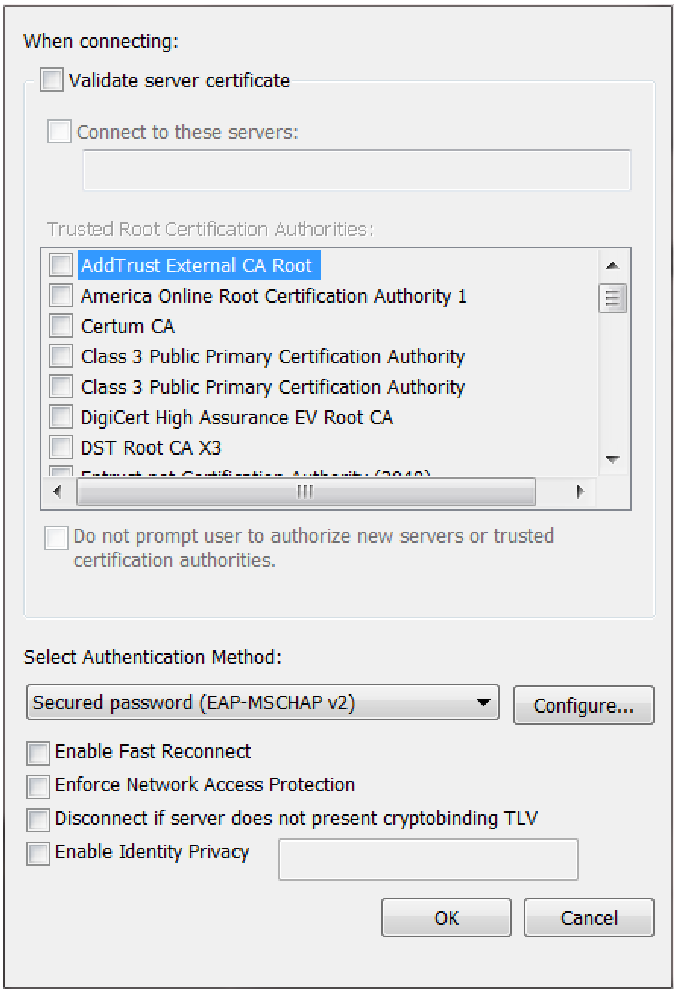
IEEE 802.1X is a security protocol designed for large enterprise style networks, with large amounts of users, each potentially needing a different level of access permission. This is accomplished through the use of a Remote Authentication Dial In User Service (RADIUS) server which remotely manages Authentication, Authorization, and Accounting (AAA) for connecting users. WPA-Enterprise Wi-Fi networks adopt this architecture.

While 802.1X networks are considered secure when implemented correctly, there are many ways to incorrectly configure supplicants that create man-in-the-middle vulnerabilities. The following discussion focuses on 802.1X networks using the Protected Extensible Authentication Protocol (PEAP).

II. Vulnerabilities

If a supplicant does not validate the server certificate (see Fig. 1), then attackers can easily create a fake AP with the same BSSID/SSID as the target network. Clients who unwittingly attempt to connect to the fake network will not validate the server certificate, and have no way to determine that the server they are connecting is not the valid server. The supplicant establishes a valid TLS tunnel with the rogue server, and transmits a username in clear-text along with an MSCHAPv2 hash of the user's password. While the user credentials are hashed, MSCHAPv2 is not a secure hashing algorithm and has been shown to be easily crackable [1].

Another attack becomes possible if the target network validates a server certificate signed by a public CA, but does not specify a server name. When this occurs, attackers can use any certificate signed by the CA to "validate" their network.



When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ America Online Root Certification Authority 1
□ Certum CA
□ Class 3 Public Primary Certification Authority
□ Class 3 Public Primary Certification Authority
□ DigiCert High Assurance EV Root CA
□ DST Root CA X3
□ Entrust.net Certification Authority (2048)

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

Fig. 1: 802.1X supplicant configuration window.

Since the supplicant is configured to trust any certificate issued by that CA, the client will connect to the rogue network without issue and transmit its credentials to the attacker in the same form as mentioned above.

The above attacks can easily be mounted using open source software, such as FreeRADIUS-WPE [2] developed by Joshua Wright and Brad Antoniewicz, a patch for FreeRadius [3] that logs captured credentials.

III. EMPIRICAL SURVEY

A. Methodology

We conduct a survey of the wireless network configurations at 262 public and private not-for-profit universities classified by the Carnegie Institute as large, 4-year institutions. The survey is conducted by examining the university network setup pages and FAQs.

B. Findings

The vast majority of institutions make their network set-up publicly available. Thus, only 7 out of 262 web sites require authentication to view network setup, network FAQ, or detailed network structure pages.

Based on information collected from the web sites, over half of the institutions, uses 802.1X to secure their wireless networks. The rest use some form of user access control (e.g., MAC filtering, IP filtering, etc.), proprietary client configuration, VPNs, or keep their networks open.

Among the 153 institutions deploying 802.1X networks, 46 do not validate the server certificate and 119 do not specify the server name. Thus, an astonishing 77.8% of the surveyed 802.1X networks may be vulnerable to one or both of the attacks described in Section II.

IV. CONCLUSION

There is nothing inherently wrong with WPA-Enterprise using PEAP, nor is it considered weak when implemented correctly. However, as our survey shows, a high fraction of networks appear to be implemented incorrectly and to be insecure for various reasons. A deeper study into why network configurations are set in the current way would be valuable to determine the next course of action.

[1] Schneier, Bruce, and David Wagner. "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)." *Secure Networking—CQRE [Secure]'99*. Springer Berlin Heidelberg, 1999. 192-203

[2] On-line http://www.willhackforsushi.com/?page_id=37

[3] On-line http://freeradius.org/

This research was supported in part by the US National Science Foundation, under grant CNS-1012910.