Shmoocon RFP

Author: Joshua Wright
Contact: jwright@willhackforsushi.com, 401-524-2911

Session Title: PEAP: Pwned Extensible Authentication Protocol
Session Preference: Break It
Keywords: EAP, Wireless, 802.11, 802.1X, PEAP, TTLS, LEAP, EAP-MD5, EAP-FAST, authentication, extensible

Abstract

WiFi networks leverage various EAP types to authenticate wireless users. Many of these EAP installations are vulnerable to a variety of attacks, often revealing authentication credentials for users. In this presentation, the author will present attacks against multiple EAP types including PEAP and TTLS, demonstrating how an attacker can compromise these otherwise strong authentication mechanisms.

Presentation Description

We all know about vulnerabilities in WEP (woopee) and we've learned some valuable lessons for what is needed to secure wireless infrastructure: strong encryption, and strong authentication. In modern WPA/WPA2 networks, strong encryption is covered by TKIP and CCMP, while authentication is handled by IEEE 802.1X at layer 2, with a supported EAP type at layer 3. Many organizations today have deployed wireless networks using this model, commonly using PEAP or TTLS as the authentication mechanism.

During the analysis and investigation of several EAP clients and customer networks, the author discovered that not everything is so rosy in wireless-authentication land. Many users deploy their EAP authentication mechanisms in an insecure fashion, leaving them vulnerable to offline dictionary attacks, precomputed password attacks (via rainbow tables), and network impersonation attacks.

In this presentation, I'll present tools and techniques used to attack wireless authenication mechanisms, starting very quickly with not-so-common platform attacks, culminating with an effective attack against PEAP and TTLS networks.

Presentation Outline

Attacking Wireless Authentication
  + New WPA-PSK attack against wireless clients away from their infrastructure networks (2-3 slides)

+ Updating on attacking LEAP with rainbow tables (4-5 slides)
+ Impersonating EAP-FAST networks (8-10 slides)
+ Attacking PEAP and TTLS networks (15-18 slides)
+ Fixing your crappy EAP deployments (2-3 slides)

Other Conference Information

ShmooCon is my favorite con every year. I have not presented this material at any other conference (I've been saving it for ShmooCon). I also don't like presentations that "make the rounds" across hacker cons and are repeated at different conferences, so I plan to only present this material at ShmooCon.

Facilities Required

Shmooball Virtual Defense Shield
Scene Whores
VGA projector

Bio

Joshua Wright is the author of several tools designed to demonstrate vulnerabilities in wireless networks, an editor for the Wireless Vulnerabilities and Exploits (WVE) project, and a regular speaker at information security conferences.   When not breaking wireless networks, Josh likes to work on his house, where he breaks things of a different sort.