The BYOD PEAP Show
Mobile Devices Bare Auth

Josh Yavor
iSEC Partners
DEF CON XXI
August 4, 2013
“It’s amazing to me that lots of people seemed to have missed this issue in PEAP and other EAP methods, as it’s still extremely useful in most of the pen-tests I engage in.”
– Joshua Wright, May 2010

- Windows and OS X
- FreeRADIUS-WPE
- “PEAP and TTLS can be secure when deployed carefully”

¹http://www.willhackforsushi.com/?page_id=37
Bring Your Own Device
All the cool kids are doing it

- Growth
- 60%-85% of companies
- “Bring Your Own Definition”
- EAP Types
“Enterprises who are depending on the mutual authentication properties of MS-CHAPv2 for connection to their WPA2 Radius servers should immediately start migrating to something else.” – Moxie Marlinspike, July 29, 2012²

- Divide and conquer
- $100 = 100%$ in 24 hours

²https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/
Take Aways

Spoiler Alert

- Real-world deployments are messy
- PEAP is unsafe for BYOD environments
- Impact is enormous
- Immediate corrective action required
- No easy fix
- Users are in control
Bottom Line

Defense

IF YOUR CORPORATE BYOD NETWORK SUPPORTS PEAP

YOU'RE GONNA HAVE A BAD TIME
Bottom Line

Offense

ONLY HAVE A LAPTOP AND $100

AD CREDS
Some Disagree

“In a properly implemented wireless network, this MS-CHAPv2 exploit is a non-issue. There is no need for Wi-Fi network administrators to abandon PEAP. Period.”

---

3revolutionwifi.blogspot.com/2012/07/is-wpa2-security-broken-due-to-defcon.html
Risk Characteristics

**Lower Risk**
- Individual users (depends)
- Smaller organizations
- Static user base

**Higher Risk**
- Internal network assets
- Larger organizations
- Transient user base
Misconfiguration is Everywhere
Be cruel to your school

Google
inurl:edu PEAP Android configure

About 1,100,000 results (0.32 seconds)
For Mobile Devices

Image of a mobile device showing Wi-Fi settings with the following options:
- Security: 802.1x EAP
- Signal strength: Good
- EAP method: PEAP
- Phase 2 authentication: MSCHAPV2
- CA certificate: Unspecified
- User certificate: Unspecified

Options to Connect or Cancel.
Even for Windows

- SSID: 
- Authentication Method: WPA or WPA2-Enterprise (depending on availability on your Wi-Fi enabled device).
- Data Encryption: TKIP or AES (AES is preferred.)
- Other Settings: Uncheck box for validating the server certificate and do not authenticate using Windows login account or as guest.
### PEAP 101

Why is PEAP so popular?

<table>
<thead>
<tr>
<th>EAP Type Support</th>
<th>iOS</th>
<th>Android</th>
<th>Windows Phone 8</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Wireless Authentication Comparison

<table>
<thead>
<tr>
<th>Access Control Granularity</th>
<th>Open</th>
<th>WPA2</th>
<th>WPA2 Ent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Group of users who know password</td>
<td>Individual user accounts</td>
<td></td>
</tr>
<tr>
<td>wifi? ok!</td>
<td>getyourownwifi</td>
<td>evalDoer / 1337p455</td>
<td></td>
</tr>
</tbody>
</table>
### Wireless Authentication Comparison

<table>
<thead>
<tr>
<th></th>
<th>Open</th>
<th>WPA2</th>
<th>WPA2 Ent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>N/A</strong></td>
<td>Change password, update all devices</td>
<td>Modify single user account</td>
<td></td>
</tr>
<tr>
<td><strong>wifi? ok!</strong></td>
<td><code>getyourownwifi2</code></td>
<td><code>Error: User account locked</code></td>
<td></td>
</tr>
</tbody>
</table>
Association to AP

802.thisOneGoesTo11
Outer Authentication

Thanks to Brad & Joshua

![Diagram showing mobile device connecting to SSID: corp-secure, then to RADIUS server, with steps for identity (AD Username) and server certificate for outer authentication and secure tunnel establishment.]
Inner Authentication with MSCHAPv2

Thanks to Moxie
Android

EAP Types

peapshow

Security
802.1x EAP

EAP method
- PEAP
- PEAP
- TLS
- TTLS
- PWD

Identity
- josh

Anonymous identity

Cancel  Save
Android

PEAP Configuration

peapshow

Security
802.1x EAP
EAP method
PEAP
Phase 2 authentication
None
CA certificate
(unspecified)
User certificate
(unspecified)
Identity
josh
Anonymous identity

Cancel Save
Android

CA Configuration

peapshow

Security
802.1x EAP

EAP method
PEAP

Phase 2 authentication
None

CA certificate
(unspecifed)

Identity
josh

Anonymous identity

Cancel Save
Android

Inner Authentication

peapshow

Security

802.1x EAP

EAP method

PEAP

Phase 2 authentication

None

None

PAP

MSCHAP

MSCHAPV2

GTC

Cancel

Save
iOS

PEAP Configuration

![iOS PEAP Configuration Screen](image)
iOS

CA Configuration

Example Server Certificate

Not Verified

Description: Server Authentication
Expires: Jun 14, 2014, 10:41:17 AM

More Details
iOS

Cert Details

Subject Name

Country Name: FR
State or Province Name: Radius
Organization Name: Example Inc.
Common Name: Example Server...
Email Address: admin@example.com

Issuer Name

Country Name: FR
State or Province Name: Radius
BlackBerry
BlackBerry
EAP Types

![Wi-Fi Security Configuration](image)

- **Enterprise Sub-Type:**
  - PEAP
  - LEAP
  - EAP-TLS
  - EAP-FAST
  - EAP-TTLS
  - EAP-SIM
  - EAP-AKA

- **Username:**
- **Password:**
- **CA certificate:**
  - <None selected>

- **Inner link security:**
- **Token:**
  - <None selected>

- **Server subject:**
- **Server SAN:**

- **Disable Server Certificate Validation**

- **Options:**
  - Cancel
  - Connect
BlackBerry

PEAP Configuration

Manually Connect to Network

Security Type:
- WPA/WPA2 Enterprise

Enterprise Sub-Type:
- PEAP

Username:
Password:
CA certificate:
- <None selected>

Inner link security:
- AUTO

Token:
- <None selected>

Server subject:
Server SAN:

Disable Server Certificate Validation

Back  Save  Save and Connect
BlackBerry

CA Configuration

- Baltimore CyberTrust Root
- GTE CyberTrust Global Root
- Certicom MobileTrust RSA Root
- Entrust.net Secure Server CA
- Entrust.net CA (2048)
- Entrust.net Global Secure Server CA
- Entrust.net Client CA
- Entrust Root CA
- Equifax Secure Certificate Authority
- GeoTrust Global CA
- GeoTrust Universal CA
Windows Phone 8
Windows Phone 8

PEAP Configuration

Connecting to the secure WiFi network peapshow.

Username: josh.isec

Password: ************

Show password

Validate server certificate: Off

done  cancel
Windows Phone 8

CA Configuration

SIGN IN

Connecting to the secure WiFi network peapshow.

Username
josh.isec

Password

Show password

Validate server certificate
On

choose a certificate

details

done cancel
Windows Phone 8

Cert Details

CHOOSE A CERTIFICATE

com, microsoft, Microsoft Root
Microsoft Root Certificate Authority, valid until 9/5/2013

ZA, Western Cape, Durbanville
Thawte Timestamping CA, valid until 31/12/2020

Copyright (c) 1997 Microsoft
Microsoft Root Authority, valid until 31/12/2020

US, Washington, Redmond, WA
Microsoft Root Certificate Authority 2011, valid until 31/12/2020

US, MSFT, Microsoft Authenticode(tm) Root, expired 31/12/1999

US, Washington, Redmond, WA
Microsoft Root Certificate Authority 2010, valid until 31/12/2020

Copyright (c) 1999 Microsoft
Microsoft Test Root Authority, valid until 31/12/2020

Microsoft Trust Network, Microsoft
Microsoft Timestamp Root, expired 30/12/1999
Single Network

- Traditional attack
- Story time:
  - 50-100 users, shared building
  - > 1,000 users, campus
  - Extra credit
Multiple Networks

- Curated Lists
- Geographical, industry, other?
- Story time:
  - Industry
  - Geographical
  - Extra credit
All The Devices

- Everything (almost)
- Challenges
- Story time
Pwning 101

- Single target
- Multiple targets
Existing Tools

- FreeRADIUS-WPE
- hostapd & hostapd-wpe
- DD-WRT & OpenWrt
The Goal
What’s Next?

- *WRT scripts
- *WRT integration
- hostapd-python-script

---

5github.com/nims11/hostapd-python-script
Attacking PEAP

It’s Tool Time!

Getting Fancy

- Dynamic target selection
- GPS (wigle.net?)
- Single tool
How do we fix this?

Hide yo’ kids, hide yo’ WiFi
How do we fix this?

- EAP-TLS
- Better Mobile Device Management
### PEAP vs EAP-TLS

<table>
<thead>
<tr>
<th>Feature</th>
<th>PEAP</th>
<th>EAP-TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Nearly Universal</td>
<td>Nearly Universal</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Authentication</td>
<td>MSCHAPv2</td>
<td>Certificate</td>
</tr>
<tr>
<td>Easy to Configure</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Easy to Manage</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Josh Yavor (iSEC Partners)
Doing PEAP “Right”

- Mobile Device Management
- Custom CA vs Public CA
- Separate accounts
Doing PEAP “Right”
In order to access the DefCon Secured Wireless Network, please ensure you have the SecureTrust Root CA Chain certificate properly installed. In most modern browsers, this isn't an issue, but just in case, you can obtain the Root from:

https://ssl.trustwave.com/support/certificates/stca.crt
Victims Needed

Fair warning

- Turn off all of your WiFi devices if you do not wish to participate
- Targeting only DefConSecure
- No Man-in-the-Middle
- Username and MSCHAPv2 challenge/response collected
- Username and response displayed
- Brief Denial of Service
- Yes, I could crack your password later, but I know you didn’t reuse an important one (right?)
- I expect to capture only a handful, but maybe we’ll get lucky
Additional Resources


Thank Yous

- DEF CON
- iSEC Partners / NCC Group
- EFF
- The “victims”
Josh Yavor
Senior Security Engineer
iSEC Partners
https://www.isecpartners.com
@schwascore