The BYOD PEAP Show

Mobile Devices Bare Auth

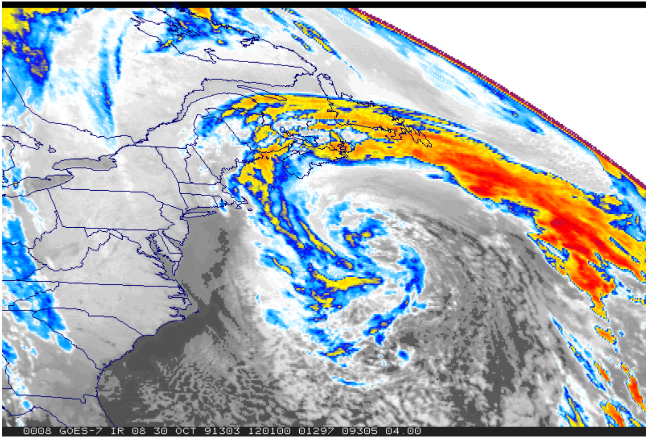
Josh Yavor

iSEC Partners

DEF CON XXI

August 4, 2013

A Perfect Storm



[1] noaa.gov

PEAP: Pwned Extensible Authentication Protocol

Joshua Wright & Brad Antoniewicz - ShmooCon 2008

> "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[1]

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

[1] `http://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

CloudCracker

Moxie Marlinspike, David Hulton, Marsh Ray - DEF CON XX

> “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, 2012[2]

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

[2] https://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
INSTRUCTOR
YOU'RE GONNA HAVE A BAD TIME
quickmeme.com

Bottom Line

Offense

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."[3]

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

Risk Characteristics

Lower Risk

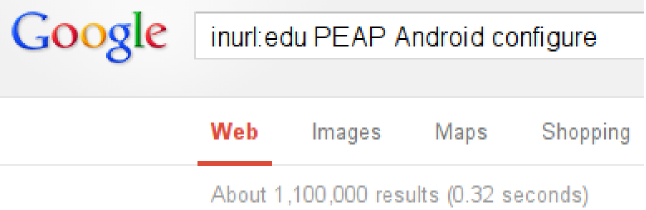
- Individual users (depends)
- Smaller organizations
- Static user base

Higher Risk

- Internal network assets
- Larger organizations
- Transient user base

Misconfiguration is Everywhere

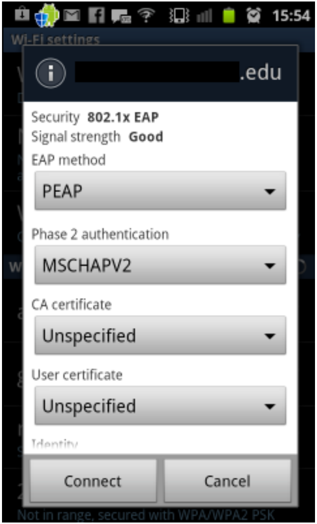
Be cruel to your school



inurl:edu PEAP Android configure

About 1,100,000 results (0.32 seconds)

For Mobile Devices



[redacted].edu

Security **802.1x EAP**

Signal strength **Good**

EAP method: PEAP

Phase 2 authentication: MSCHAPV2

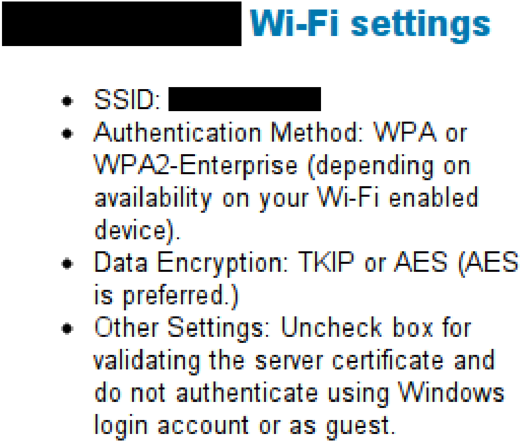
CA certificate: Unspecified

User certificate: Unspecified

Identity

Not in range, secured with WPA/WPA2 PSK

Even for Windows



[redacted] Wi-Fi settings

- SSID: [redacted]
- 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?

EAP Type Support				
	iOS	Android	Windows Phone 8	BlackBerry
PEAP	Yes	Yes	Yes	Yes
EAP-TLS	Yes	Yes	No	Yes
EAP-TTLS	Yes	Yes	No	Yes
EAP-FAST	Yes	No	No	Yes

Wireless Authentication Comparison

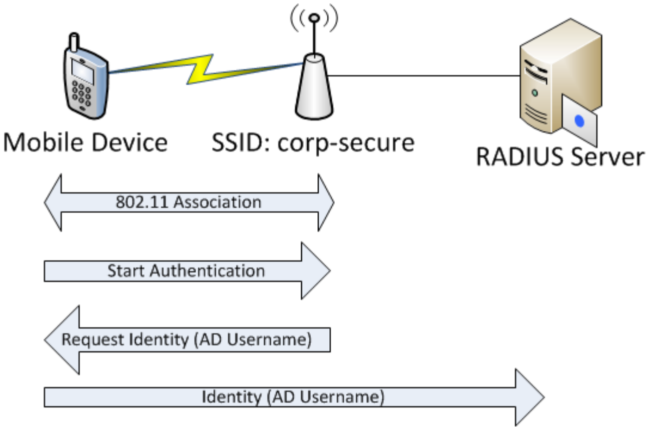
Access Control Granularity		
Open	**WPA2**	**WPA2 Ent.**
None	Group of users who know password	Individual user accounts
wifi? ok!	*getyourownwifi*	*evalDoer / 1337p455*

Wireless Authentication Comparison

Response to Credential Compromise		
Open	**WPA2**	**WPA2 Ent.**
N/A	Change password, update all devices	Modify single user account
wifi? ok!	*getyourownwifi2*	*Error: User account locked*

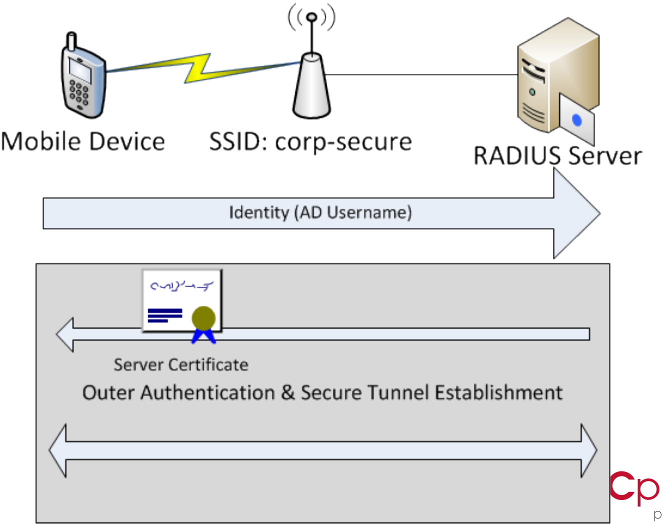
Association to AP

802.thisOneGoesTo11



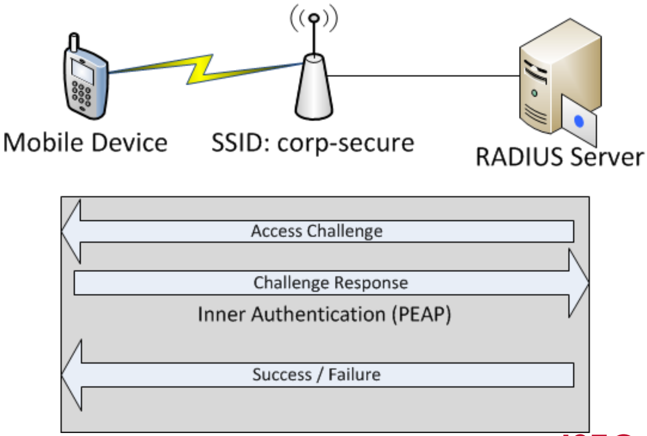
Outer Authentication

Thanks to Brad & Joshua



Inner Authentication with MSCHAPv2

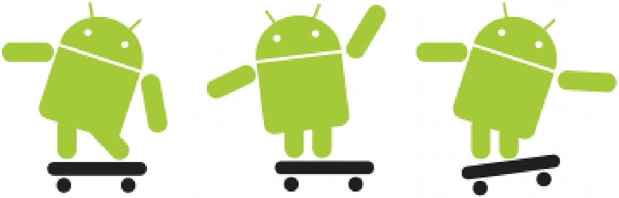
Thanks to Moxie



Mobile Platforms

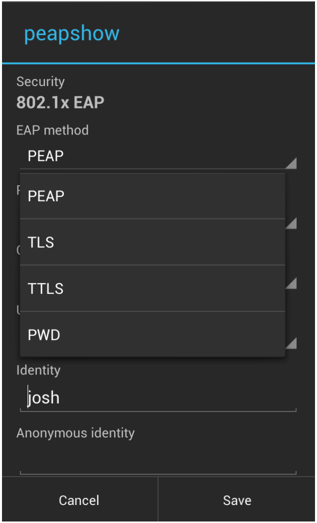
[2] ocio.osu.edu

Android



Android

EAP Types



peapshow

Security
802.1x EAP

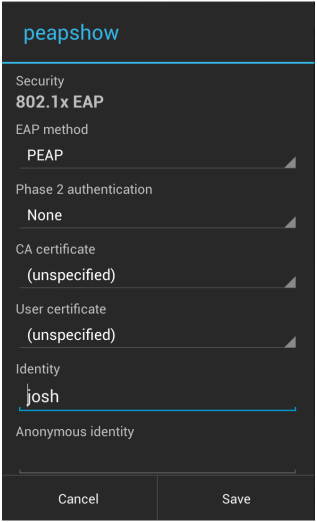
EAP method: PEAP

Identity: josh

Anonymous identity

Android

PEAP Configuration



peapshow

Security
802.1x EAP

EAP method
PEAP

Phase 2 authentication
None

CA certificate
(unspecified)

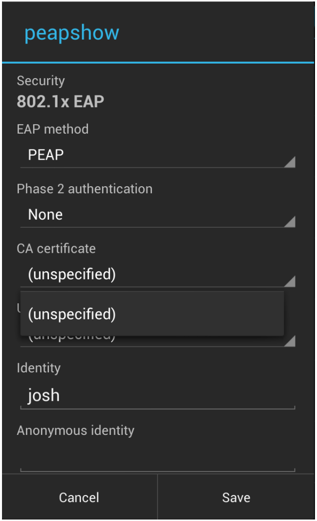
User certificate
(unspecified)

Identity
josh

Anonymous identity

Android

CA Configuration



peapshow

Security
802.1x EAP

EAP method
PEAP

Phase 2 authentication
None

CA certificate
(unspecified)

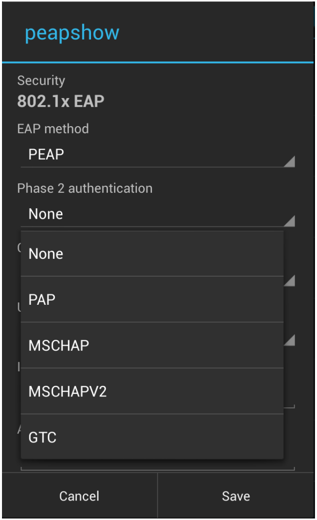
(unspecified)

Identity
josh

Anonymous identity

Android

Inner Authentication



peapshow

Security
802.1x EAP

EAP method
PEAP

Phase 2 authentication
None

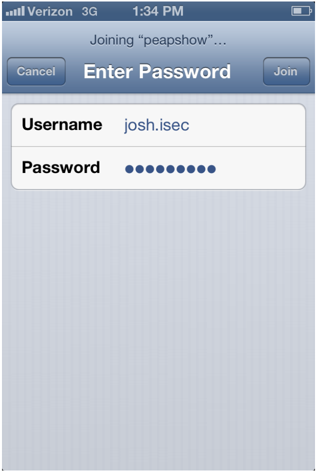
iOS

iSECpartners part of nccgroup

[3] apple.com

iOS

PEAP Configuration



Joining “peapshow”…

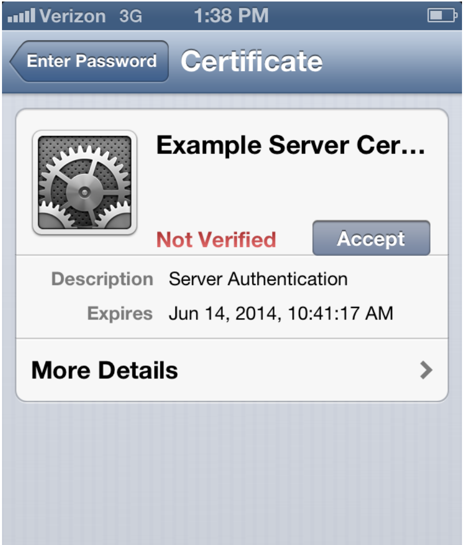
Enter Password

Username josh.isec

Password ●●●●●●●●●

iOS

CA Configuration



Verizon 3G 1:38 PM

Enter Password

Certificate

Example Server Cer...

Not Verified

Accept

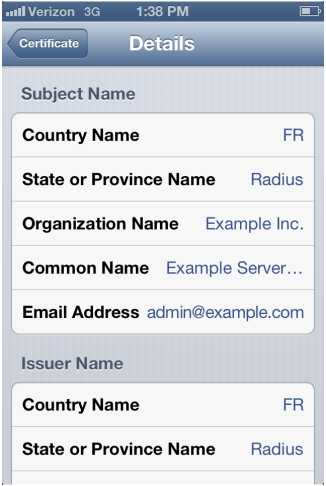
Description Server Authentication

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

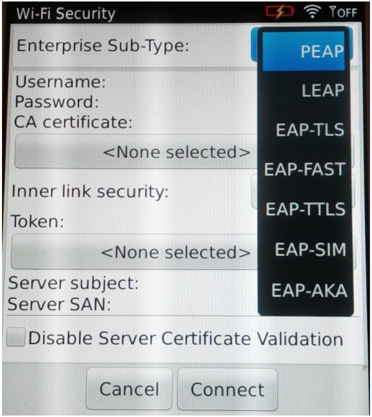
Issuer Name

Country Name	FR
State or Province Name	Radius

BlackBerry

BlackBerry

EAP Types



Wi-Fi Security

Enterprise Sub-Type: PEAP

Username:
Password:
CA certificate: <None selected>

Inner link security:

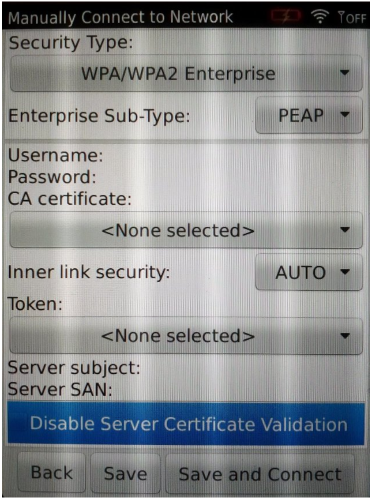
Token: <None selected>

Server subject:
Server SAN:

□ Disable Server Certificate Validation

BlackBerry

PEAP Configuration



Manually Connect to Network

Security Type: WPA/WPA2 Enterprise

Enterprise Sub-Type: PEAP

Username:
Password:
CA certificate: <None selected>

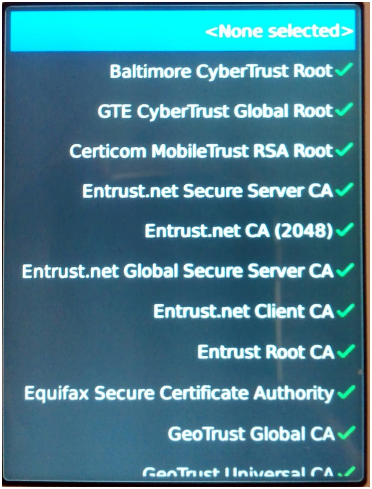
Inner link security: AUTO

Token: <None selected>

Server subject:
Server SAN:

BlackBerry

CA Configuration



<None selected>

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 ✓

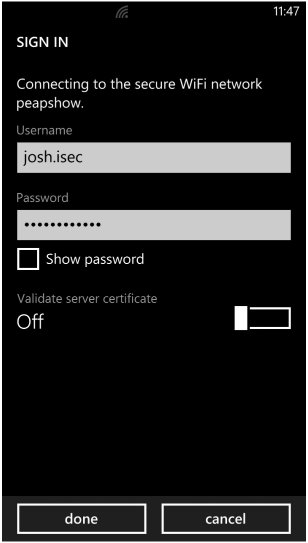
GeoTrust Universal CA ✓

Windows Phone 8

[4] microsoft.com

Windows Phone 8

PEAP Configuration



11:47

SIGN IN

Connecting to the secure WiFi network peapshow.

Username

josh.isec

Password

•••••••••••••

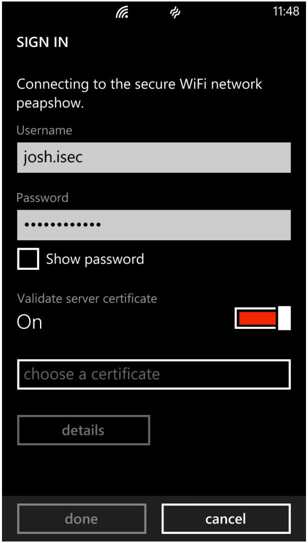
□ Show password

Validate server certificate

Off

Windows Phone 8

CA Configuration



11:48

SIGN IN

Connecting to the secure WiFi network peapshow.

Username: josh.isec

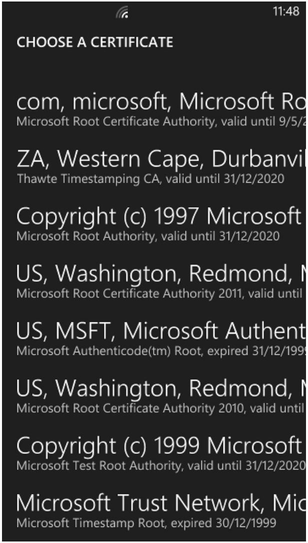
Password: •••••••••••••

□ Show password

Validate server certificate: On

Windows Phone 8

Cert Details



11:48

CHOOSE A CERTIFICATE

com, microsoft, Microsoft Ro
Microsoft Root Certificate Authority, valid until 9/5/2

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

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

US, Washington, Redmond, M
Microsoft Root Certificate Authority 2011, valid until

US, MSFT, Microsoft Authent
Microsoft Authenticode(tm) Root, expired 31/12/199

US, Washington, Redmond, M
Microsoft Root Certificate Authority 2010, valid until

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

Microsoft Trust Network, Mic
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

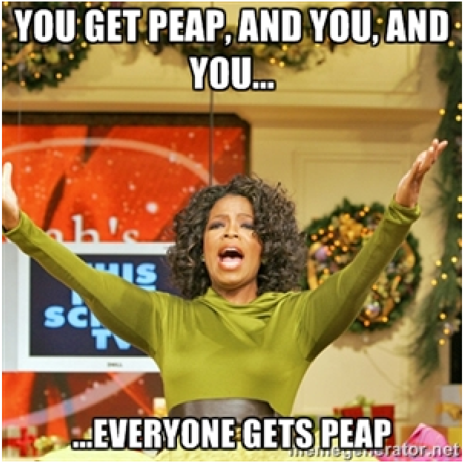
Pwning 101

- Single target
- Multiple targets

Existing Tools

- FreeRADIUS-WPE
- hostapd & hostapd-wpe
- DD-WRT & OpenWrt

The Goal


YOU GET PEAP, AND YOU, AND YOU...
...EVERYONE GETS PEAP
memegenerator.net

What's Next?

- *WRT scripts
- *WRT integration
- hostapd-python-script[5]

[5] github.com/nims11/hostapd-python-script

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

Feature	PEAP	EAP-TLS
Support	Nearly Universal	Nearly Universal
Server Authentication	Yes	Yes
User Authentication	MSCHAPv2	Certificate
Easy to Configure	Yes	No
Easy to Manage	Yes	No

iSECpartners
part of nccgroup

Doing PEAP "Right"

- Mobile Device Management
- Custom CA vs Public CA
- Separate accounts

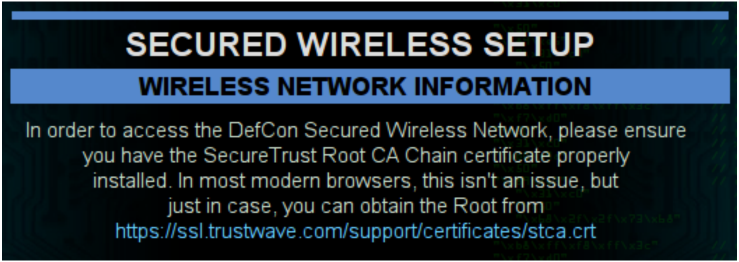
Doing PEAP “Right”

23 August 2010 © 2000 - Warner Bros. Entertainment, Inc.

23 August 2010 © 2000 - Warner Bros. Entertainment, Inc.

DefConSecure

Hacking the hackers



SECURED WIRELESS SETUP

WIRELESS NETWORK INFORMATION

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

- **Windows Phone 8 WiFi Configuration Guide** - http://www.windowsphone.com/en-US/how-to/wp8/start/connect-to-a-wi-fi-network
- **Apple iOS WiFi Deployment Guide** - http://images.apple.com/iphone/business/docs/iOS_6_Wifi_Sept12.pdf
- **Smart Phone WiFi Certifications** - http://certifications.wi-fi.org/search_products.php?search=1&lang=en&filter_category_id=24&listmode=1
- **Android WPA2 Enterprise UI Bug** - https://code.google.com/p/android/issues/detail?id=1386

Thank Yous

- DEF CON
- iSEC Partners / NCC Group
- EFF
- The “victims”

Josh Yavor
Senior Security Engineer
iSEC Partners
`https://www.isecpartners.com`
`@schwascore`