BYO-Disaster

Why Corporate Wireless Still Sucks!
We’re just nerds with random ideas and inconsistent results!
### Why you should stay!

<table>
<thead>
<tr>
<th>What</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain Clear-Text credentials from any PEAP enabled WPA2-Enterprise Network without cracking a single HASH.</td>
<td>Explore a “Functionality Issue” discovered with how IOS / OSX devices process MSChapV2.</td>
</tr>
<tr>
<td>Get access to a new set of tools that automates all the attacks for you.</td>
<td>Demonstrate the use of EAP-GTC as the inner authentication mechanism in place of MSChapV2</td>
</tr>
</tbody>
</table>
Client Responds with MS-ChapV2 hash and Peer Challenge
Accept Password Anyway
Server Sends TLV-Success
No Password in database
Peer Challenge does not match
Uh, what?
Fine, why not
Client Responds TLV-Success
IPWNER
Reject Password
Client Checks for Captive Portal
Attacker Responds with Captive Portal
Server Challenges Client
Client Responds Challenge
Server checks password in database
Server Challenges Client
Client Responds TLV-Success
Client Checks for Captive Portal
Attacker Responds with Captive Portal
Status: **Connected**

Wi-Fi is connected to joshiepooooo and has the IP address 192.168.10.7.

**Network Name:** joshiepooooo

- **Ask to join new networks**
  Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

**802.1X:** Default

- **Authenticating via PEAP (MSCHAPv2)**
- **Connect Time:** 00:01:21
Now that the MITM is complete, we can direct all DNS requests to our captive portal page and capture credentials in Clear-Text!
What Just Happened?

- IOS/OSX supplicants do not appear to require MSChapV2 success when connecting to the wireless network. So much for mutual authentication.
- Bypassing inner authentication.
- Establishing a MITM connection.
- Trapping captive portal requests by default, and redirect it to our malicious portal.
- User re enters credentials which are now captured in clear-text. Hackers Win again!
“After examining your report we do not see any actual security implications. It is the responsibility of the client to ensure that they are communicating with a trusted server before attempting the MSCHAPv2 inner authentication.

(The server could just as well have suggested the EAP-GTC protocol, after which the client would have provided its password in cleartext as the server instructed.)”
EAP Method created by Microsoft/Cisco for use with PEAPv1

Created to support hardware token cards and one time passwords

Similar to PEAPv0 EAP-MSCHAPv2 with no peer challenge

Some clients do not state what type of password they are asking for, they just prompt for a username and password

Can we use this to our advantage?
Client Responds with "GTC" password

Server Sends TLV-Success anyway

GTC fails

No password for user

Sure I trust you, why not?

Client Responds TLV-Success

Server Requests one-time password

PEAPINGTOM

Full connection established

Sure I trust you, why not?

Full connection established
Hi, welcome to the DefConSecure network or, more realistically, its evil twin. Time to change that password. Want to know why? Track 1, 4pm, Saturday.
Clear-Text Anyone?

Thanks Radius, it was awesome of you to put clear text passwords in your debug file!
Attack works on devices that support PEAPv1-GTC natively.

- IOS/OSX
- Android (does not prompt for cert, NEAT!)
- *n?x works in Ubuntu but does require user setup
- Windows – safe for now, no native support

No captive portal required, MITM attack is trivial and includes clear text passwords

Instant capture of MSCHAPv2 passwords on IOS devices after user accepts certificate from evil twin.
Things You Need!

• Host system
  • *Ubuntu 12.04*
• Wi-Fi Adapter
  • *Alfa AWUS051NH*
• Radius Patch
  • *PuNk1n.patch*
• HAVOC-APPS
  • *LootBooty Wi-Fi Tools*
A historical perspective

- Cracking hashes is too hard
- Can we trick the client into just giving it to us?
- What if radius accepted everything?
- Started with past work from other attacks.
- Unexpected discoveries