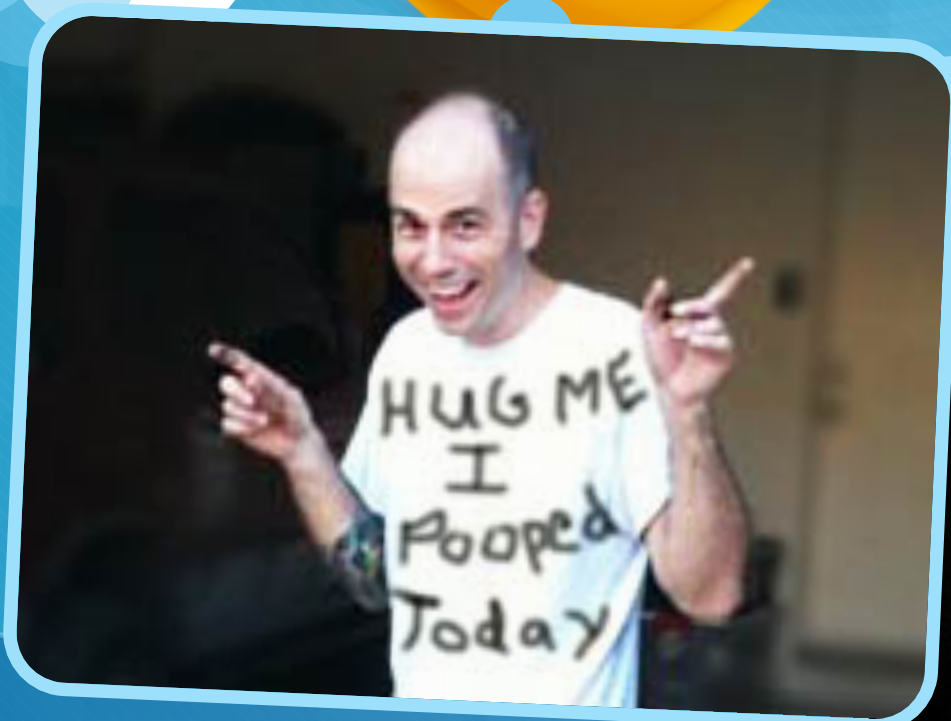


DefCon 2013

BYO-Disaster

Why Corporate Wireless Still Sucks!



djwishbone



PuNk1nPo0p

We're just nerds with random ideas and inconsistent results!

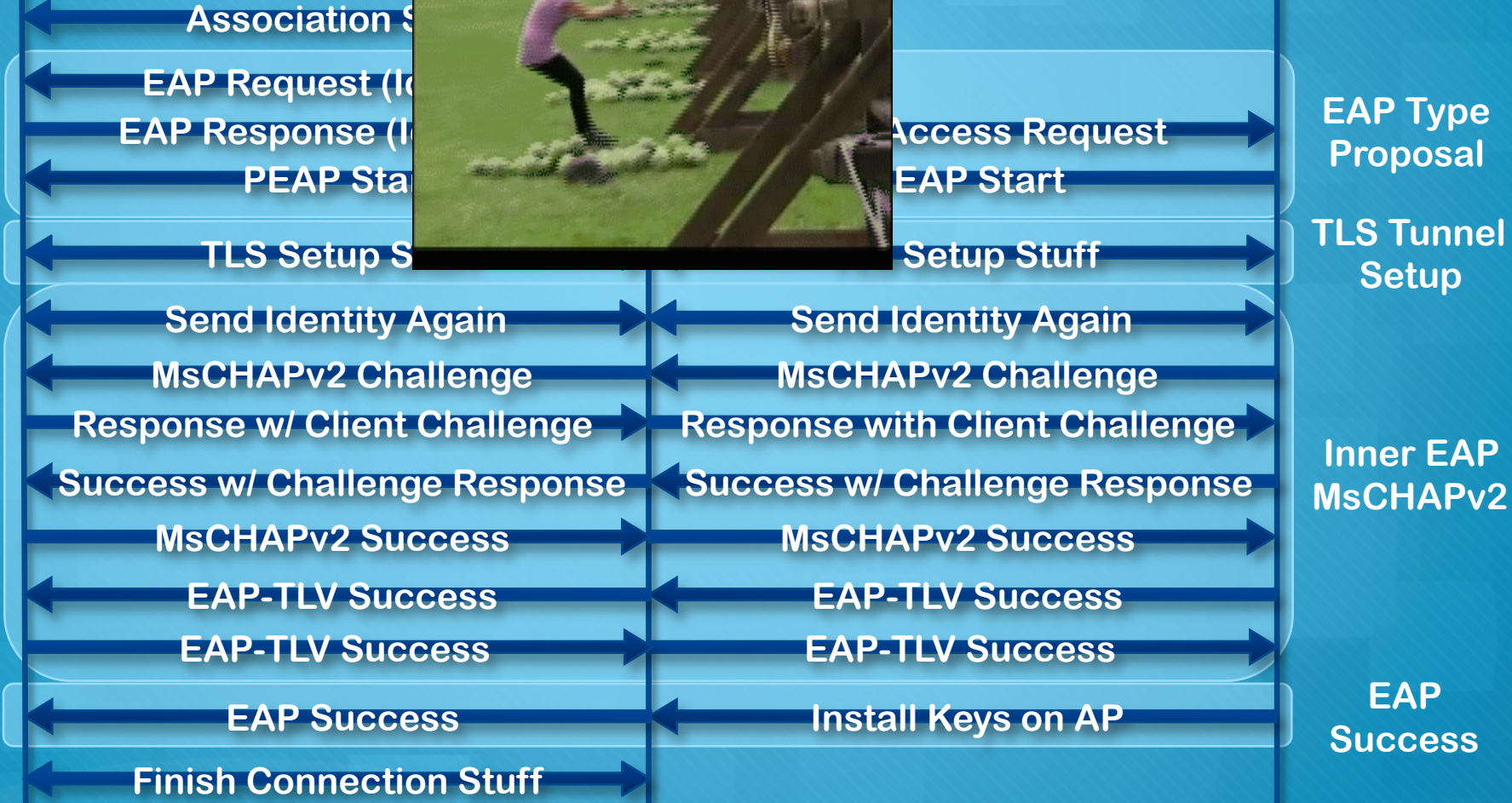
Why you should stay!

What

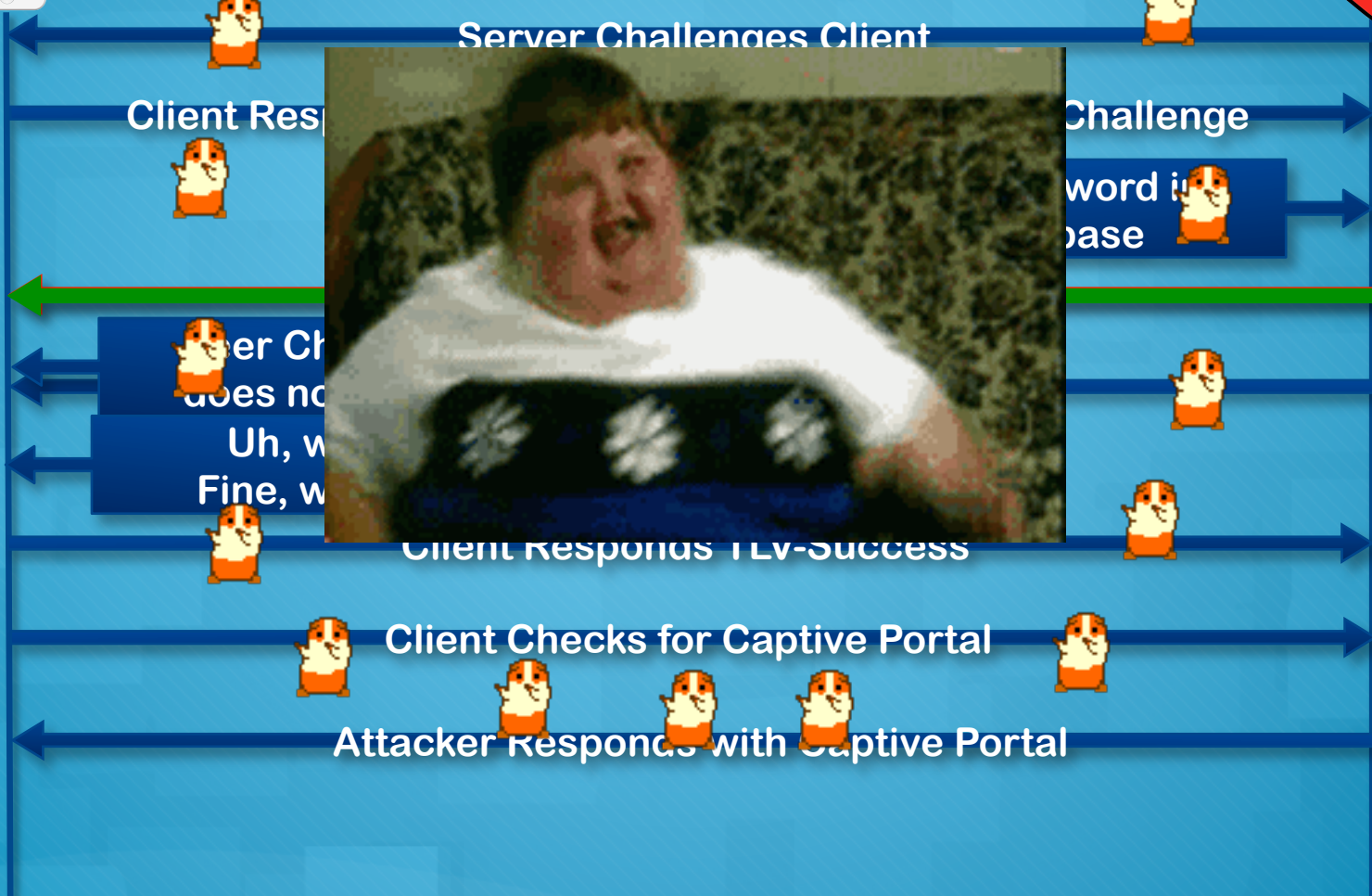
- Obtain Clear-Text credentials from any PEAP enabled WPA2-Enterprise Network without cracking a single HASH.
- Get access to a new set of tools that automates all the attacks for you.

How

- Explore a “Functionality Issue” discovered with how IOS / OSX devices process MSChapV2.
- Demonstrate the use of EAP-GTC as the inner authentication mechanism in place of MSChapV2



IPWNER



Server Challenges Client

Client Responds

Challenge

Server Challenge does not pass

Uh, what? Fine, what?

Client Responds TLV-Success

Client Checks for Captive Portal

Attacker Responds with Captive Portal

No Service

Enter Passw



Descripti

Expir

More De

Status: **Connected**

Turn Wi-Fi Off

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

Network Name: joshiepooooo

Ask to join new networks

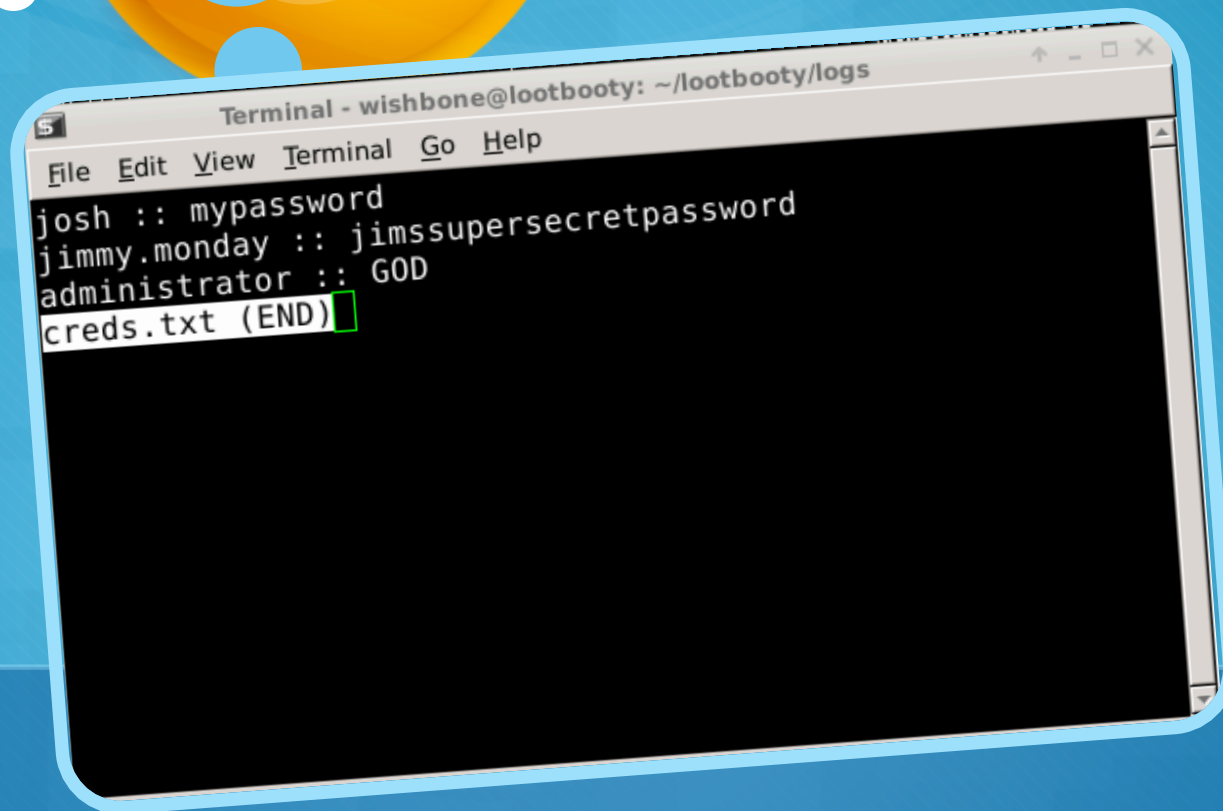
Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

802.1X: Default

Disconnect

Authenticated via PEAP (MSCHAPv2)
Connect Time: 00:01:21

Cancel

A terminal window titled "Terminal - wishbone@lootbooty: ~/lootbooty/logs" is shown. The window has a menu bar with "File", "Edit", "View", "Terminal", "Go", and "Help". The terminal output shows the following lines:

```
josh :: mypassword
jimmy.monday :: jimssupersecretpassword
administrator :: GOD
creds.txt (END)
```

The text "creds.txt (END)" is highlighted with a green box. The terminal window is set against a blue background with stylized white and yellow clouds.

Clear-Text Anyone?

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 network, even though it is required for mutual authentication.
- Bypassing inner authentication.
- Establishing a MITM connection.
- Trapping captive portal requests by default, and redirect it to our server.
- User re enters credentials which are captured in clear-text. Hackers Win again!



Responsible Disclosure

hahaha, funny!

“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.)”



GENERIC TOKEN CARD

- 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?

PEAPINGTOM



Server Requests one-time password

Client Responds with "GTC" password

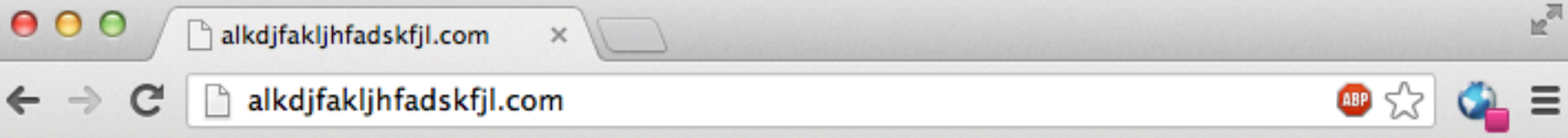
GTC fails
password for user

Server says
away

Sure I trust
why not

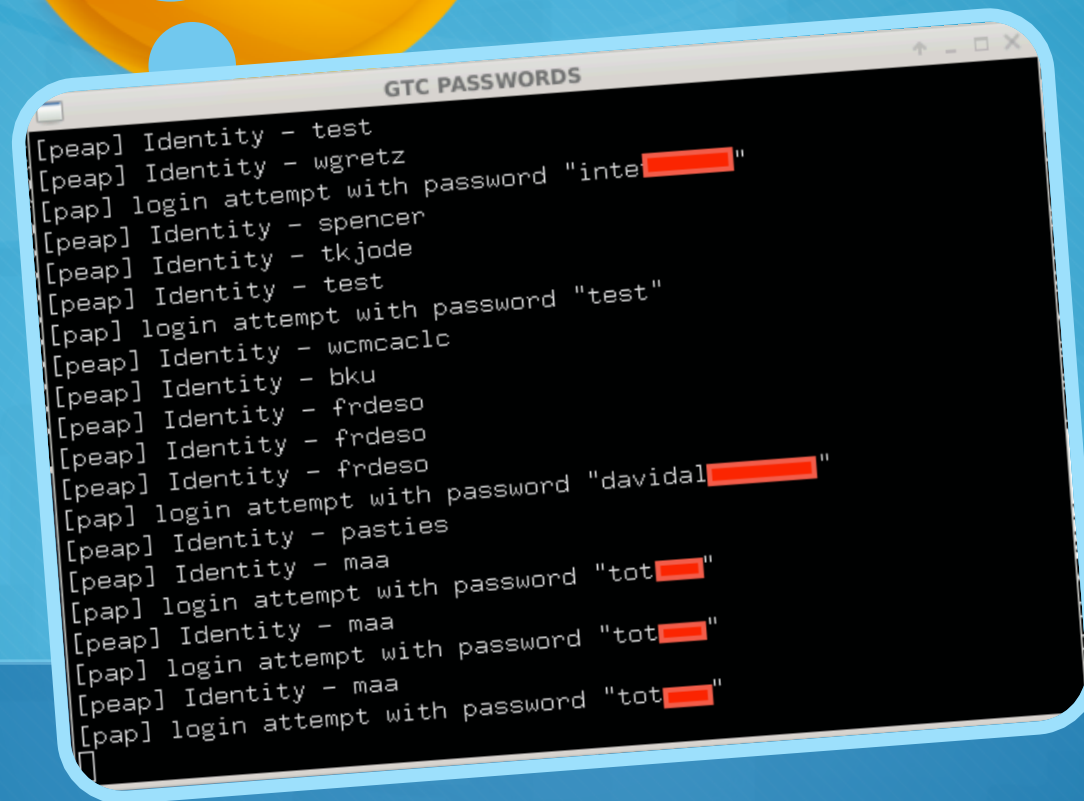
Full connection
established





Hi, welcome to the DefConSecure network or, more realistically, its evil twin. Time to chnge that password. Want to know why? Track 1, 4pm, Saturday.





```
GTC PASSWORDS
[peap] Identity - test
[peap] Identity - wgretz
[pap] login attempt with password "inte[REDACTED]"
[peap] Identity - spencer
[peap] Identity - tkjode
[peap] Identity - test
[pap] login attempt with password "test"
[peap] Identity - wcmcaclc
[peap] Identity - bku
[peap] Identity - frdeso
[peap] Identity - frdeso
[peap] Identity - frdeso
[pap] login attempt with password "davidal[REDACTED]"
[peap] Identity - pasties
[peap] Identity - maa
[pap] login attempt with password "tot[REDACTED]"
[peap] Identity - maa
[pap] login attempt with password "tot[REDACTED]"
[peap] Identity - maa
[pap] login attempt with password "tot[REDACTED]"
```

Clear-Text Anyone?

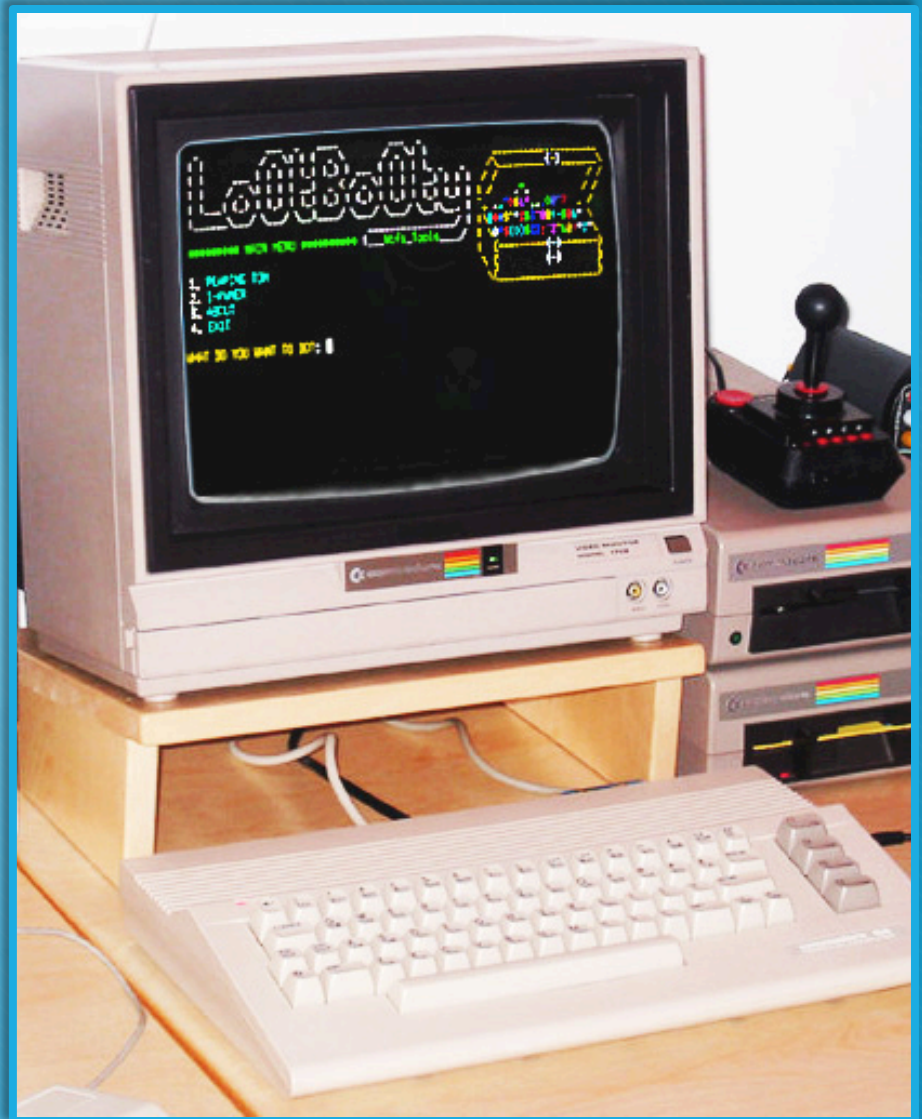
Thanks Radius, it was awesome of you to put clear text passwords in your debug file!

GTC Attack – PEAPingtom

- 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.

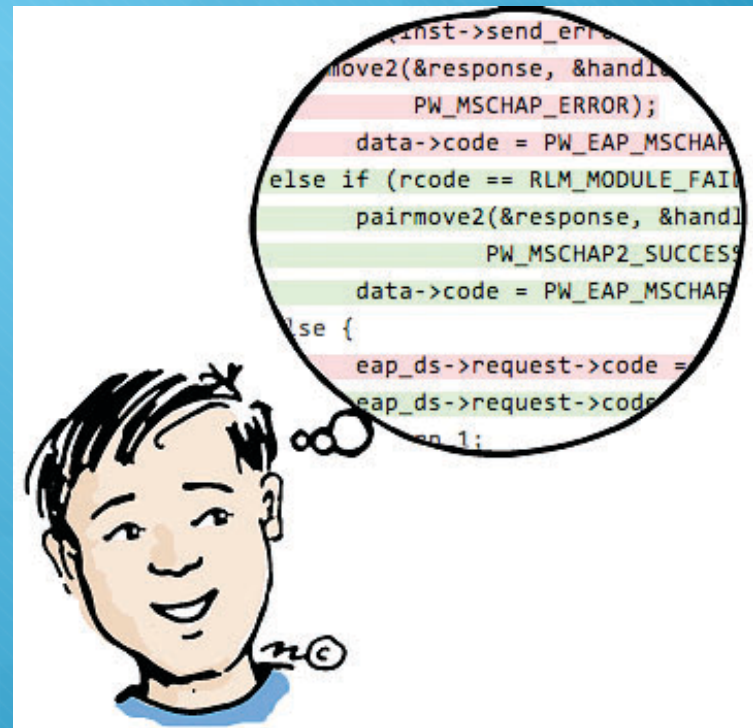
Things You Need!

- 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





www.LootBooty.com

Thank You!