Capturing WPA2 Enterprise credentials with a Pi

Richard Frovarp
Principal Software Engineer
North Dakota State University

Standard disclaimer

What I say is my own opinion and not that of my employer

Why a Pi and not a Pineapple?

$35 < $Pineapple

Everything described will work on a Pineapple, and possibly work better.

Types of WPA2

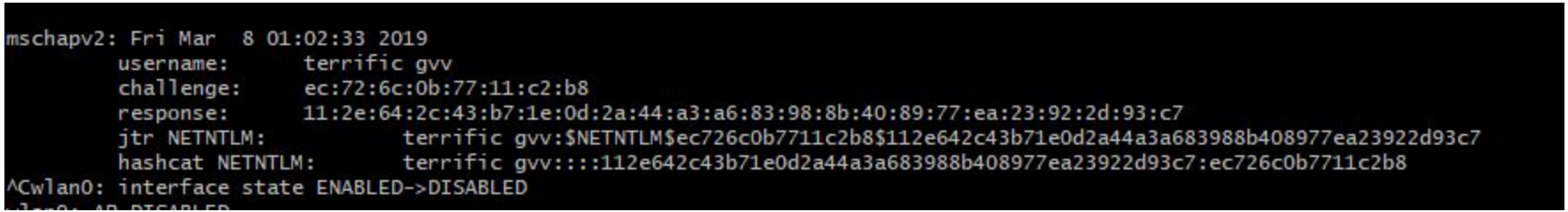
- Personal
  - PSK (PreShared Key) that is the same between devices
  - Exceedingly common at home and consumer devices
  - Some systems can do per MAC PSK, but it using Personal mechanisms
- Enterprise
  - For when you want each user to use their own credentials
    - Much easier to manage who has access across the enterprise. One person leaves, just revoke their credential and don't have to update every other device with new PSK.
  - Credential typically takes two forms:
    - Username and password, frequently against an enterprise directory like OpenLDAP or AD
    - x509 certificates

WPA2 Enterprise credentials

- x509 requires PKI to sign certificates
  - However, since it is just a cert, you can't compromise standard directory credentials
- Username and password
  - Can we perhaps compromise the password?

hostapd-wpe

- Install Kali on your favorite Pi. 3B's are the easiest, 3B+ and 4's require additional hardware
- sudo apt install hostapd-wpe
  - This time OpenSSL isn't lying when it says that it will take a while
- kill dhcp
  - watch out for this
- Maybe edit the SSID
- Launch, and watch credentials come in


mschapv2: Fri Mar 8 01:02:33 2019
username: terrific gvv
challenge: ec:72:6c:0b:77:11:c2:b8
response: 11:2e:64:2c:43:b7:1e:0d:2a:44:a3:a6:83:98:8b:40:89:77:ea:23:92:2d:93:c7
jtr NETNTLM: terrific gvv:$NETNTLM$ec726c0b7711c2b8$112e642c43b71e0d2a44a3a683988b408977ea23922d93c7
hashcat NETNTLM: terrific gvv::::112e642c43b71e0d2a44a3a683988b408977ea23922d93c7:ec726c0b7711c2b8
^Cwlan0: interface state ENABLED->DISABLED

Method being attacked

- Targeting PEAP using MSCHAPv2
  - MSCHAPv2 was state of the art for Windows 98 / NT 4.0 SP 4
  - PEAP from 2005

Abstracted process

- Device looks for the SSID
- Sends anonymous identity in the plain to connected RADIUS system
- Is connected with end RADIUS responsible for account
- TLS session is created between device and end RADIUS
- Identity is sent in plain and creds are sent in MSCHAPv2 format

hostapd-wpe

- Acts as the destination RADIUS
- Gets username and creds

```
mschapv2: Fri Mar  8 01:02:33 2019
         username:      terrific gvv
         challenge:     ec:72:6c:0b:77:11:c2:b8
         response:      11:2e:64:2c:43:b7:1e:0d:2a:44:a3:a6:83:98:8b:40:89:77:ea:23:92:2d:93:c7
         jtr NETNTLM:           terrific gvv:$NETNTLM$ec726c0b7711c2b8$112e642c43b71e0d2a44a3a683988b408977ea23922d93c7
         hashcat NETNTLM:       terrific gvv::::112e642c43b71e0d2a44a3a683988b408977ea23922d93c7:ec726c0b7711c2b8
^Cwlan0: interface state ENABLED->DISABLED
```

asleap

- Developed 2004 by Joshua Wright
- We end up with control of the random value
- Protocol DES encrypts same number three times using NTLM hash
- 16 byte NT hash is split into 7 + 7 + 2
  - Third DES is 2^16 possible permutations
- Dictionary search

Defenses

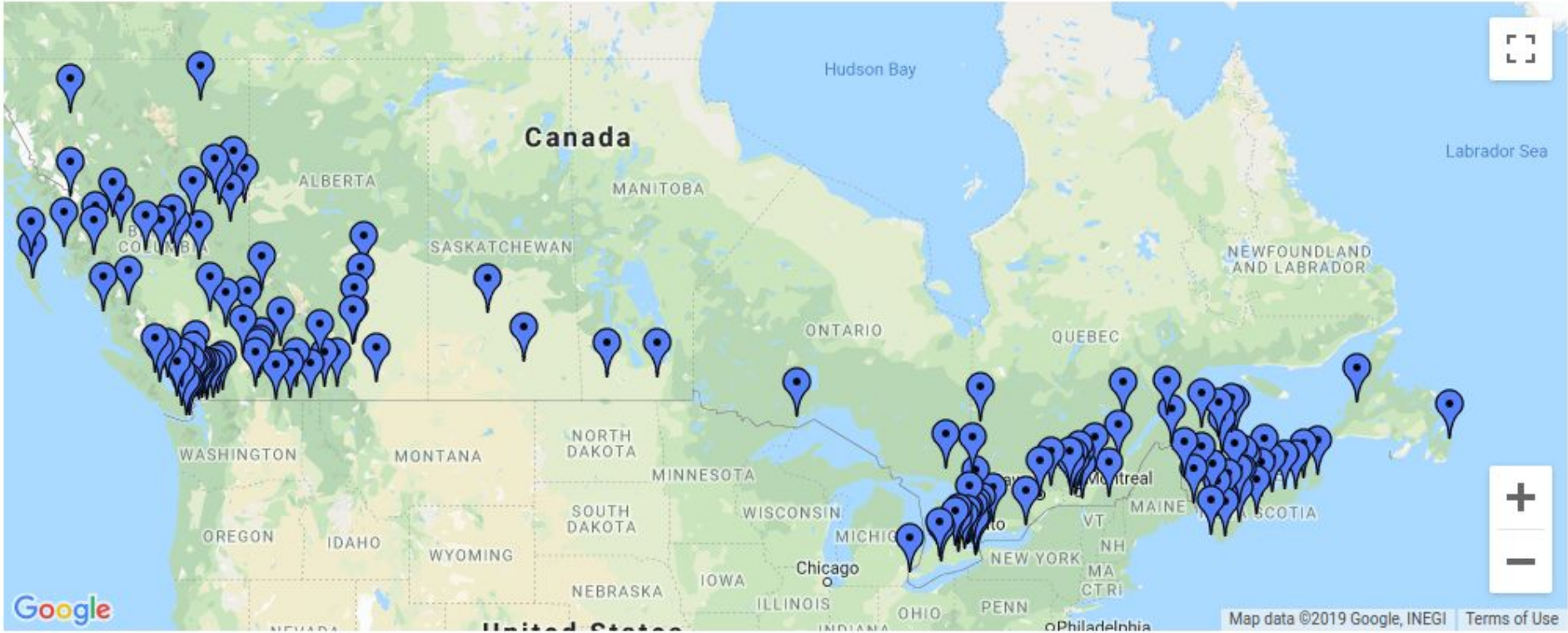
- Run EAP-TLS

Pin RADIUS certificate

- Clients can be configured to validate the identity of the RADIUS system by checking their certificate.
- Apple devices do this by default by requiring that you accept the cert the first time you connect
- However….
  - Sure you could figure out social engineer an Apple user to accept the new cert.
  - It's REALLY easy to setup a device using PEAP. While you may be good, there's nothing stopping a user from setting it up on their phone without your help.
- So really only a partial solution

EAP-TLS

- Secure, but difficult to support
- You need PKI infrastructure to generate and sign certificates
- Apple devices need a profile, which actually works out quite nicely for install.
- Windows and Android devices are more complicated
- Sometime devices are locked down and can't get the custom certificates to join the network
- Android appeared to be all over the place: sometimes it worked, sometimes it didn't. Updates would break it.


Hudson Bay
Canada
Labrador Sea
ALBERTA
MANITOBA
SASKATCHEWAN
NEWFOUNDLAND AND LABRADOR
ONTARIO
QUEBEC
WASHINGTON
MONTANA
NORTH DAKOTA
MINNESOTA
SOUTH DAKOTA
WISCONSIN
MAINE
OREGON
IDAHO
WYOMING
NEBRASKA
IOWA
ILLINOIS
OHIO
PENN
NEW YORK
VT
NH
MA
CT
RI
Chicago
Philadelphia
Google
Map data ©2019 Google, INEGI
Terms of Use

eduroam federation

GÉANT project of entities in 101 territories to allow students, faculty, and staff connect to wireless across the globe.

Challenge

- Lots and lots of devices.
- We see about 11k devices a day

Thanks

See https://frovarp.dev for slides and updates.