# RFC 8110 - Opportunistic Wireless Encryption

Some background information…

# History...

## draft-wkumari-owe - "OWE: Opportunistic Wireless Encryption"

- Originally documented in 2015  by Wes George and myself.
- Use WPA2-PSK with key == SSID
    - SSID: Starbucks -> PSK: Starbucks

- Example implementations:
    - HostAPd:  Add ‘`vendor_elements=dd05646a740100`’ to /etc/hostapd/hostapd.conf on Pi
    - OpenWRT:

```
#This adds the OWE 802.11 Vendor Specific Information Element to the beacon frames.
append bss_conf "# OWE: Opportunistic Wireless Encryption - draft-wkumari-owe" "$N"
append bss_conf "vendor_elements=dd05646a740100"  "$N"
```

# History...

## draft-wkumari-owe:

Q5: Doesn't this belong in [ IEEE | WiFi Alliance | <insert other SDO here> ] ?

A: Answer unclear, ask again later. I have discussed this with a number of people who participate in other SDOs, and it seems like the IETF is the best home for it, at least for now. It does not require changes to any underlying transport, it does not change any standards, it simply takes advantage of work done in other standards bodies.

# Dan Harkins and I tried to take it to IEEE…

- https://mentor.ieee.org/802.11/dcn/15/11-15-1128-01-0wng-owe.ppt

- https://mentor.ieee.org/802.11/dcn/15/11-15-1184-05-000m-owe.docx

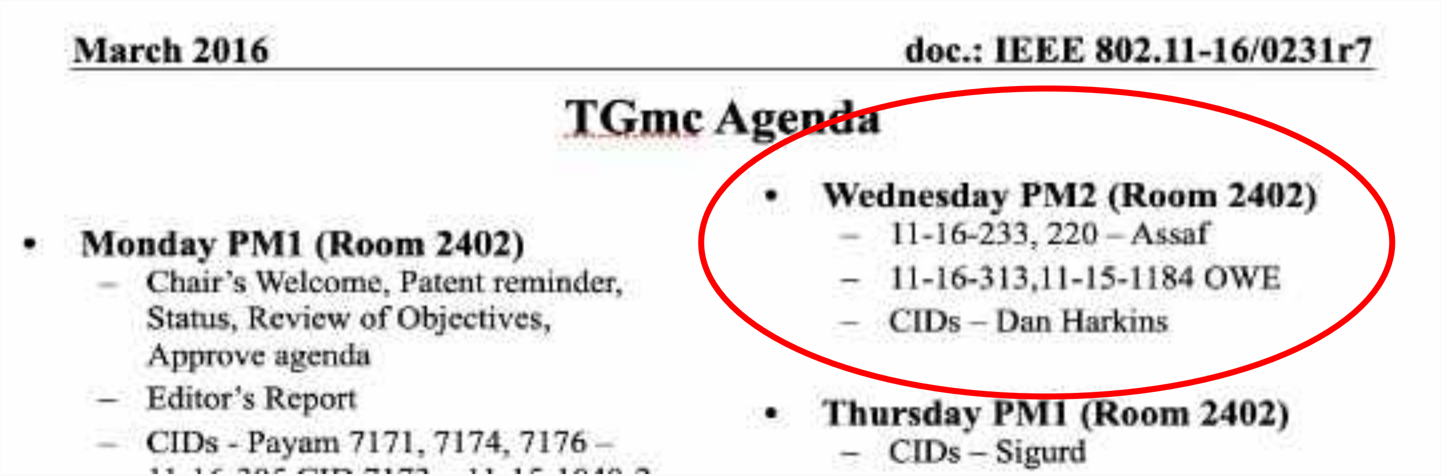
- https://mentor.ieee.org/802.11/dcn/16/11-16-0313-01-000m-the-benefits-of-opportunistic-wireless-encryption.pptx

- And many, many other documents…
- … many presentations…

# Dan Harkins and I tried to take it to IEEE…

- On the TGmc Agenda (March 2016)

https://mentor.ieee.org/802.11/dcn/16/11-16-0231-07-000m-tgmc-agenda-march-2016.pptx



March 2016 doc.: IEEE 802.11-16/0231r7

## TGmc Agenda

- **Monday PM1 (Room 2402)**
  - Chair's Welcome, Patent reminder, Status, Review of Objectives, Approve agenda
  - Editor's Report
  - CIDs - Payam 7171, 7174, 7176 –

- **Wednesday PM2 (Room 2402)**
  - 11-16-233, 220 – Assaf
  - 11-16-313,11-15-1184 OWE
  - CIDs – Dan Harkins

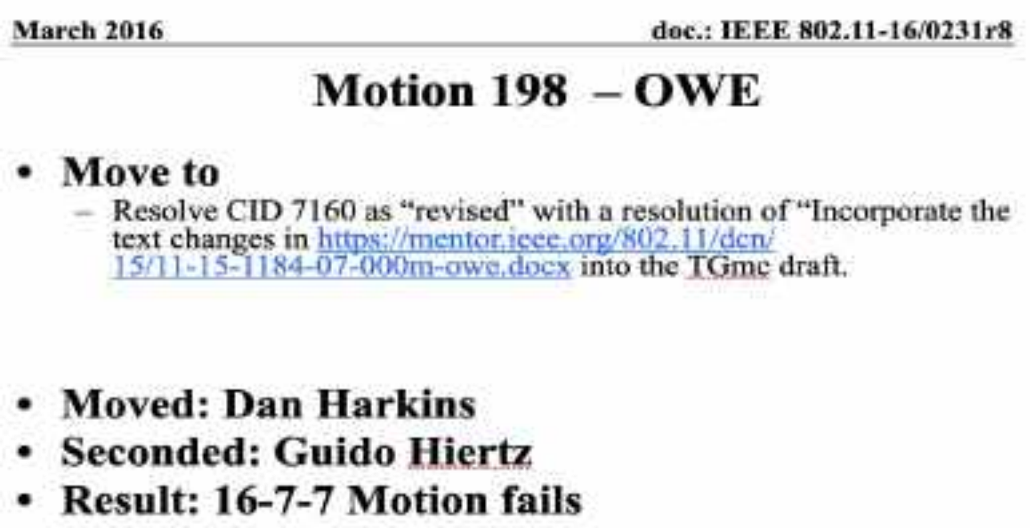
- **Thursday PM1 (Room 2402)**
  - CIDs – Sigurd

# Bad things happened...

# Dan Harkins and I tried to take it to IEEE…

- TGmc Agenda March 2016 - 17-Mar-2016 07:14:45 ET

  https://mentor.ieee.org/802.11/dcn/16/11-16-0231-08-000m-tgmc-agenda-march-2016.pptx



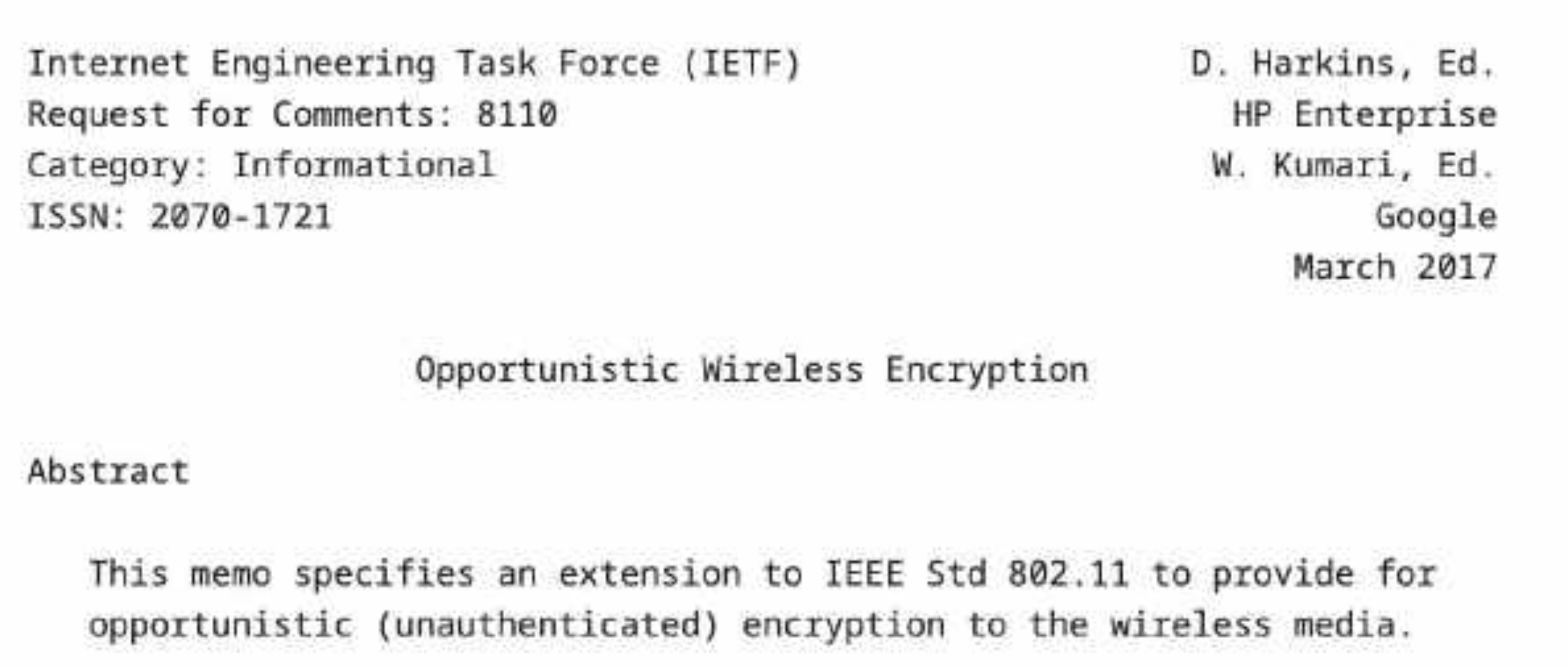
March 2016 doc.: IEEE 802.11-16/0231r8

## Motion 198 – OWE

- Move to
  - Resolve CID 7160 as "revised" with a resolution of "Incorporate the text changes in https://mentor.ieee.org/802.11/dcn/15/11-15-1184-07-000m-owe.docx into the TGmc draft.

- Moved: Dan Harkins
- Seconded: Guido Hiertz
- Result: 16-7-7 Motion fails

# So we took it back to the IETF…



Internet Engineering Task Force (IETF)
Request for Comments: 8110
Category: Informational
ISSN: 2070-1721

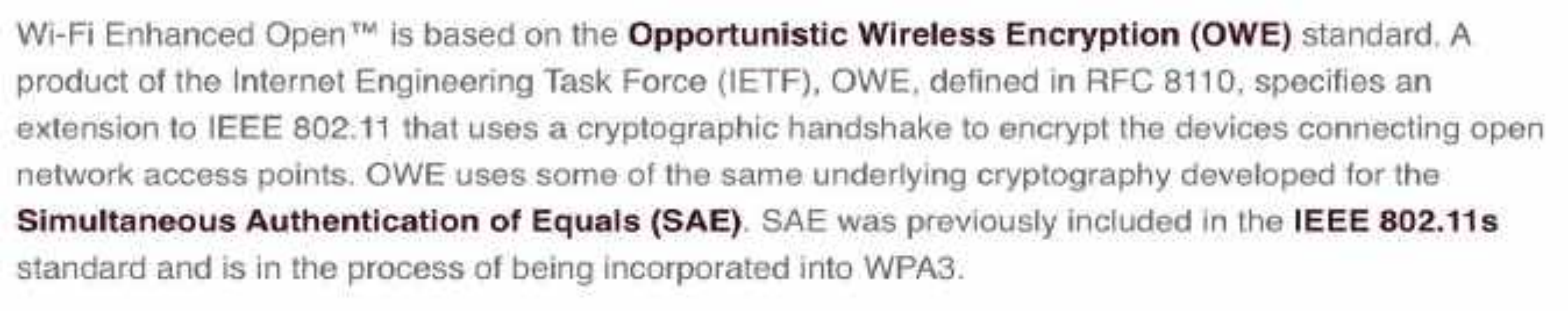
D. Harkins, Ed.
HP Enterprise
W. Kumari, Ed.
Google
March 2017

Opportunistic Wireless Encryption

Abstract

This memo specifies an extension to IEEE Std 802.11 to provide for opportunistic (unauthenticated) encryption to the wireless media.

# Deployment…



Wi-Fi Enhanced Open™ is based on the **Opportunistic Wireless Encryption (OWE)** standard. A product of the Internet Engineering Task Force (IETF), OWE, defined in RFC 8110, specifies an extension to IEEE 802.11 that uses a cryptographic handshake to encrypt the devices connecting open network access points. OWE uses some of the same underlying cryptography developed for the **Simultaneous Authentication of Equals (SAE)**. SAE was previously included in the **IEEE 802.11s** standard and is in the process of being incorporated into WPA3.

- From Feb 2020:
- Android
- iOS
- Cisco
- Aruba
- [ ...]

# If IEEE wants to take it over…

- Peter Yee (IEEE 802.11/IETF liaison representative) received request IEEE 802.11's TGme (the IEEE 802.11 maintenance group) asking:
  1) Would RFC 8110  be better incorporated into IEEE 802.11:
  2) Would I be ok with that?
  3) What would the process be / timing
     a) make it historic in IETF first??
     b) My personal view: If this were to happen, we do a joining RFC8110bis, saying that we are all friends and working together…

But, before any of that, can an unencumbered technology developed in an open SDO like the IETF be moved into an SDO with different licencing regimes?