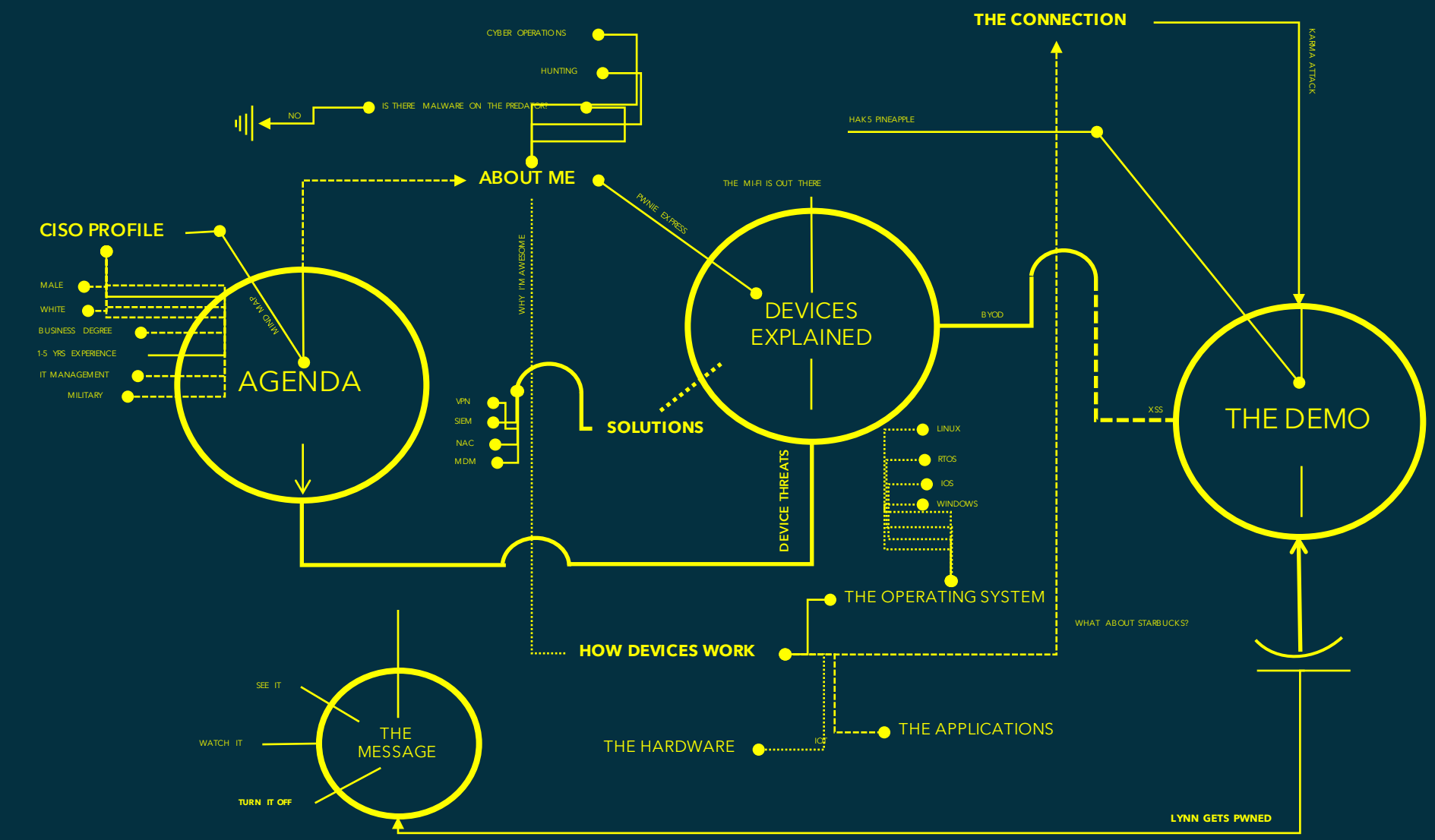
THE NEW DEVICE THREAT LANDSCAPE

Risks & Mitigations

Yolonda N. Smith

THE GAME PLAN



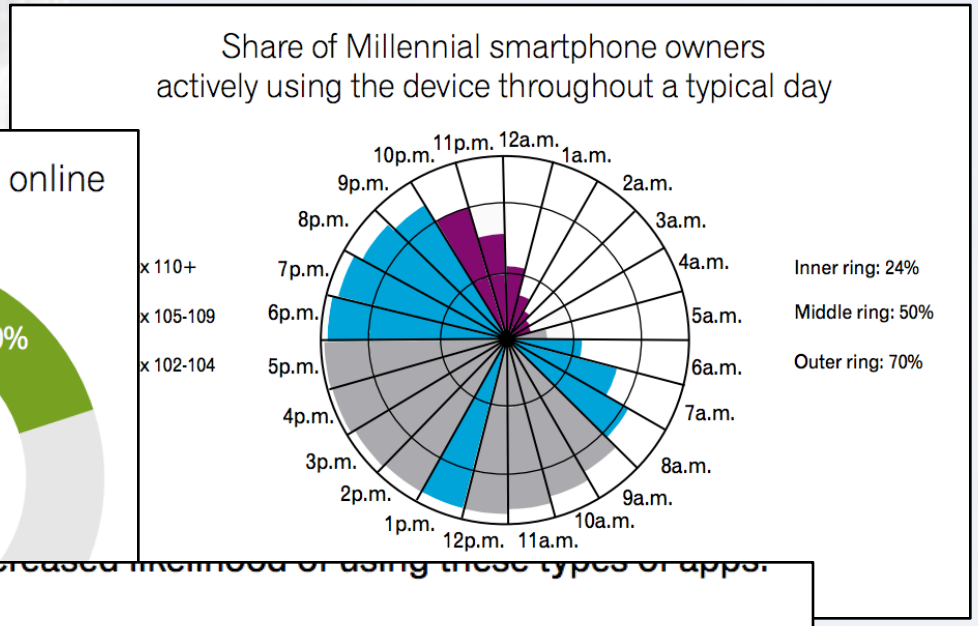
#hackEWF

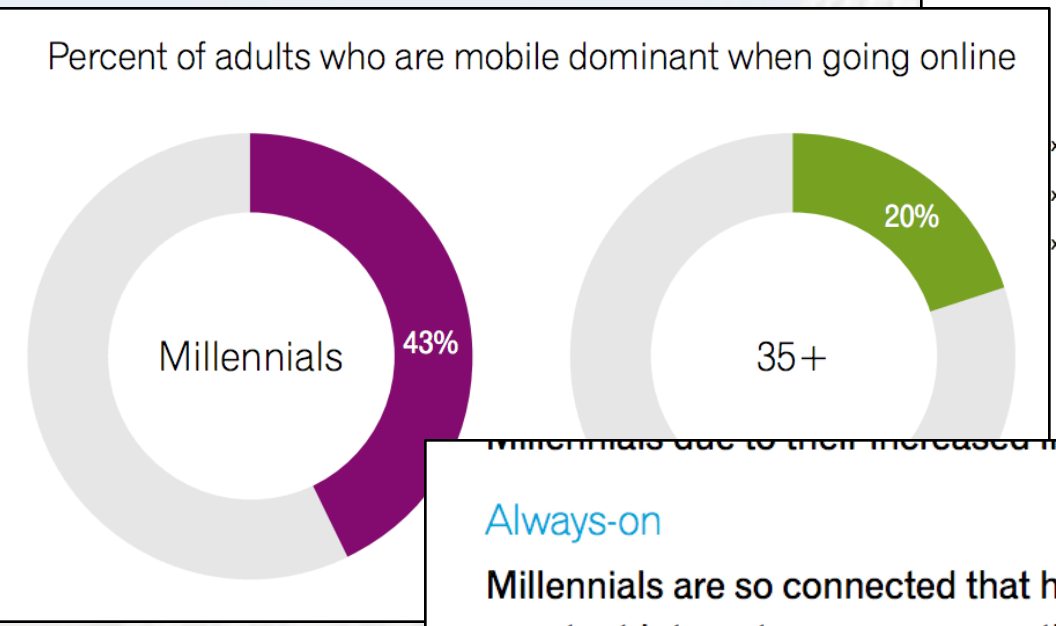
Yolonda in 1 Slide

#hackEWF

MILLENNIAL MENACE

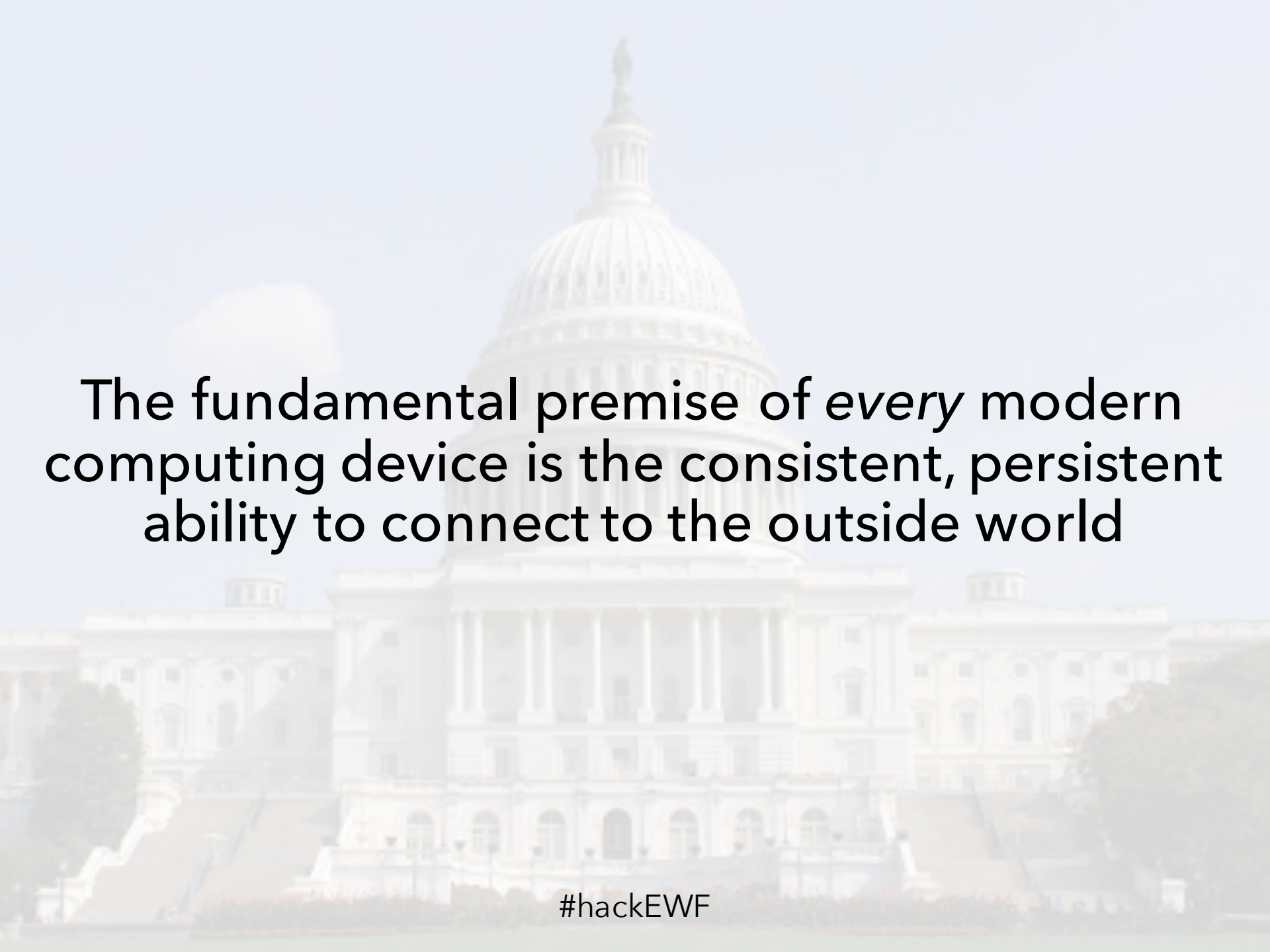
The Connected Workforce





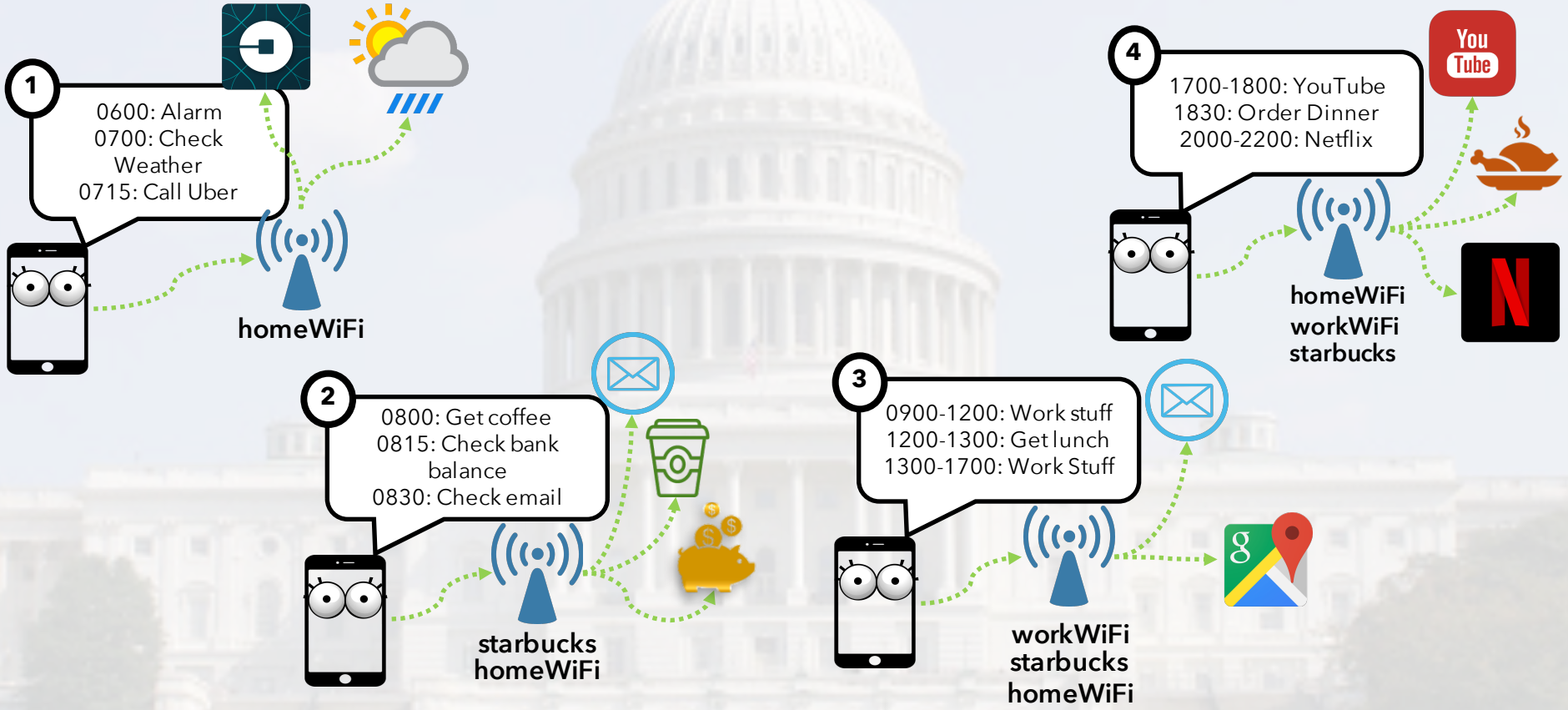
Always-on

Millennials are so connected that half (50 percent) say that they need constant Internet access even on-the-go (compared with 38 percent of all adults). Smartphones are a natural solution to this need and 43 percent of Millennials say that they now access the Internet more through their phone than through a computer compared with just 20 percent of adults ages 35 and older. Hispanic Millennials are even more likely to be mobile dominant with 46 percent accessing the Internet more through their phone than a computer.

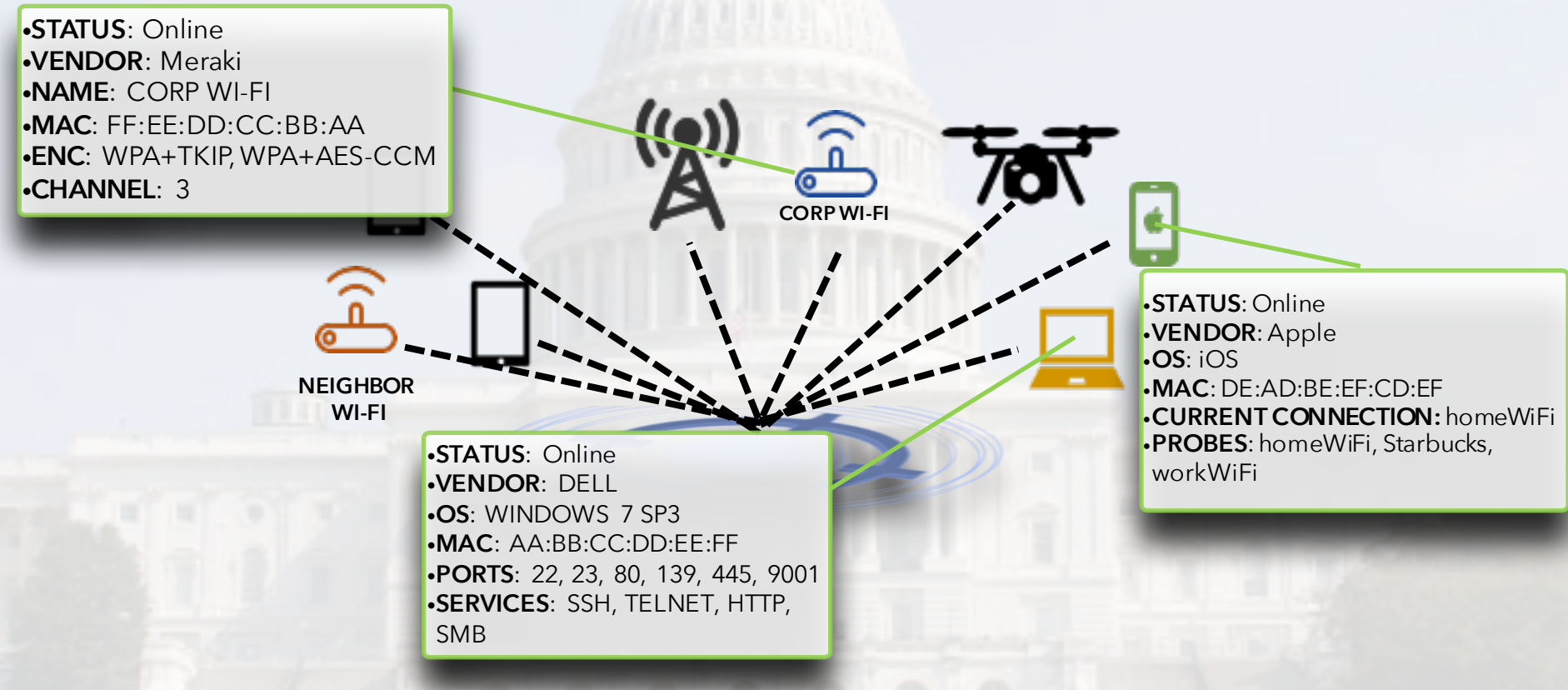


The fundamental premise of *every* modern computing device is the consistent, persistent ability to connect to the outside world

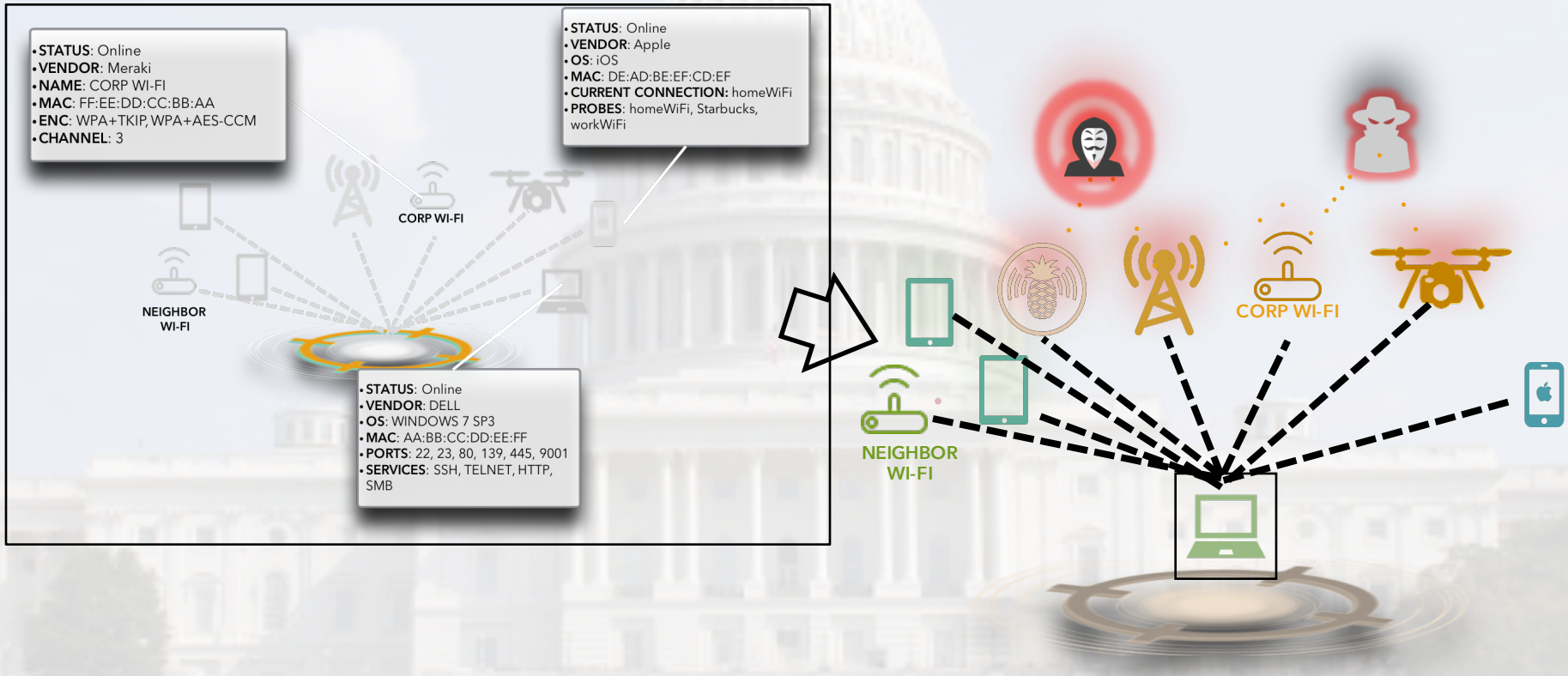
A Day in the Life of Your Device



Our Devices Are Talking…What Are They Saying?



Good Things Talk to Bad Things



Doesn’t my VPN Save Me?

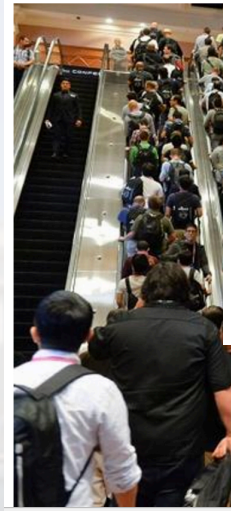
Home / Security Watch / First Look at a Wi-Fi Attack Happening at Black Hat Right Now

First Look at a Wi-Fi Attack Happening at Black Hat Right Now

BY MAX EDDY AUGUST 4, 2016 10:49AM EST 10 COMMENTS

How bad could it be?

0 SHARES

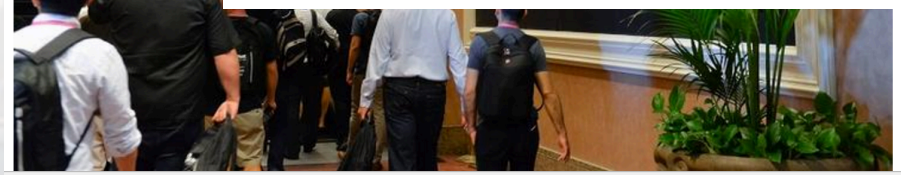


ReadandShare · 2 months ago

@Max Eddy, who wrote, "if som… has co… f t… access point, they can decrypt your traffic, monitor it, and then pass it along t… …ded destination with you being none the wiser."

As an individual user, I don't care too much if people snooped my browsing CNN and PCMag. But when emailing (Android Chrome browser using HTTPS) or banking (bank app also encrypted) -- my understanding is that the snooper will just get a bunch of gibberish. You say they can decrypt. But if indeed they can decrypt HTTPS traffic - don't we have a far, far bigger problem worldwide than just an insecure Wifi?

NO



//MOST POPULAR ARTICLES

Crypto Wars: Why the Fight to Encrypt Rages On

…Xbox One Tips and

//DISCOVER...

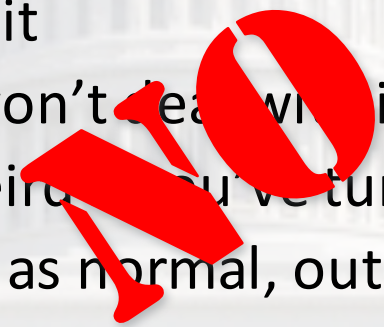
The Biggest Software Flops of All Time

The Eerie World of Abandoned Arcade Games

#hackEWF

Yeah, but I have Anti-Virus…

- Client-side attacks start off-network against known-good devices & can circumvent basic controls
  - Anti-virus won't catch it
  - Policy Orchestration won't [illegible] it
  - SIEM may think it's weird [illegible] tuned it correctly
  - Firewalls will look at it as normal, outbound traffic



PROVE IT!

#hackEWF

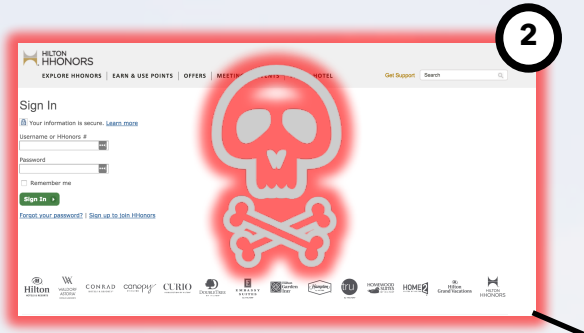
This is a targeted attack, done with the permission and discretion of EWF. The specific exploits and tools presented here were acquired, purchased & configured for demonstration purposes only against *a specific, designated device*. No other devices were targeted as part of this exercise, so if your laptop stops working it wasn't me, okay? Just turn off your Wi-Fi to be on the safe side.

You ***should not*** attempt to do this without expressed, written permission of the granting authority .

DISCLAIMER

#hackEWF

Constructing the Attack



2

4

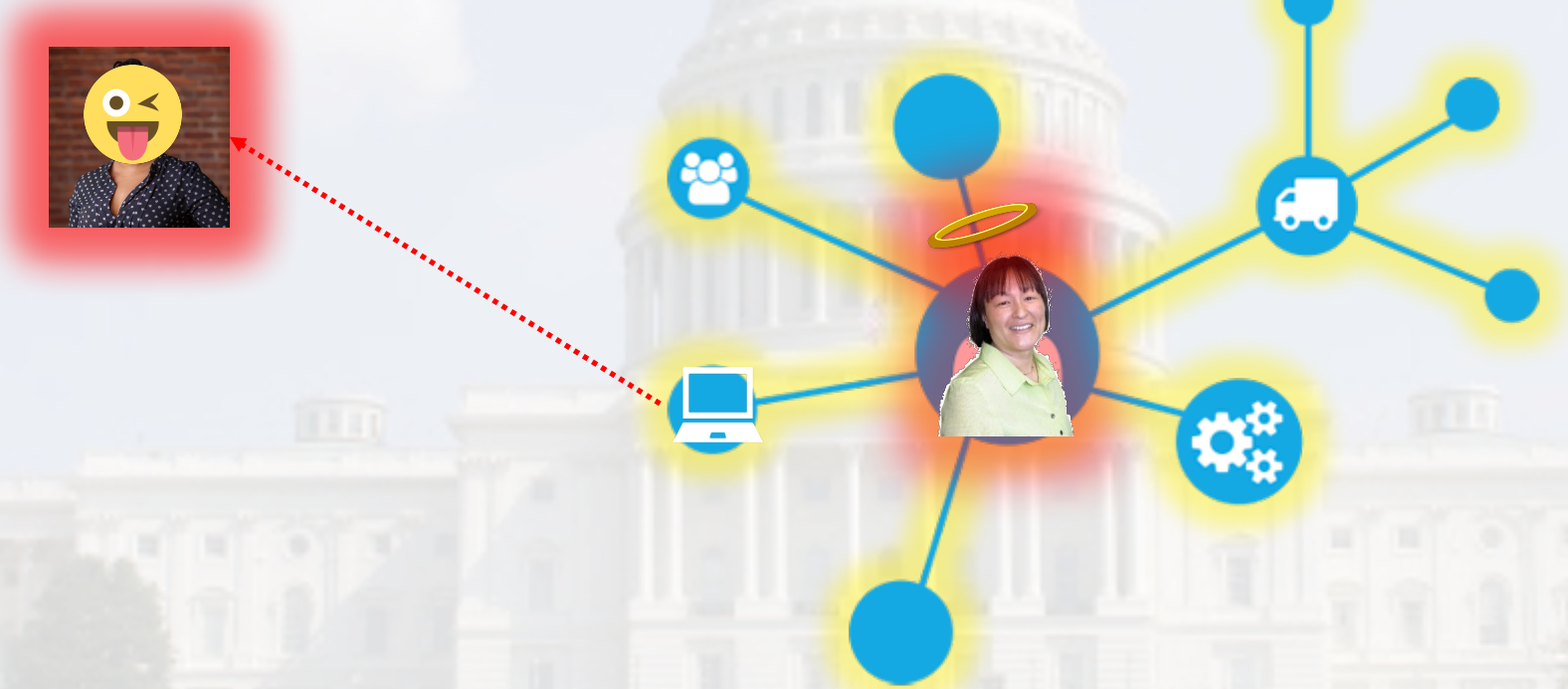
1

3 Credential Grabbing

Objectives
1. Snag Credentials
2. Drop backdoor on laptop
3. Gain access to privileged networks & data

#hackEWF

Impact to the Organization



Tools of the Attack

- Hak5 Pineapple Nano - ~$100 USD
- Kali Linux (Rolling) & Associated Tools
- Social Engineering Toolkit
- Metasploit
- Windows 10 Virtual Machine (for testing)
- Various cables, chords
- Lots of candy to keep me motivated

Total cost of this attack: $150 + 2 hours

For the purposes of this demonstration, we were intentionally heavy handed and obvious with the tools, payloads and delivery mechanism to show each part of the attack.

In reality there are ***many*** sophisticated & stealthy ways to evade detection & quarantine.

Check out Mass Mailer, Spearphishing attacks from SET (@HackingDave, Trusted Sec)

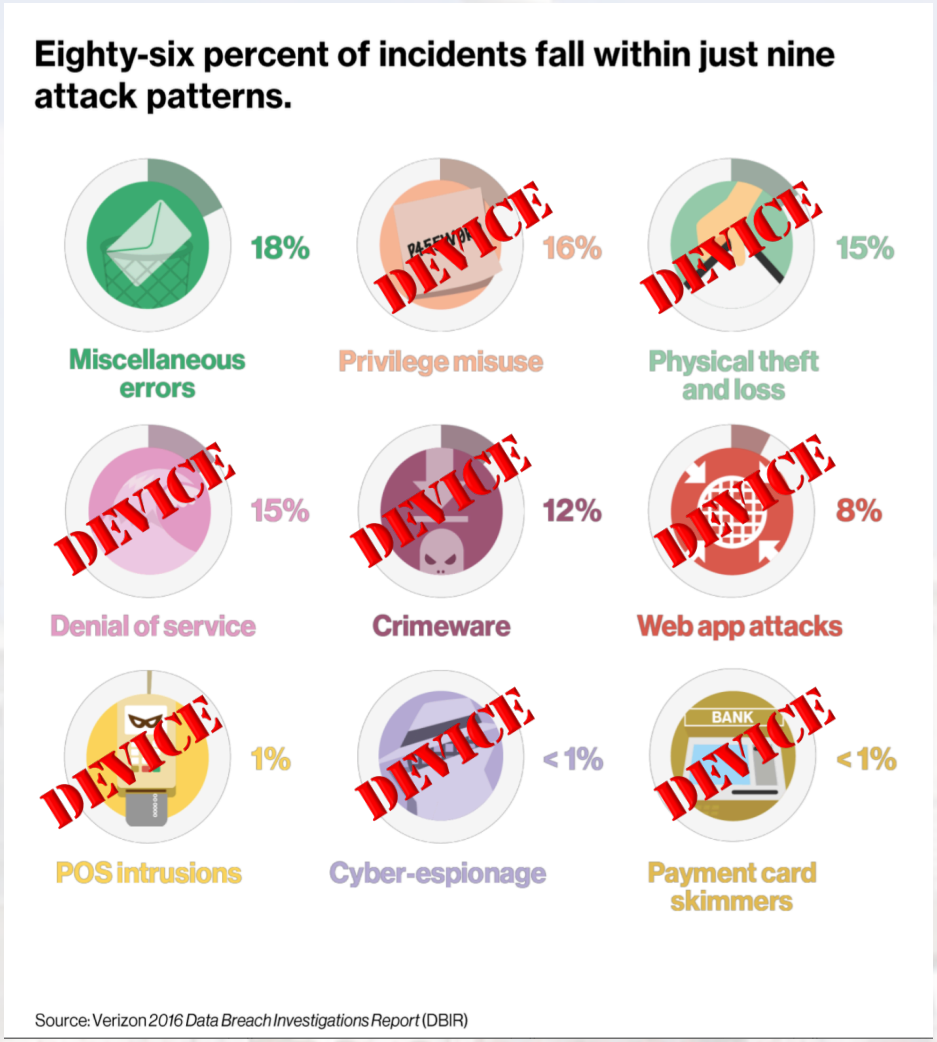
VEIL Framework (by @harmj0y)

DISCLAIMER

THE MESSAGE

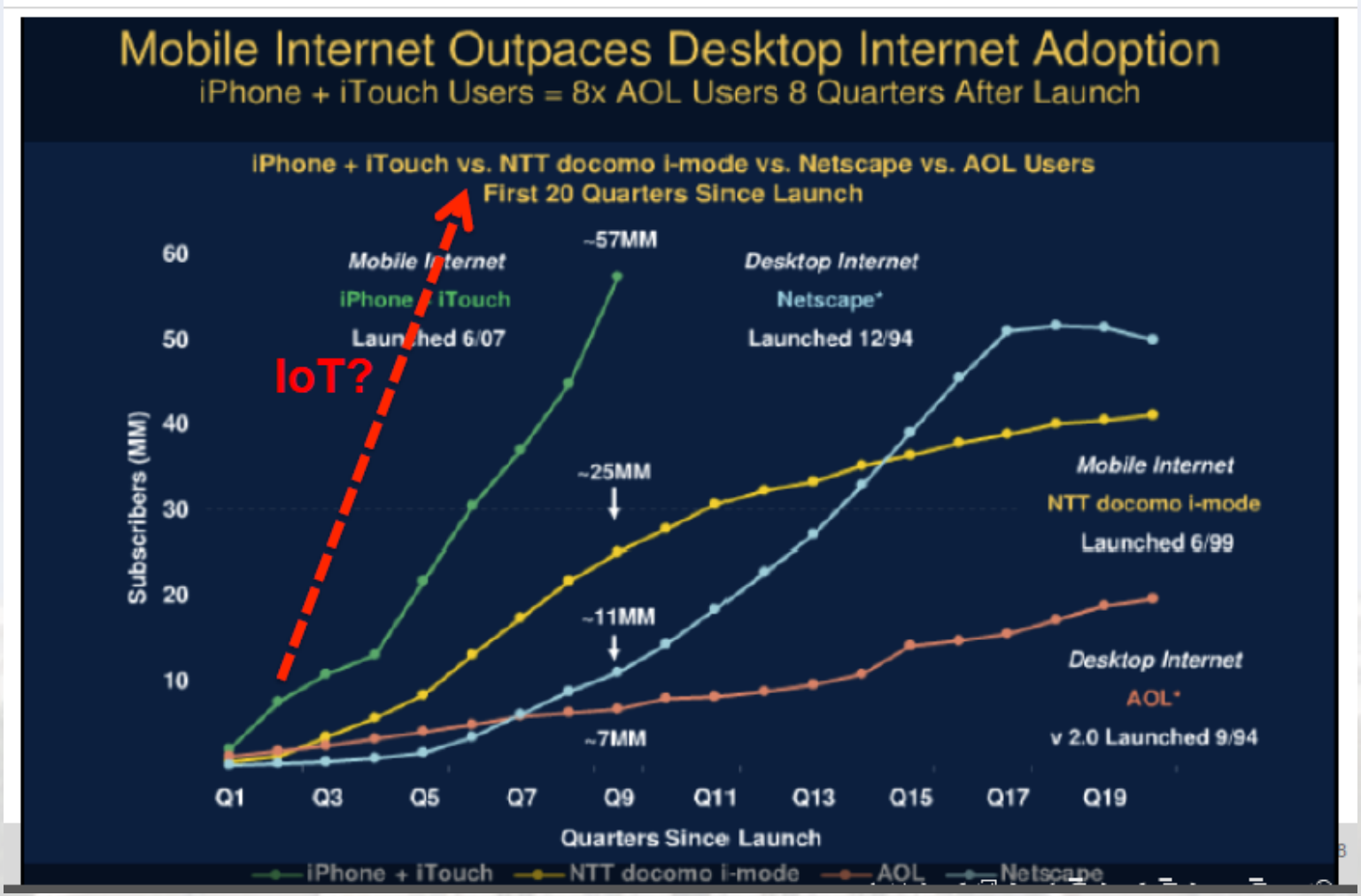
#hackEWF

Devices at the *Center* of Modern Attacks



#hackEWF

What Does History Tell Us?



Source: Grey Lock Partners, John Pescatore (SANS)

Things *You* Can Do

- Don't connect to (or trust) Free/Open Wi-Fi
  - If you must, refrain from sensitive/privileged transactions like online banking
- Turn on 2-factor authentication
- Use a password manager
- Yes, VPN, MDM, Anti-Virus
  - They should talk to *each other* to offer the best protection
- Delete old networks from your devices (bit more complicated for iPhone users)

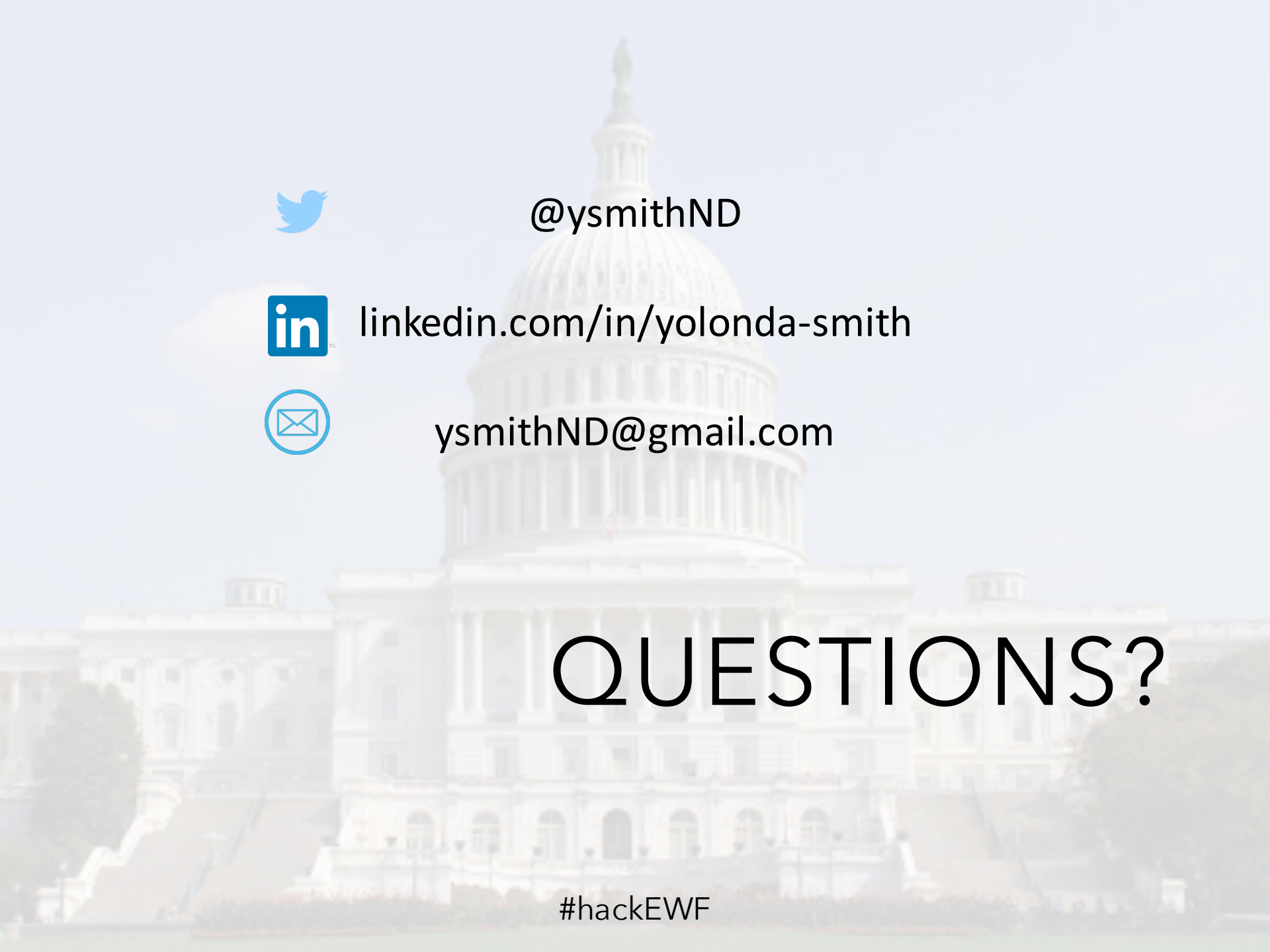
Remember: if you don't need it, turn it off!

How Organizations Should Deal With This

1. A proactive risk mitigation strategy starts with *understanding* what's out there first
   a. Build threat models from *real* data
   b. Adjust fire once you know what's out there

2. From Threat Models → **P**olicy
   a. Flexible
   b. Tied to organizational goals & objectives

3. Effective strategy will include a *combination* of technologies
   a. Application
   b. Device
   c. Network



@ysmithND

linkedin.com/in/yolonda-smith

ysmithND@gmail.com

QUESTIONS?

#hackEWF

THANK YOU!

Yolonda N. Smith