RISKS & MITIGATIONS

THE NEW DEVICE THREAT LANDSCAPE

Yolonda N. Smith

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

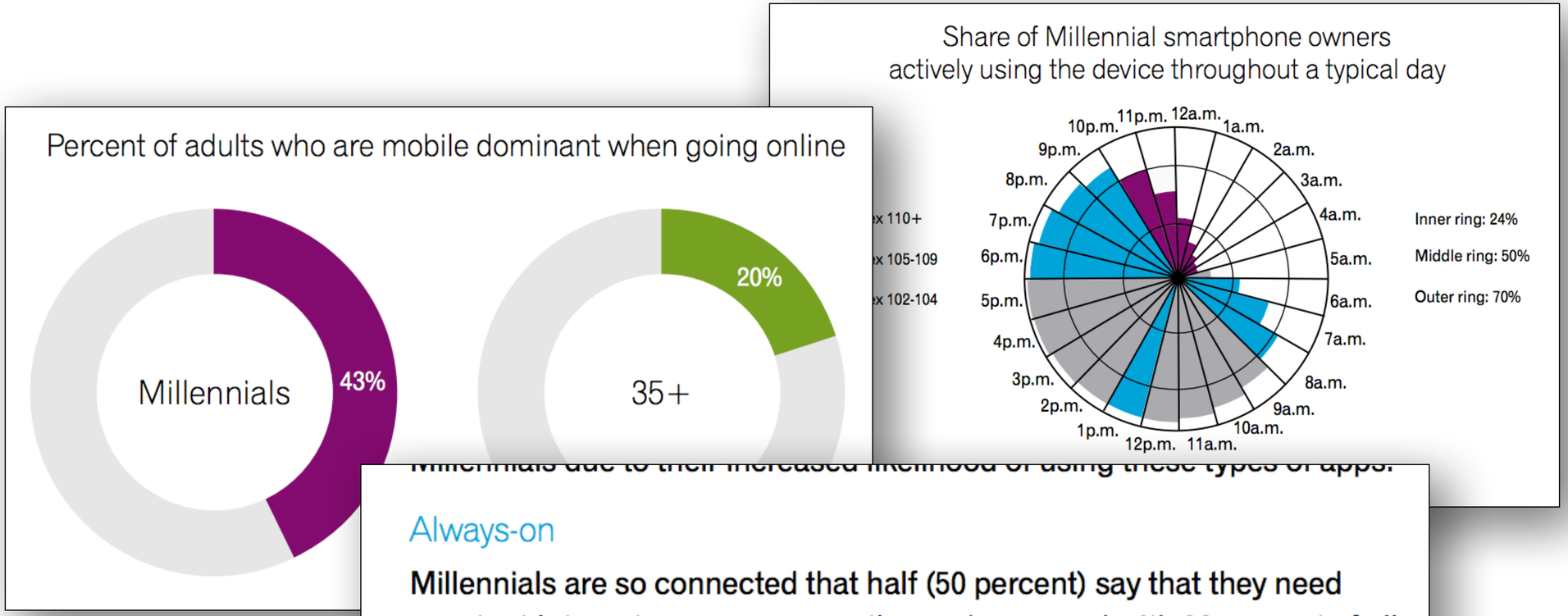
OVERVIEW

- Housekeeping
- About Me
- The Connected Workforce
- Fundamental Premise
- Demo
- Articulating the Risk
- Mitigating the Risk (*Your Role*)
- Questions

YOLONDA IN 1 SLIDE

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

THE CONNECTED WORKFORCE



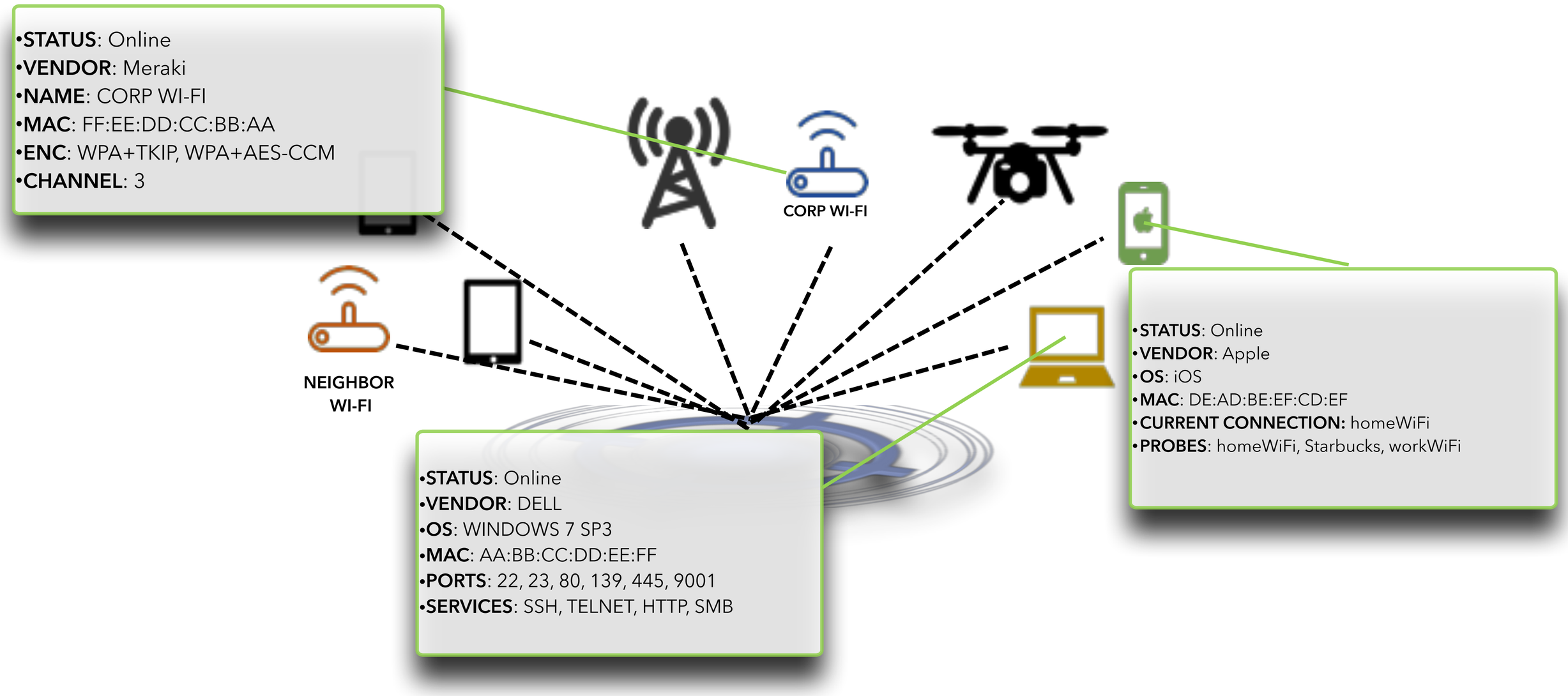
Always-on

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.

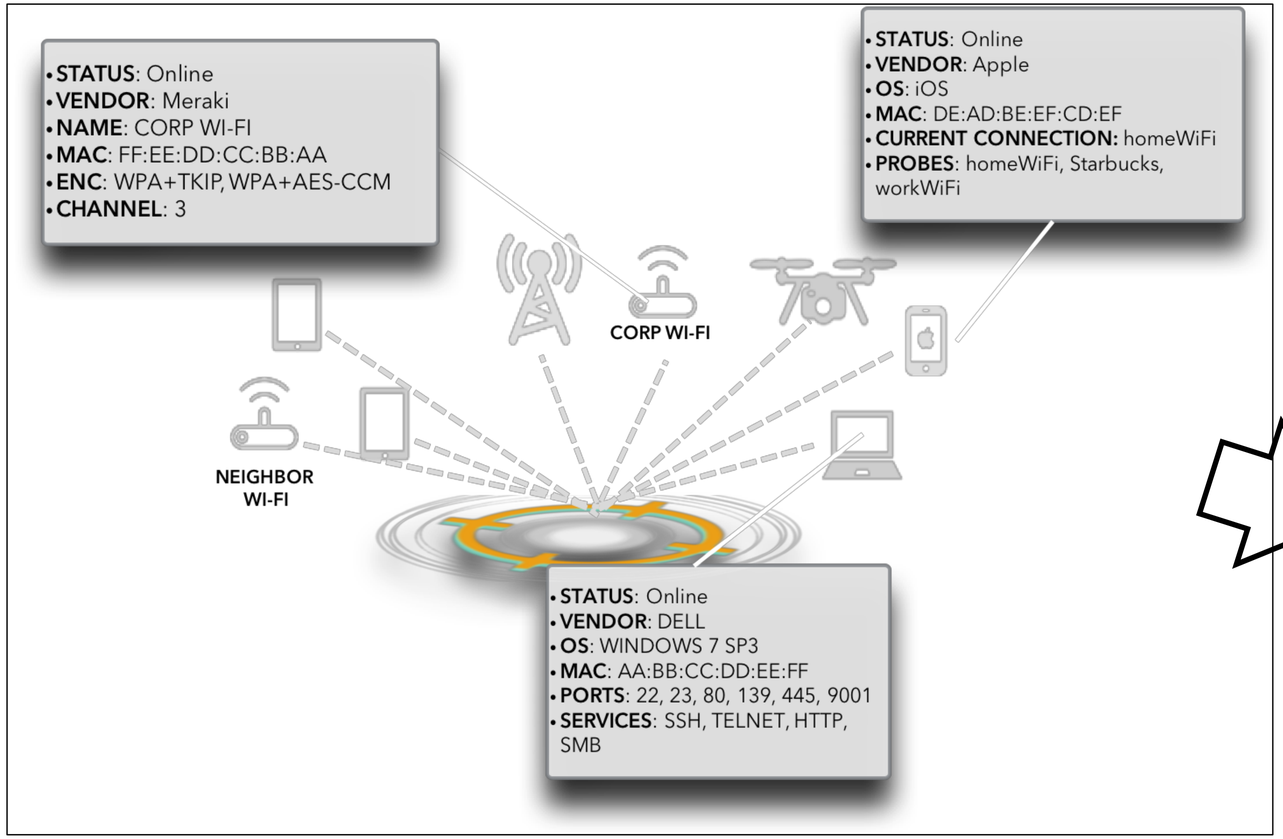
THE FUNDAMENTAL PREMISE OF EVERY MODERN COMPUTING DEVICE IS THE CONSISTENT, PERSISTENT ABILITY TO CONNECT TO THE OUTSIDE WORLD

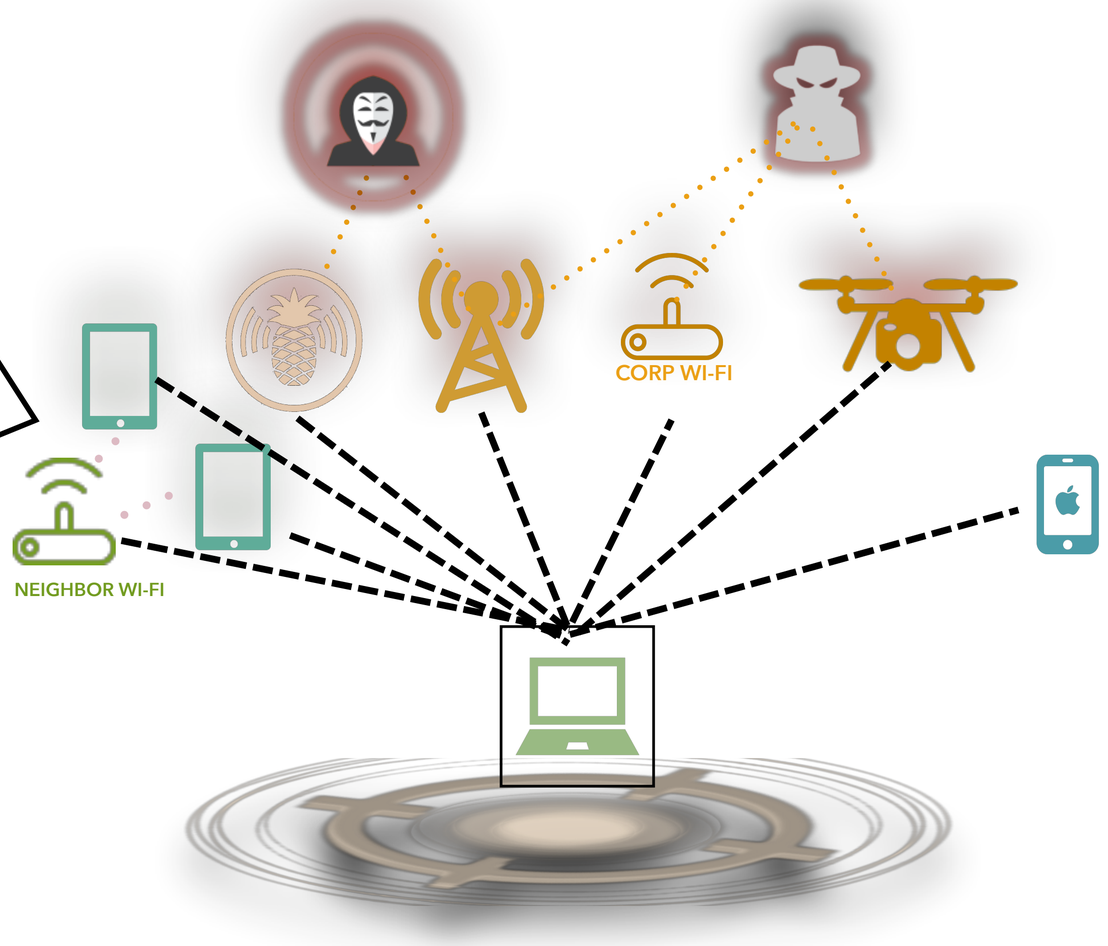
PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

OUR DEVICES ARE TALKING. . . WHAT ARE THEY SAYING?



GOOD THINGS TALK TO BAD THINGS

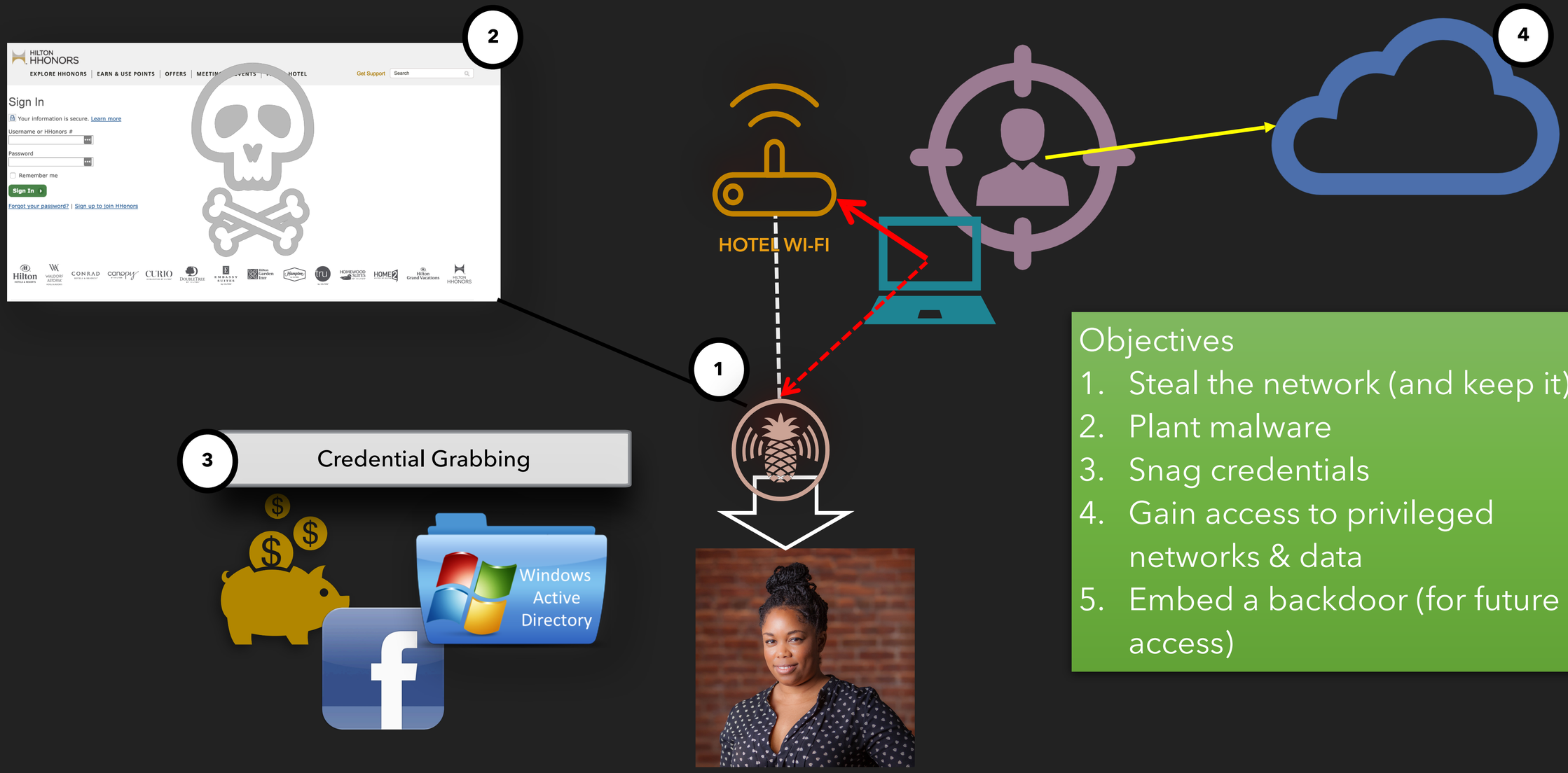




DEMO CONSTRUCT

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

CONSTRUCTING THE ATTACK



Objectives

1. Steal the network (and keep it)
2. Plant malware
3. Snag credentials
4. Gain access to privileged networks & data
5. Embed a backdoor (for future access)

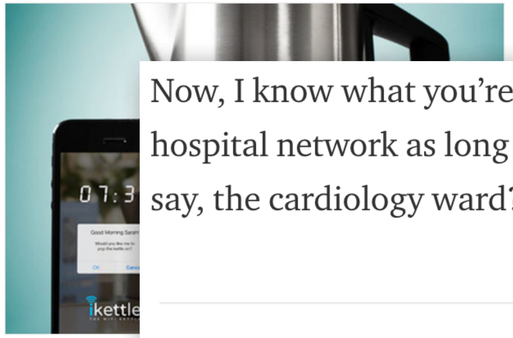
REAL WORLD EXAMPLE

Security

Connected kettles boil over, spill Wi-Fi passwords over London

Pen-tester's killer cuppas made in cracked iKettle

By Darren Pauli 19 Oct 2015 at 05:57 124 SHARE ▼



A security man has ma
across London, provin

Now, I know what you're thinking: *who ca* e smart kettle ends up on th
hospital network as long as it's not o er-special network segment like,
say, the cardiology ward? Well, I vant to burst your bubble:

23 2000

Services

23
tcp
telnet

Cardiology

user:

2000
tcp
ikettle

\xff\xfb\x01\xff\xfb\x03\xff\xfd\x18\r\ Cardiology \r\n\n\n\ruser:

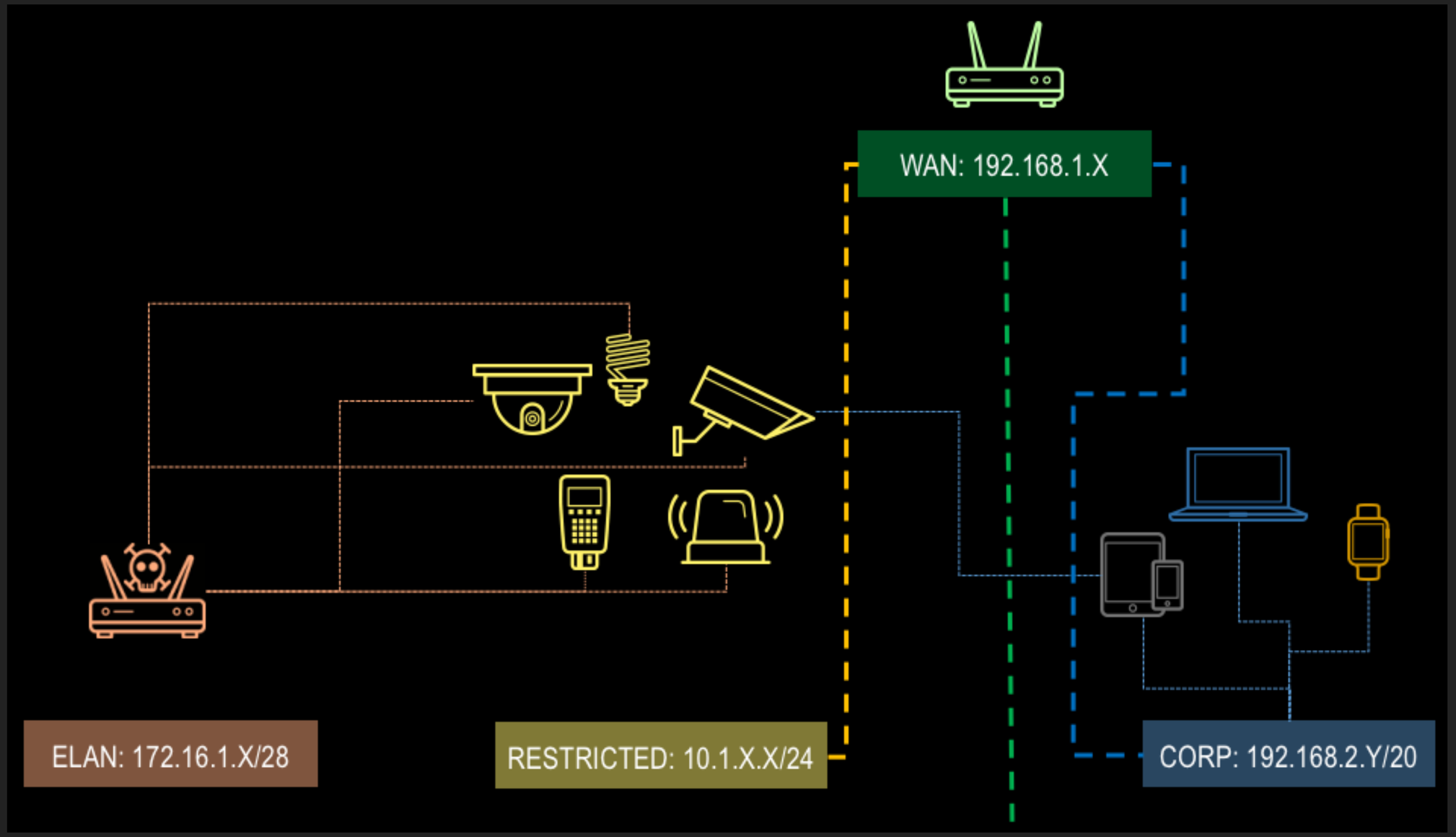
Yolonda Smith
May 30 · 7 min read

How Your Doctor's Coffee Jones is Going to Get Your Personal Data Stolen*

Read more...

OMEN JUDGES, APR 2018

TECHNICAL SETUP



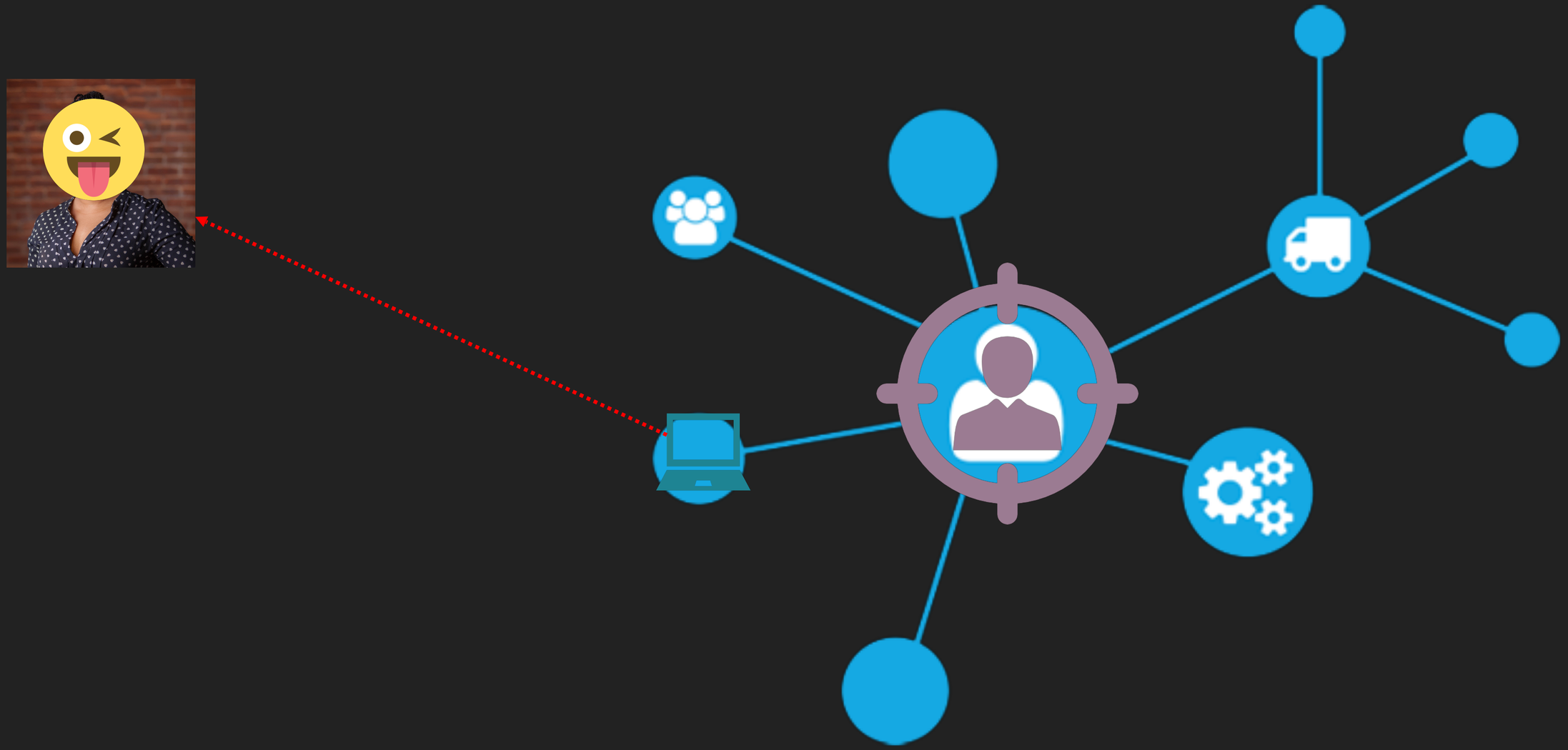
PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

TOOLS REQUIRED

1. Hak5 Pineapple running “evil” (aka *fake*) Access Point & captive portal
2. Kali Linux Virtual Machine (VM)
   - Fing network scanner (port/service fingerprinting)
   - Python & Ruby scripts (malware development)
   - Netcat (backdoor placement)
3. Social Engineering Toolkit
4. Metasploit
5. Windows 10 Virtual Machine (for testing)

Total cost for this attack: $150 USD

IMPACT TO THE ORGANIZATION



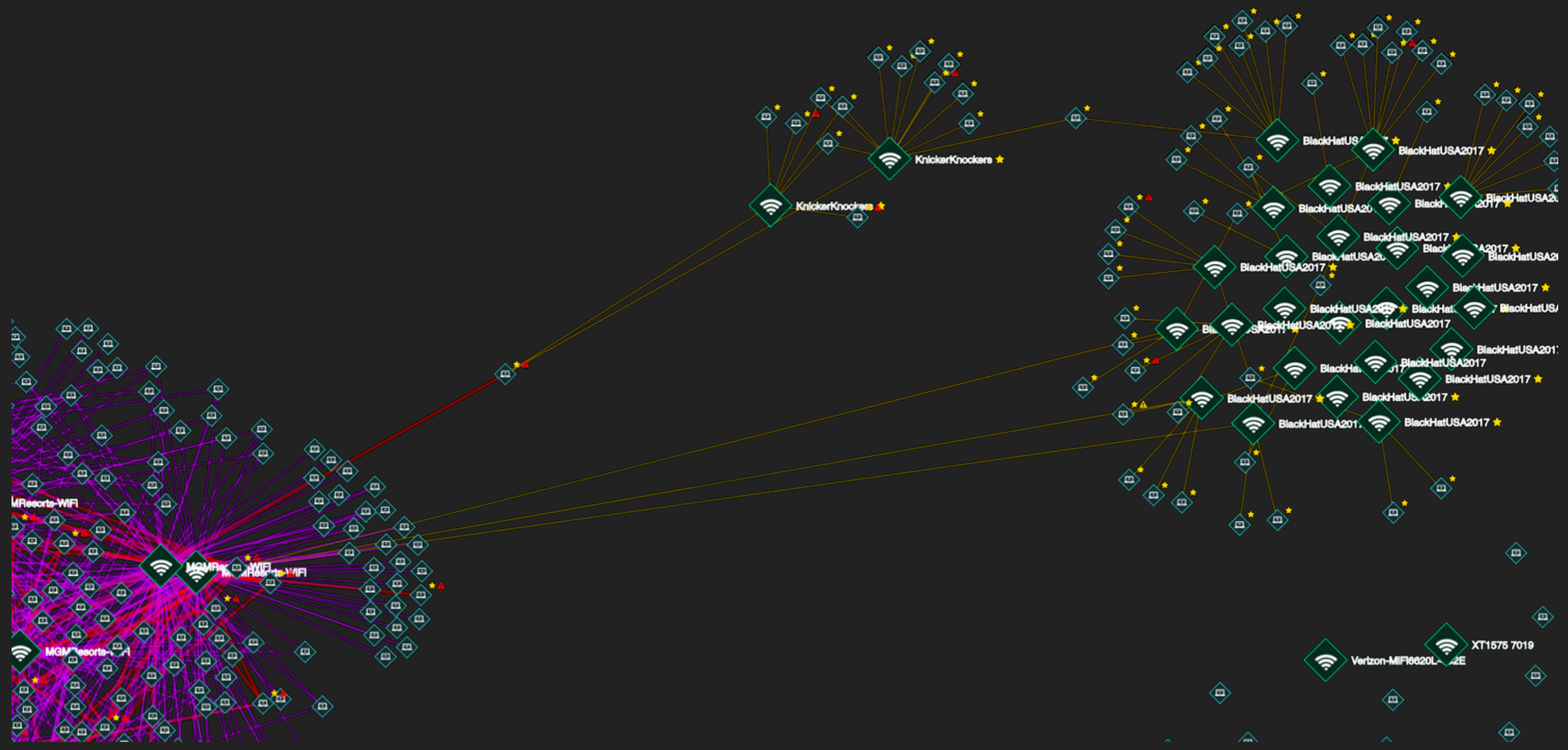
DISCLAIMER

This demonstration was prepared with the expressed and written permission of NAWJ. The demonstration was tested and vetted on specific devices, networks and software. As a precaution, now would be a good time to turn off your Wi-Fi. If you leave it on and your devices stop working, I'm going to make this face: 😫 followed immediately by this face ¯_(ツ)_/¯

You ***should not*** attempt to do this without expressed, written permission from a legal target.

WHAT YOU WON'T SEE

1. Cracking of access point passwords
   - If you want info on that, check out aircrack-ng, coWPAtty and similar tools
2. The epic battle raging for control of the devices
   - Devices are dumb & Wi-Fi is ubiquitous



DISCLAIMER

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.

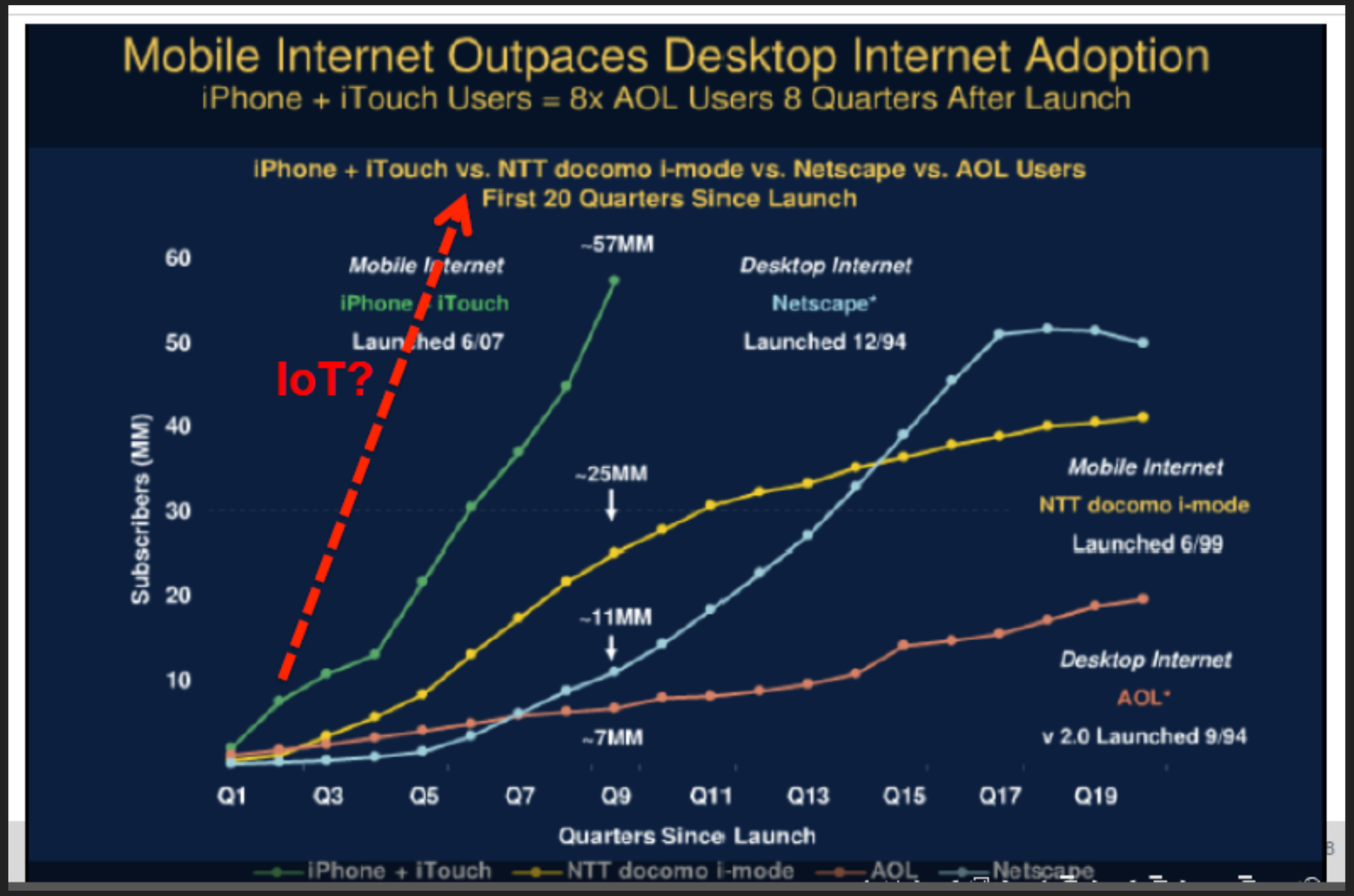
Check out Mass Mailer, Spearphishing attacks from SET (@HackingDave, Trusted Sec)

VEIL Framework (by @harmj0y)

THE RISK

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

WHAT DOES HISTORY TELL US?



Source: Grey Lock Partners, John Pescatore (SANS)

RISK SURFACE IS SPREADING

ıony on Sunday. A10

RATES
VORK

rry in the West

gested it would be able

Global Hack Pressures Officials, Victims

Security experts
of new threats a
investigators be
hunt for perpetr

The cyberattack th
around the globe
weekend, hitting bu
hospitals and gov
agencies in at least
tries, is likely to keep growing
as people around
turn to work, law-
authorities warned.

*By Nick Ko
Jenny Gro
and Stu*

Investigators
far-reaching hunt
petrator, as
around the world
mitigate damage
highest-profile
worm outbreak in
cade. Europe's pol
tion agency estim
200,000 individual terminals
had fallen victim t
while Chinese au
the number as hi
lion world-wide.
"This is someth
ven't seen before,

21 Hacked Cameras, D

OCT 16

Massive Internet Ou

services in the aftermath of the attack.

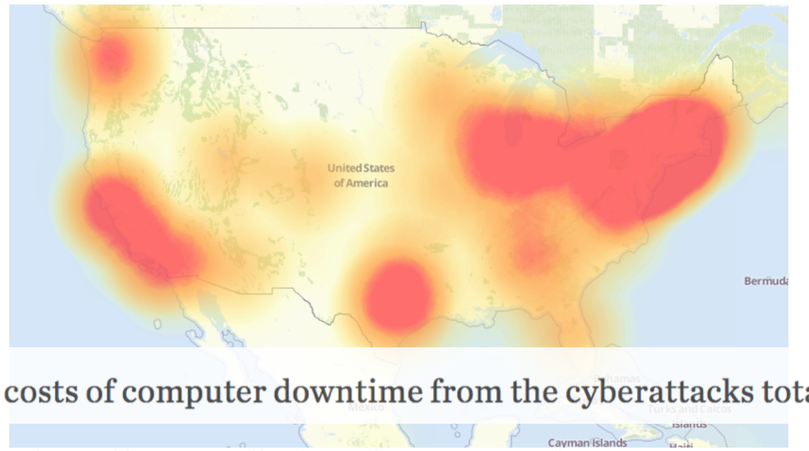
Dyn Customer Analysis: Before and After Mirai DDoS Attack

The data analyzed a representative sample of 178,000 domains hosted on Dyn before and immediately after the 2016 attacks, and revealed that more than 14,000 internet domains dropped Dyn as their DNS service provider in the wake of the incident (roughly 8%).

The findings are interesting because it's rare that the financial fallout from a DDoS attack is laid out so clearly in the public eye. But when you consider the impact of the attack on Dyn's

net a
er of Web sites was launched with the help of hacked
such as CCTV video cameras and digital video recorders,

an training their attack cannons on **Dyn**, an Internet
les critical technology services to some of the Internet's
top destinations. The attack began creating problems for Internet users reaching an array of
sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

"Everyone was running around saying we've been hacked…it spread like wildfire"

Mohamed Amri
Parts Maker, Renault SA France

The direct costs of computer downtime from the cyberattacks totals around $8 billion

The RISK Team provided me with a report detailing known indicators found in the firewall and DNS logs that I had sent over earlier. Of the thousands of domains requested, only 15 distinct IP addresses were returned. Four of these IP addresses and close to 100 of the domains appeared in recent indicator lists for an emergent IoT botnet. This botnet spread from device to device by brute-forcing default and weak passwords. Once the password w
known, the malware had full control of the device a
would check in with command infrastructure for up
and change the device's password – locking us out
5,000 systems.

While we waited for the full packet capture solution to be set up, I instructed the Network Operations Team to prepare to shut down all network access for our IoT segments once we had intercepted the malware password. Short lived as it was, the impact from severing all of our IoT devices from the internet during that brief period was noticeable across the campus – and we were determined never to have a repeat incident.

"Short of replacing every soda machine and lamp post, I was at a loss for how to remediate the situation"

Incident Commander
Unnamed Canadian University

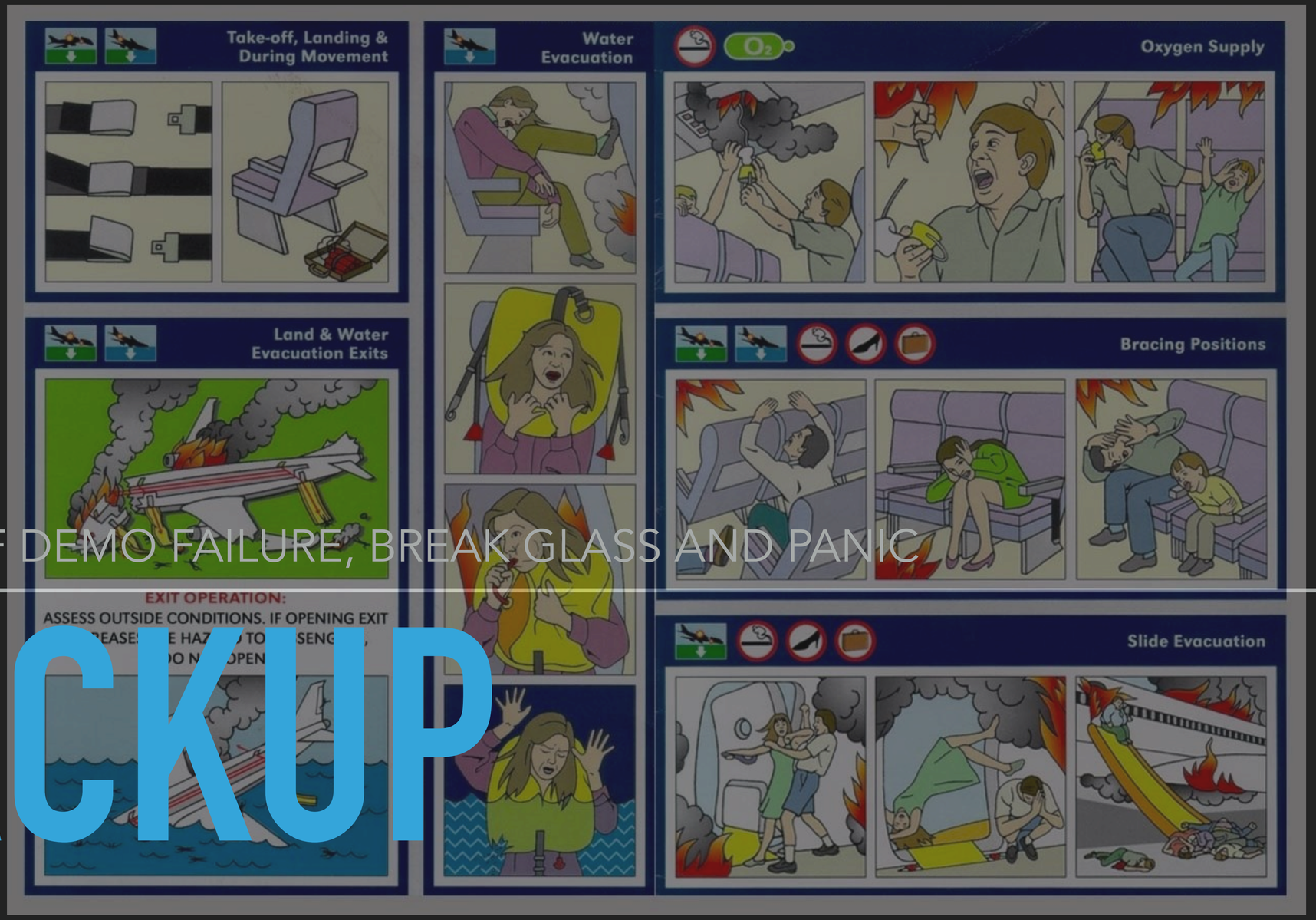
THINGS YOU CAN DO

- Utilize ‘secure’ access points when available
  - Look for the 
- Turn on 2-factor authentication
- Use a password manager
- When someone asks for your personal information, ask them what they need it for and don’t be afraid to say ‘no’
- Delete old networks from your devices (bit more complicated for iPhone users)

QUESTIONS?

@ysmithND | linkedin.com/in/yolonda-smith | ysmithND@gmail.com

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

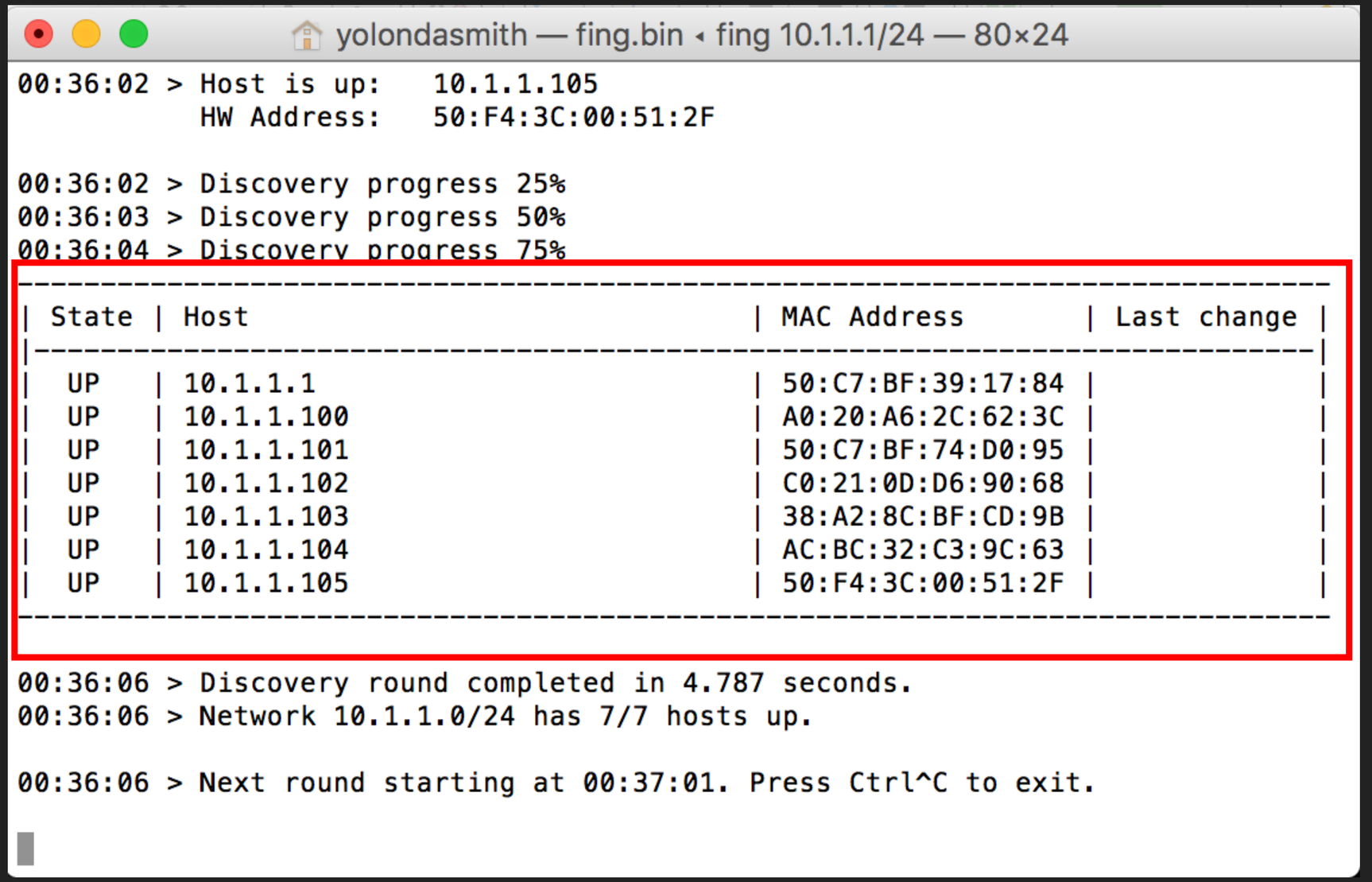


IN CASE OF DEMO FAILURE, BREAK GLASS AND PANIC

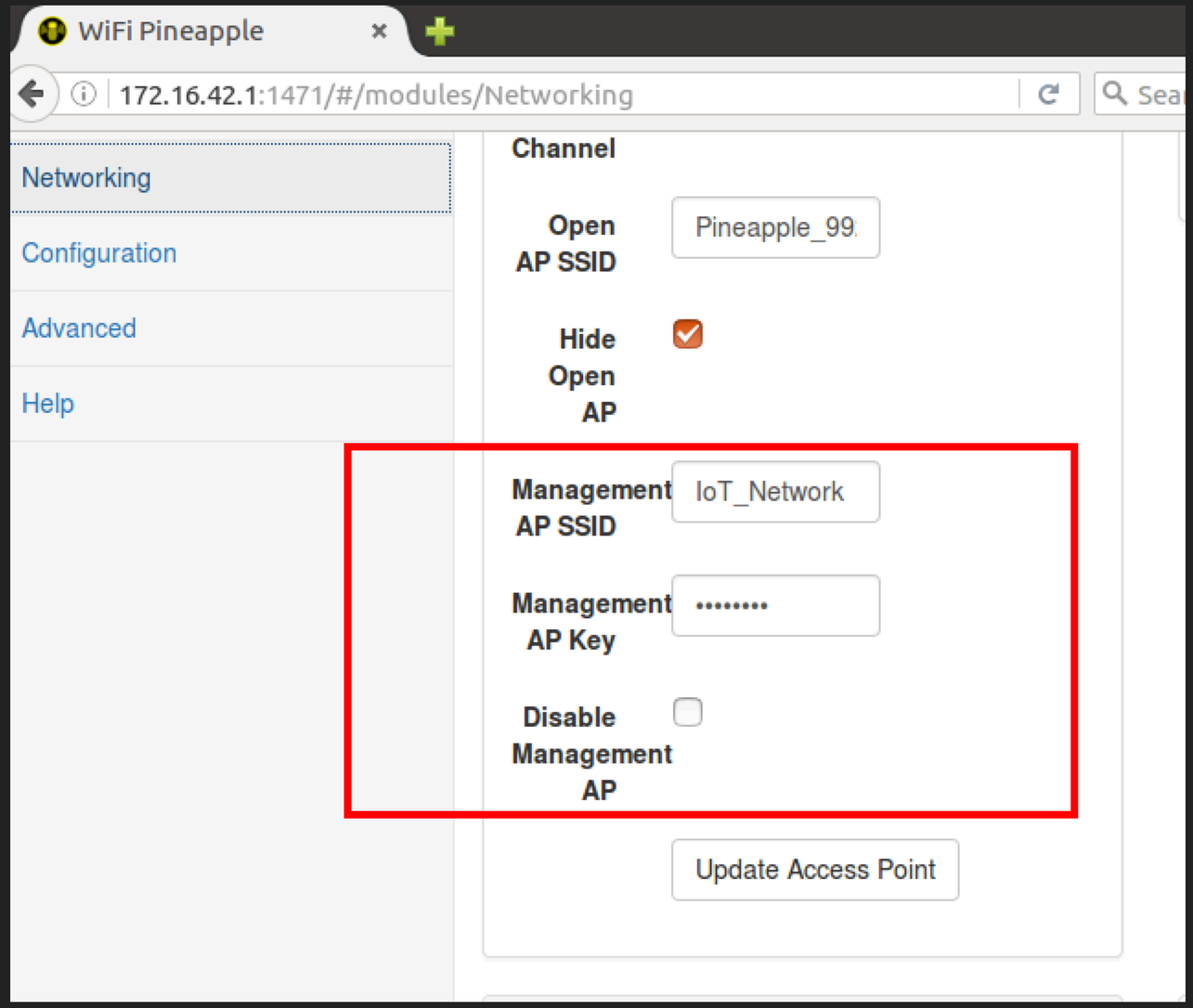
BACKUP

PREPARED FOR NATIONAL ASSOCIATION OF WOMEN JUDGES, APR 2018

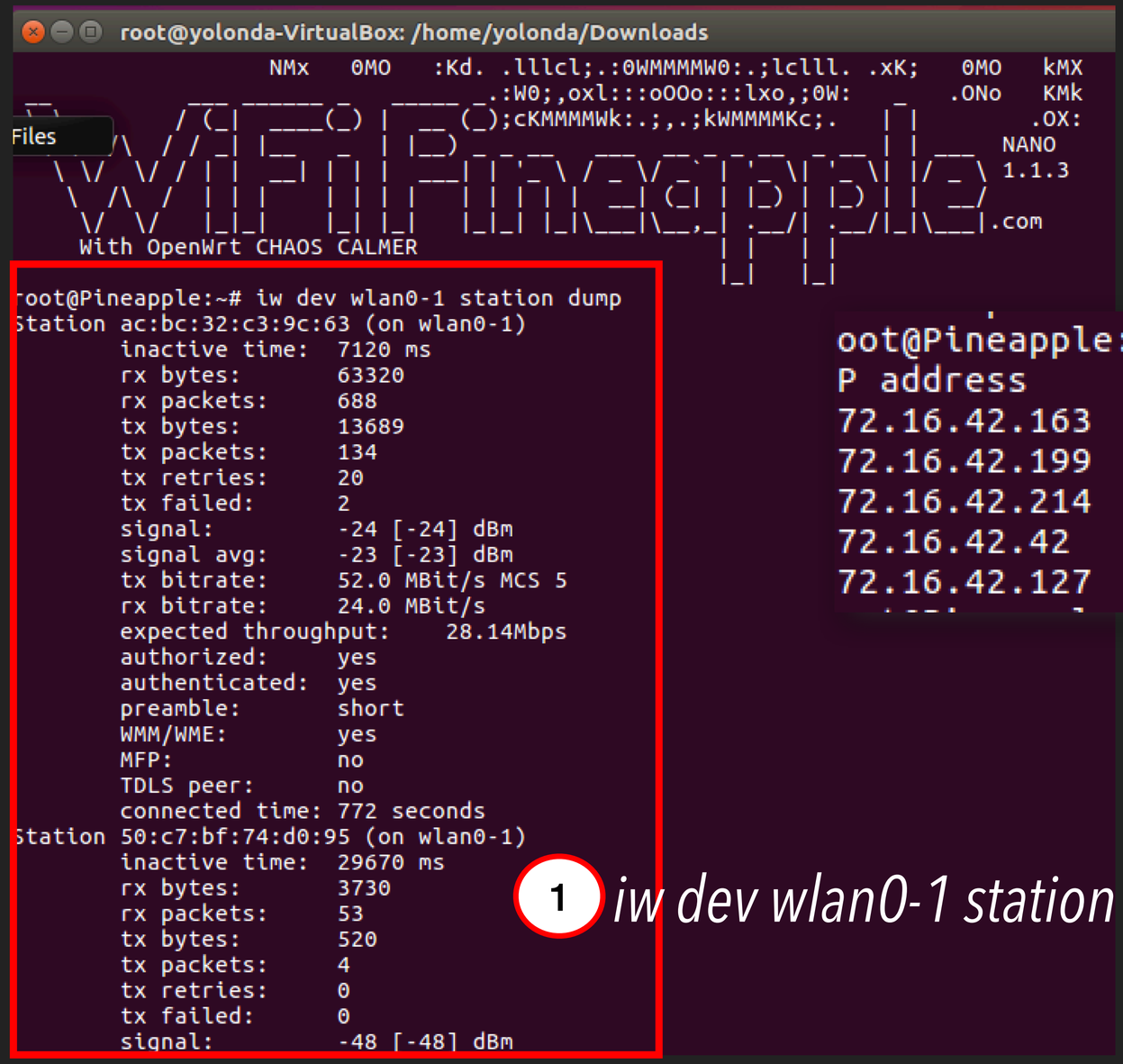
PROOF POINT 1



PROOF POINT 2



PROOF POINT 4



1 *iw dev wlan0-1 station dump*

2 *arp -a*

```
oot@Pineapple:~# arp -a
P address       HW type     Flags       HW address
72.16.42.163    0x1         0x0         00:c0:ca:90:df:59
72.16.42.199    0x1         0x2         38:a2:8c:bf:cd:9b
72.16.42.214    0x1         0x2         a0:20:a6:2c:62:3c
72.16.42.42     0x1         0x2         00:c0:ca:90:df:59
72.16.42.127    0x1         0x2         ac:bc:32:c3:9c:63
```

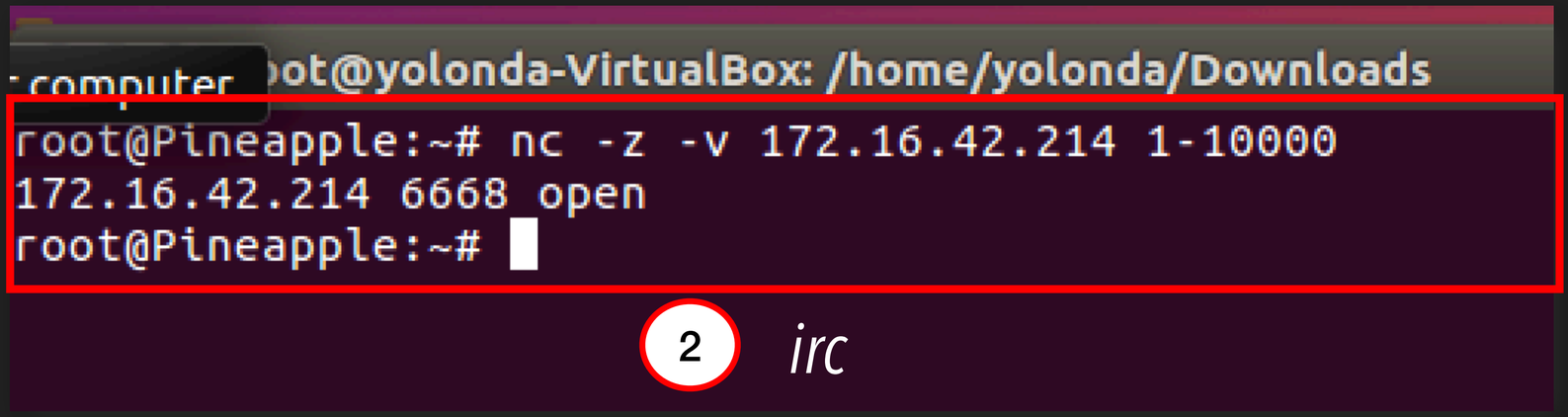
PROOF POINT 5

HotelAndra	2C:5D:93:06:15:A8	Open	no	3	-84
	6C:72:E7:D1:30:77				
HotelAndra	2C:5D:93:06:55:28	Open	no	6	-85
HotelAndra	2C:5D:93:06:6A:F8	Open	no	11	-67
Paxton	30:B5:C2:BE:01:99	Mixed WPA	yes	11	-85
HotelAndra	34:8F:27:27:15:A8	Open	no	3	-82
IoT_Network	50:C7:BF:39:17:84	Mixed WPA	yes	10	-53
CenturyLink5053	58:8B:F3:E5:67:FB	Mixed WPA	yes	11	-90
Wuhoo	60:E3:27:39:C4:35	WPA2	yes	11	-87
Blastworks AirPort01	64:A5:C3:68:74:A8	WPA2	no	6	-90
Pavia System - Wireless	74:3E:2B:11:48:98	WPA2	no	8	-83
SPRW	80:2A:A8:81:EE:64	Mixed WPA	no	6	-91
The Dark Side	8E:15:44:A8:DA:2C	Mixed WPA	no	1	-81
The Dark Side	8E:15:44:A8:DB:87	Mixed WPA	no	11	-80
TDGUEST	94:B4:0F:3C:E5:A0	Open	no	1	-76

PROOF POINT 6

```
172.16.42.127    0x1          0x2          ac:bc:32:c3:9c:
root@Pineapple:~# nc -z -v 172.16.42.199
Error: No ports specified for connection
root@Pineapple:~# nc -z -v 172.16.42.199 1-10000
172.16.42.199 4444 open
172.16.42.199 8000 open
root@Pineapple:~#
```

1 *Kerberos ticketing && webserver*



2 *irc*