RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: MBS-F03

Mobile Security Shootout: Which Smartphones Are Up to the task?

Chester Wisniewski

Senior Security Advisor
Sophos Inc.
@chetwisniewski

The landscape has settled

Is the market dictated by biases?

- Ask 10 techs, get 10 answers
- Android malware is scary
- Walled garden = safe & secure
- Fewer users means fewer attackers?

TRUTH

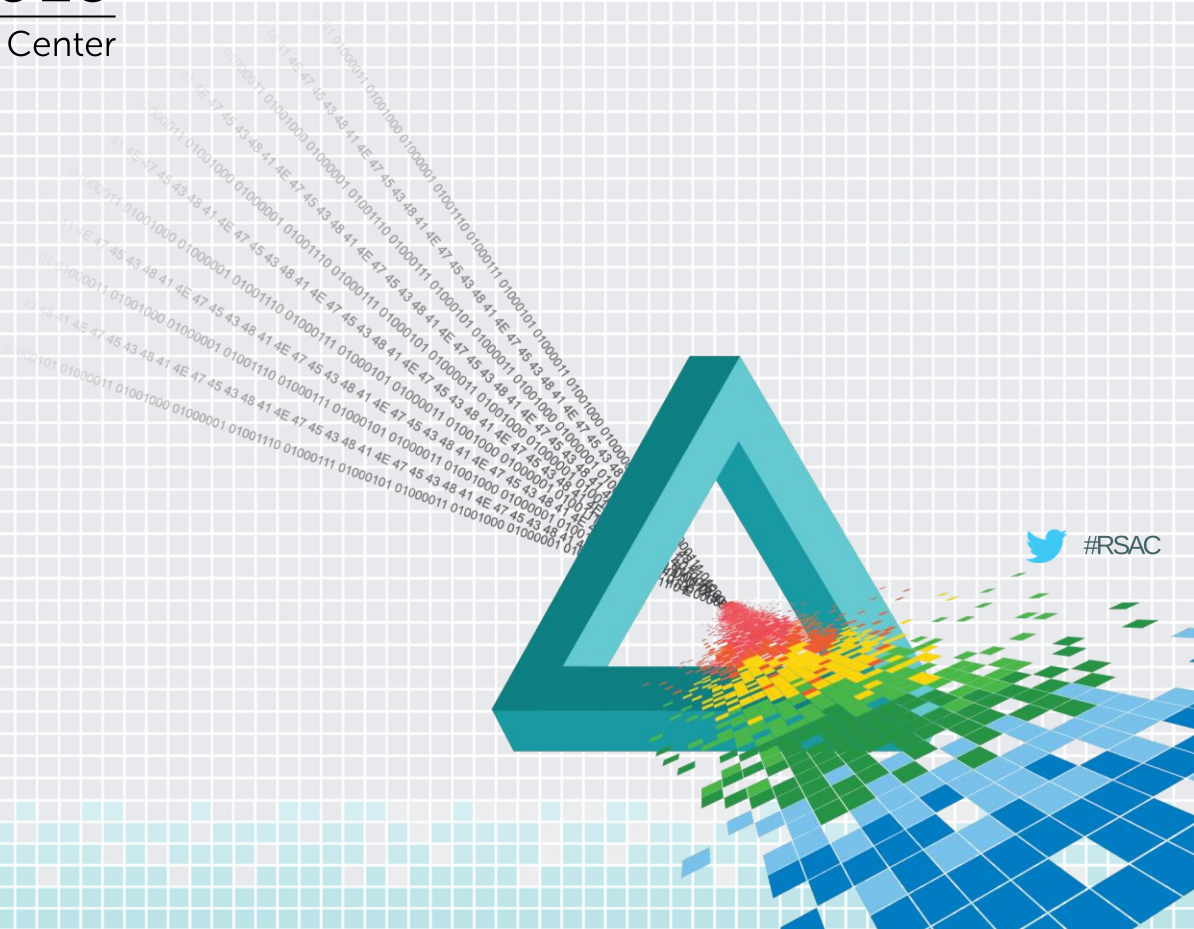
What are the questions?

- Safe from what?
- What are we protecting?
- Priorities
  - Data theft
  - Privacy
  - Productivity
  - Awareness and control

FLORIDA
0376
© 2012 RIMROCK FIREARMS
NO DAILY BAG LIMIT
ZOMBIE HUNTING PERMIT 2012/2013
RIFLES/HANDGUNS: .223 CALIBER OR LARGER
SHOTGUNS: B/BB OR LARGER. NO BIRDSHOT

RSAConference2015

San Francisco | April 20-24 | Moscone Center

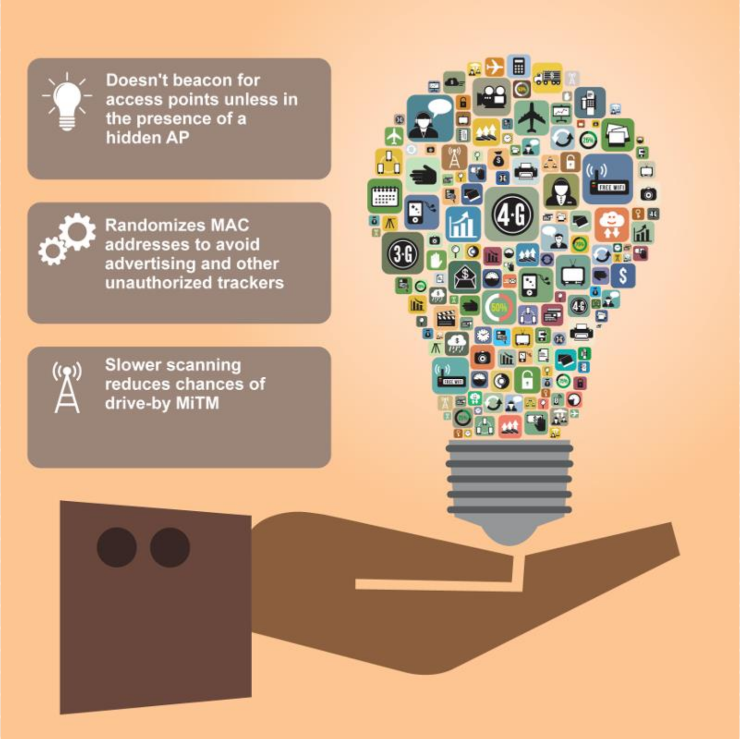


#RSAC

The platforms

Android

iOS



Doesn't beacon for access points unless in the presence of a hidden AP

Randomizes MAC addresses to avoid advertising and other unauthorized trackers

Slower scanning reduces chances of drive-by MiTM

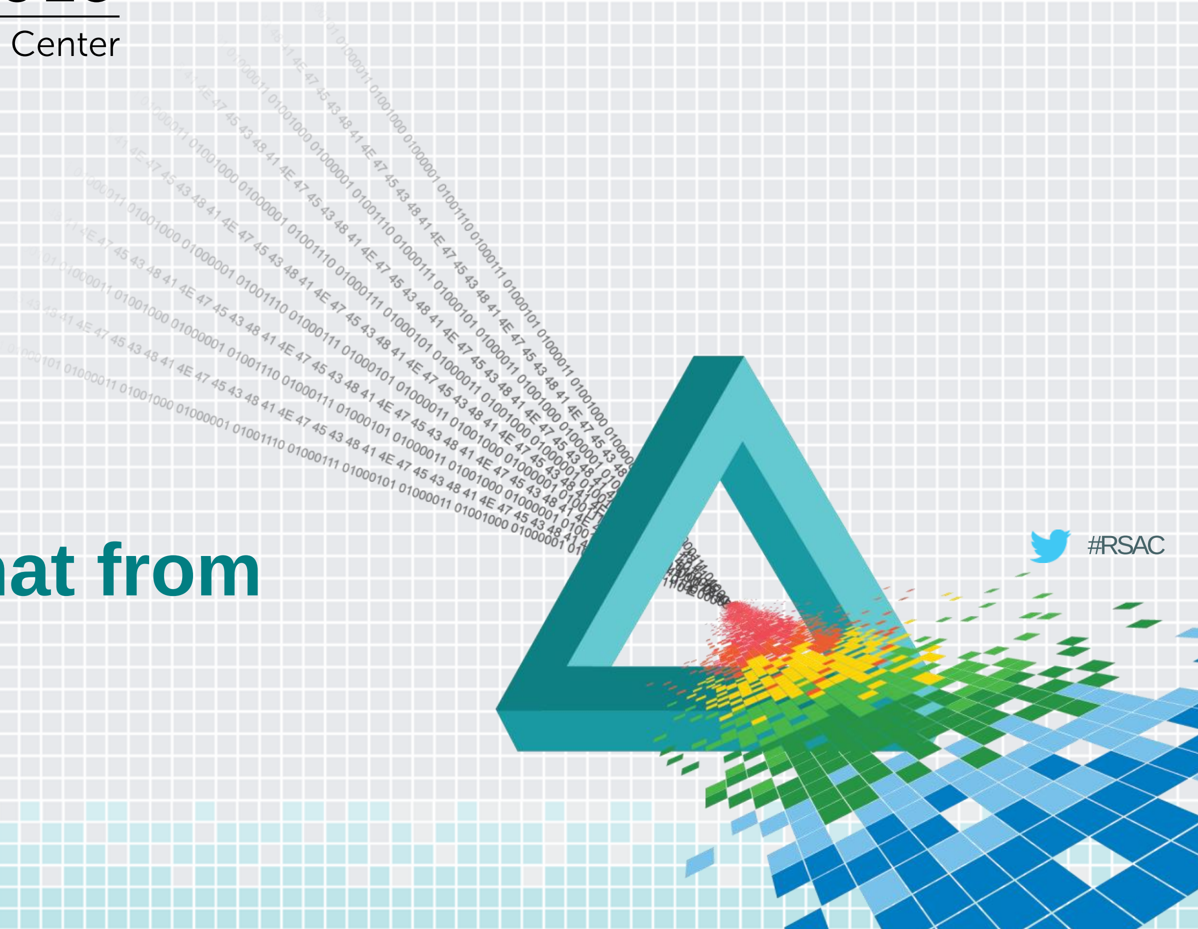
Windows Phone

A big "Thanks!" to our Black Hat Review Board for their continued commitment and dedication:

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Who is getting what from our mobiles?



#RSAC

Apps

```
SELECT       Employee
FROM         Employees
WHERE        HireDate BETWEEN

SELECT EmployeeID, FirstName, LastN
WHERE City IN ('Seattle', 'Tacoma', 'Re

SELECT       EmployeeID, FirstName, Last
FROM         Employees
WHERE        HireDate NOT BETWEEN '1
```

- One tap login
- Optional PIN
- Location includes GPS, cell tower, provider, signal strength, type, roaming
- Uploads photos without explicit permission

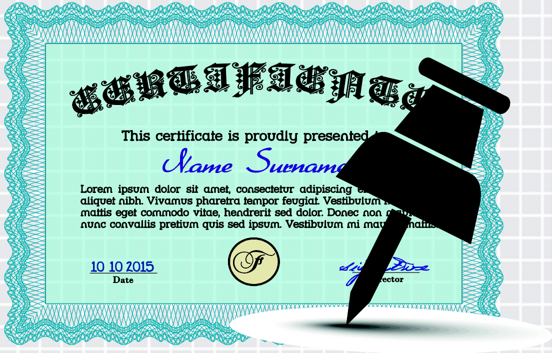
- Requires phone #
- Leaks email over HTTP
- Can hijack account over email
- Asks nicely for all permissions

- Leaks MAC address over HTTP
- Communicates with two ad networks
- Leaks internal IP address, phone #, carrier

Apps

- Leaks MAC address
- No cert validation (now fixed)
- Password sent
- Sends model, carrier, memory, storage, WiFi, battery info

- Sends off phone # and birthdate and password
- Sends location, battery, CPU, time zone, memory and storage
- No password reset verification
- Discloses if user or pw is wrong



Lorem ipsum dolor sit amet, consectetur adipiscing
aliquet nibh. Vivamus pharetra tempor feugiat. Vestibulum
mattis eget commodo vitae, hendrerit sed dolor. Donec non
nunc convallis pretium quis sed ipsum. Vestibulum mi mau

- Collects model, carrier, country

- All HTTPS
- No pinning
- No passwords transmitted
- No ads

What can happen – The flashlight app

- You probably don’t want this, which brings us to the tools that really matter. Control.

Taking action on what we've learned

ActiveSync to the rescue…?

- Not all platforms are created equal

Microsoft® Exchange ActiveSync®

Android 5.0, Lollipop

Windows Phone

Items to consider

- Is BYOD worth it?
- What information will you allow to be accessed from mobile devices?
- Certificates, passcodes, WiFi, VPN, Camera
- Most importantly: Application control
- The cloud.

Bottom line

STANDBY
MUTE
AUDIO
CH+
SUBTITLE
MENU
EXIT
VOL-
OK
VOL+
FAVOURITE
CH-
TV/RADIO
1
2
3
RETURN
4
5
6
NAVI
7
8
9
0
REV
FWD
ZOOM
V.MODE
PLAY
PAUSE
STOP
REPEAT
FILE
TIMER

WHERE?
WHEN? WHY?
WHEN?
WHY?
WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
WHEN?
WHO?
WHAT?
WHERE?
WHEN?
HOW?
HOW?
WHEN?
WHERE? WHICH? WHOSE? WHEN? WHY?
WHERE?
WHOSE?
HOW?
WHEN? WHERE?
HOW?
WHICH?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHY? HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHERE? WHICH? WHOSE? WHEN? WHY?
WHAT?
WHY? HOW? WHERE?
WHO? WHOSE?
WHERE? WHAT? HOW?
WHAT?
WHY?
WHO?
HOW?
WHERE? WHAT? HOW?
WHERE?
WHERE? WHICH? WHOSE? WHEN? WHY?
HOW? WHERE? WHY?
WHERE?
HOW?
HOW? WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
WHERE?
WHAT?
HOW?
HOW?
WHERE?