OWASP

Open Web Application Security Project

OWASP Mobile Top Ten 2015 Data Synthesis

Key Observations and Data Synthesis

Participants Submitted Data

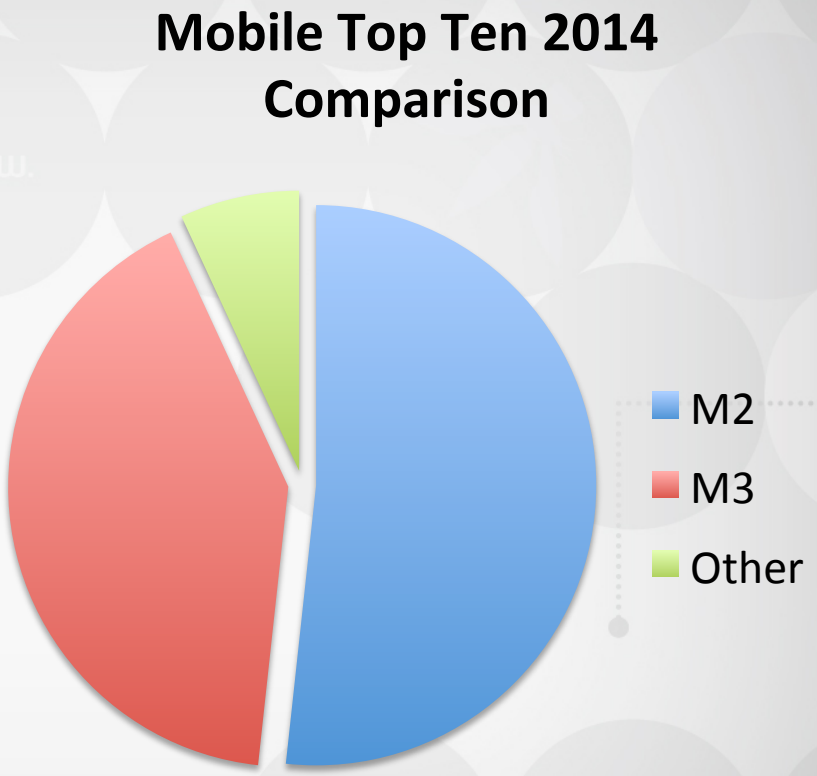
- Mobile Top Ten 2015 Data Had Largest Contribution of Data in History of OWASP Mobile Top Ten:

  - Arxan Technologies
  - Bug Crowd
  - HackLabs
  - IBM X-Force Threat Intelligence
  - KRVW
  - MetaIntelli
  - Pure Hacking
  - Secure Network
  - Denim Group
  - Veracode
  - HP
  - WhiteHat

- Key Trends?

KRVW

- Small sample set (20 apps)
- Largely anecdotal
- Breakdown:
  - Highest issues found in insecure data storage
  - Next most prevalent issue: insecure transit of sensitive information
  - Other: certificate validation issues



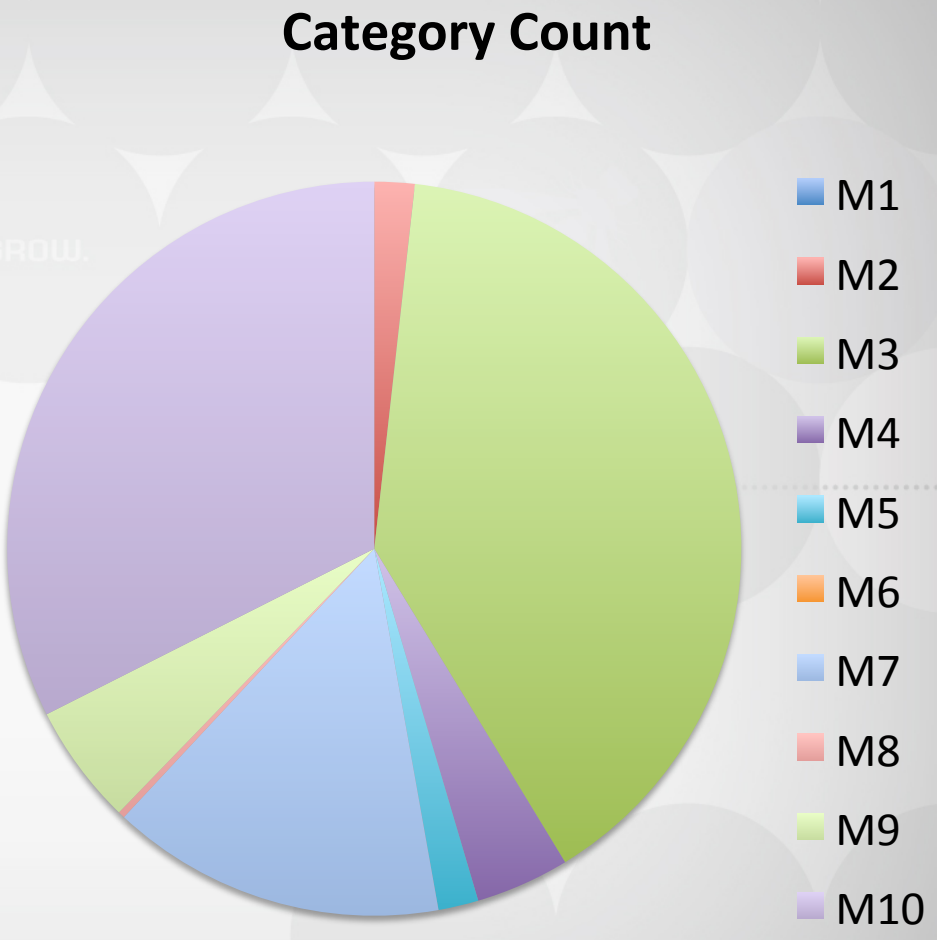
MetaIntelli

Large sample set (38,000 apps)

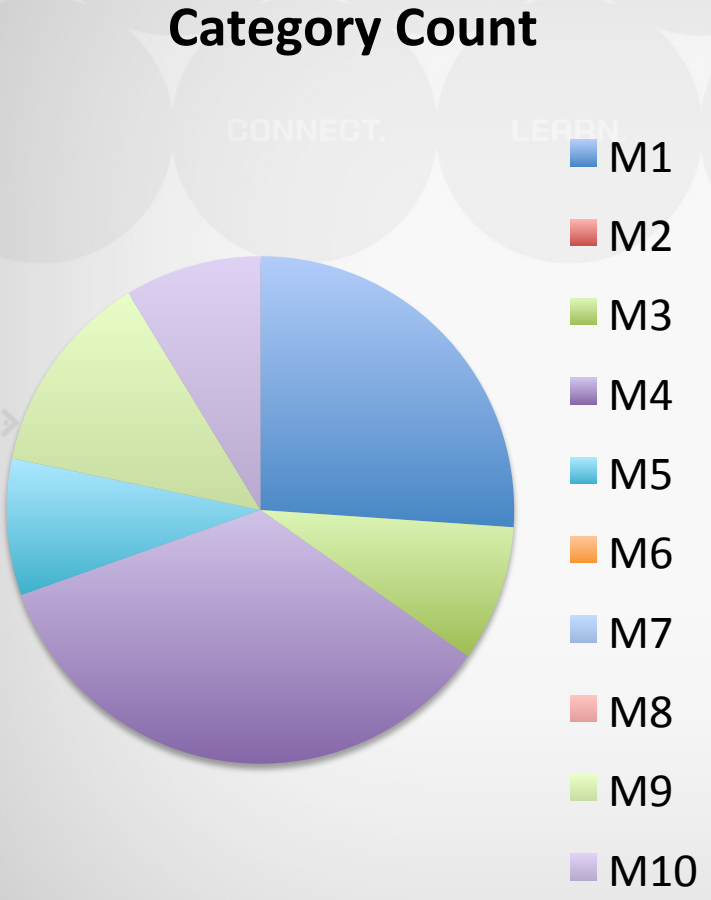
Biggest issues:

1. Insufficient Transport Layer Protection
2. Lack of Binary Protections
3. Client Side Injection

* No outliers found*



Pure Hacking



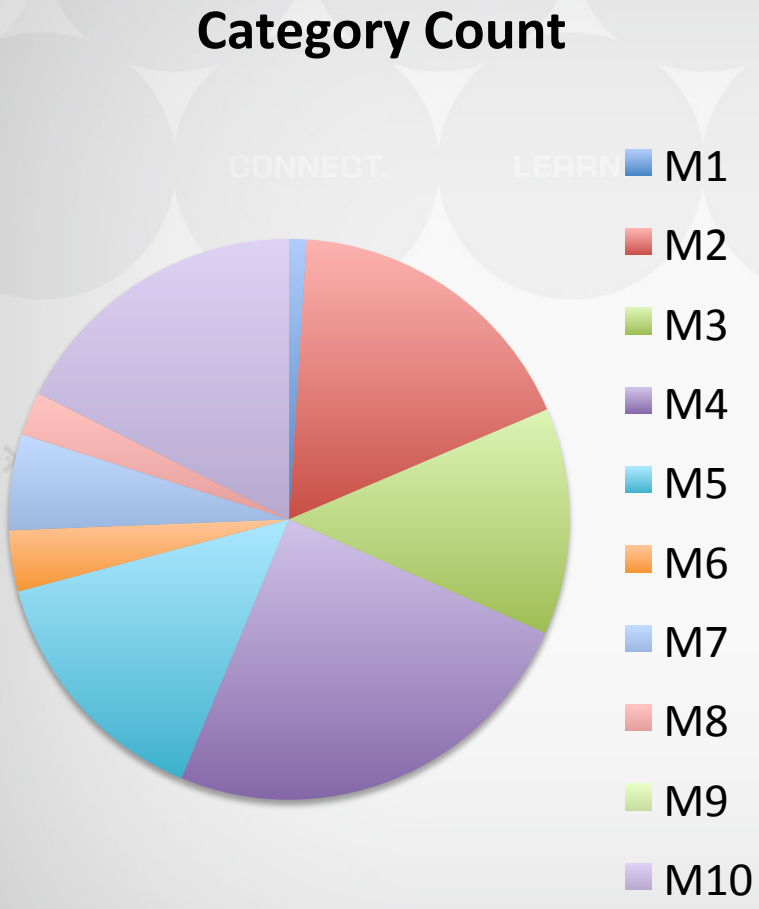
Small sample set (7 apps)

Biggest issues:

1. Unintended data leakage
2. Weak Server Side Controls

No outliers

BugCrowd



Moderate sample size (433 vulns)

Biggest issues:

1. Unintended Data Leakage
2. Insecure Data Storage
3. Lack of Binary Protection

No outliers

Arxan Technologies

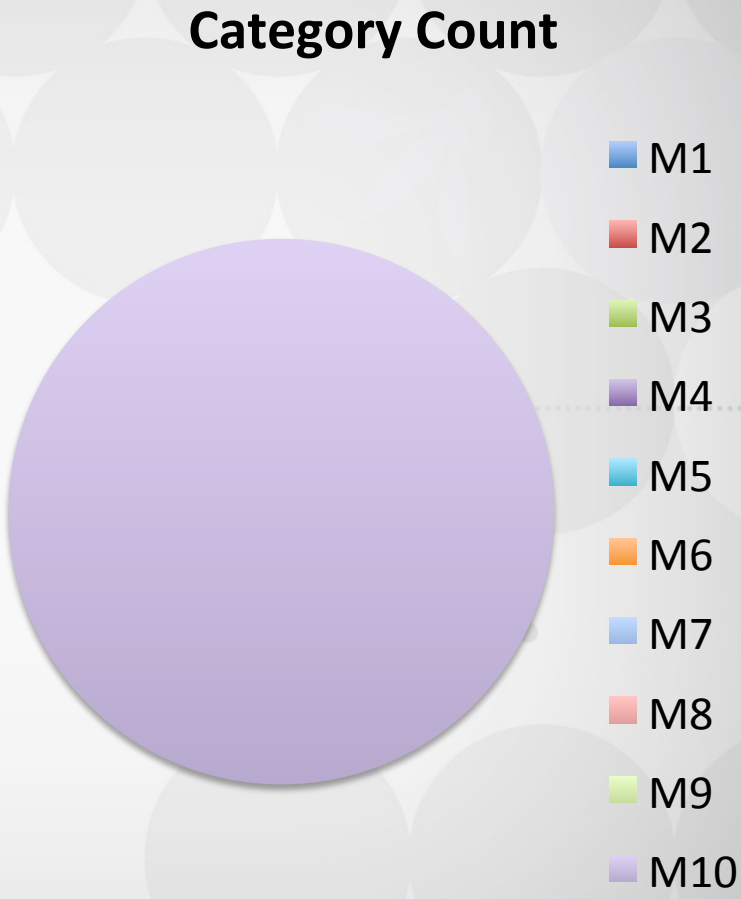
Moderate sample size (200+ apps)

Focused exclusively on M10

Biggest issue found:

1. Exposed binaries easy to reverse engineer / modify

No outliers



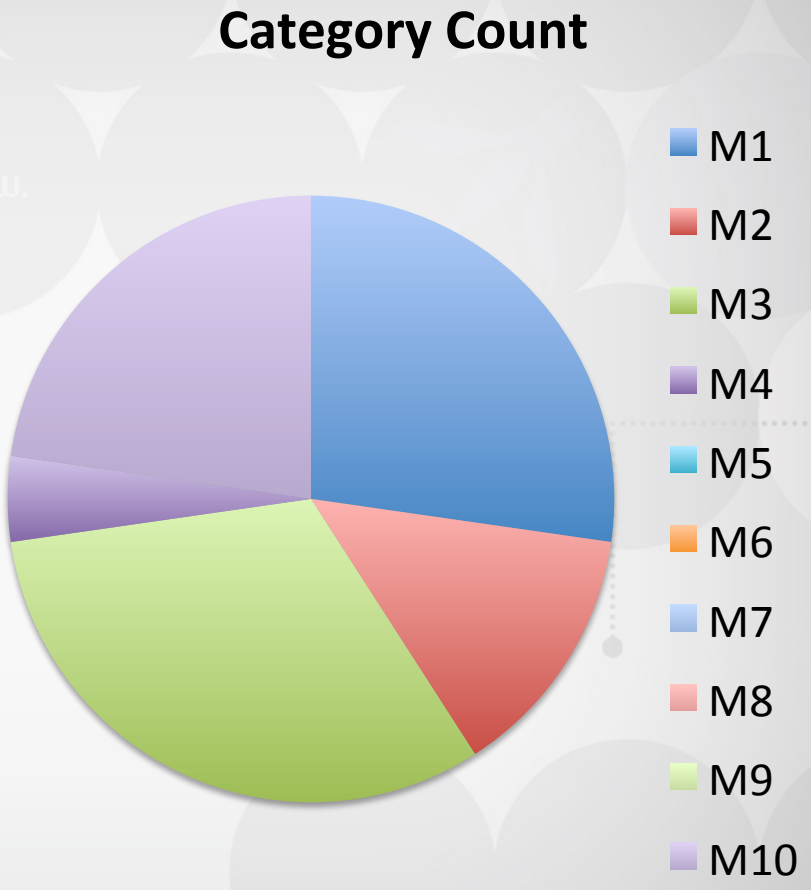
Hacklabs

Small sample size (23 vulns)

Biggest issues:

1. Insufficient Transport Layer Protection;
2. Weak Server Side Controls;
3. Lack of Binary Protection

No outliers



Key Observations

- In the datasets observed, data fits well within existing categories
  - This only implies that 2014 adequately catches what people are currently looking for
- Most commonly reported vulnerabilities:
  - Data security issues;
  - Data transport issues;
  - Binary protection issues;
- Next steps: finish off with additional observational data sets from HP, etc.