A SURVEY OF MOBILE MALWARE IN THE WILD

Adrienne Porter Felt, Matthew Finifter,
Erika Chin, Steve Hanna, and David Wagner
University of California, Berkeley

Does mobile malware exist?

What does it do?

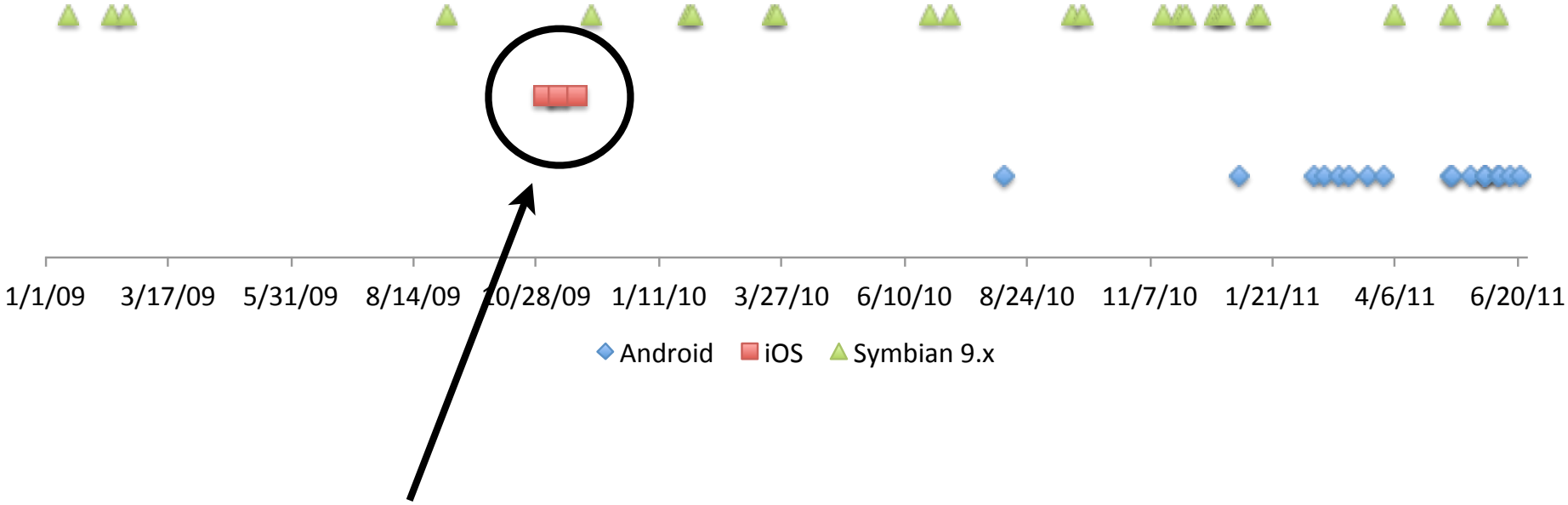
Do existing defenses work?

MALWARE IN THE WILD

iOS	4
Symbian 9.x	24
Android	17
Total	**45**

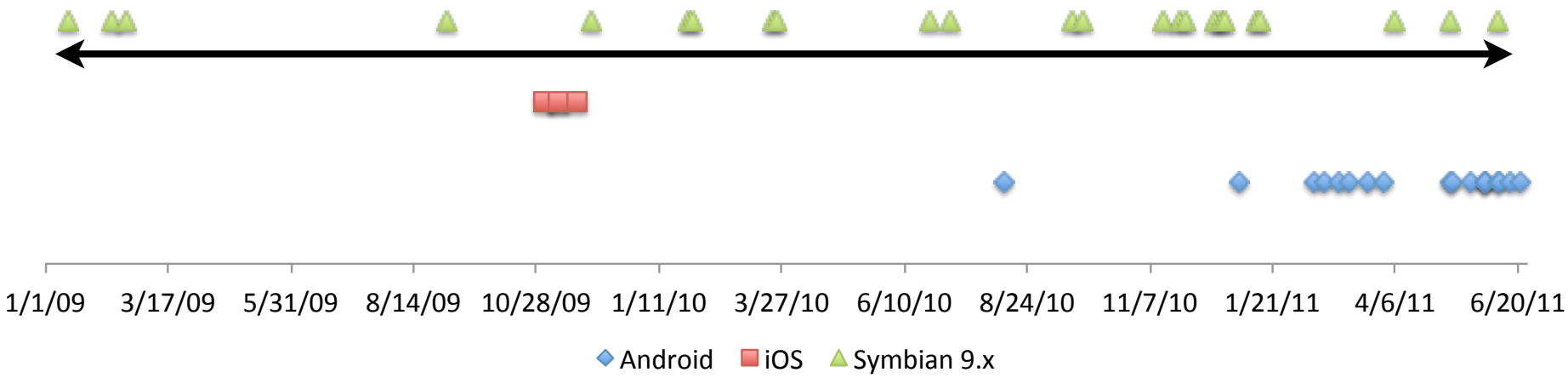
Survey of known malware
from January 2009-June 2011

TIMELINE



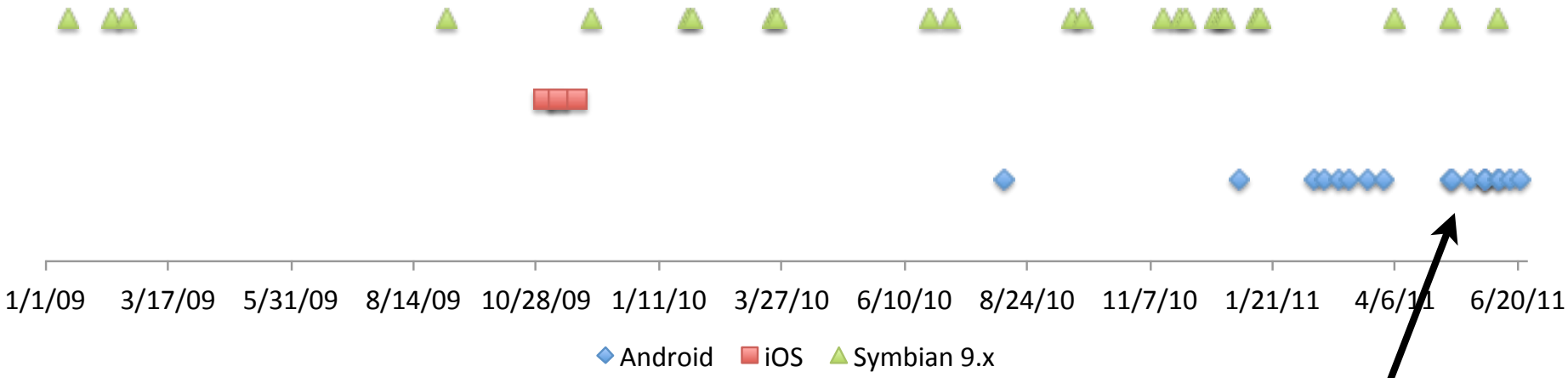
iOS malware clustered around 1 backdoor

TIMELINE



Symbian 9.x malware is evenly spread out

TIMELINE



Android malware seems to be increasing

MOTIVATIONS

BEHAVIOR SURVEY

Steals user information	**60%**
Premium calls or SMS	**53%**
Sends SMS ad spam	18%
Novelty and amusement	13%
Steals user credentials	9%
Search engine optimization	2%
Ransom	2%

45 pieces of malware
(some exhibit multiple behaviors)

USER INFORMATION

Steals user information	**60%**

- Location, browsing history, list of installs
- IMEI for stolen phones

SMS

Premium calls or SMS	**53%**
Sends SMS ad spam	18%

- Easy & lucrative for Symbian/Android
- Special setting to allow sending SMS?
  - Only 0.8% of Android apps use this ability

MORE TO COME?

Steals user credentials	9%
Search engine optimization	2%

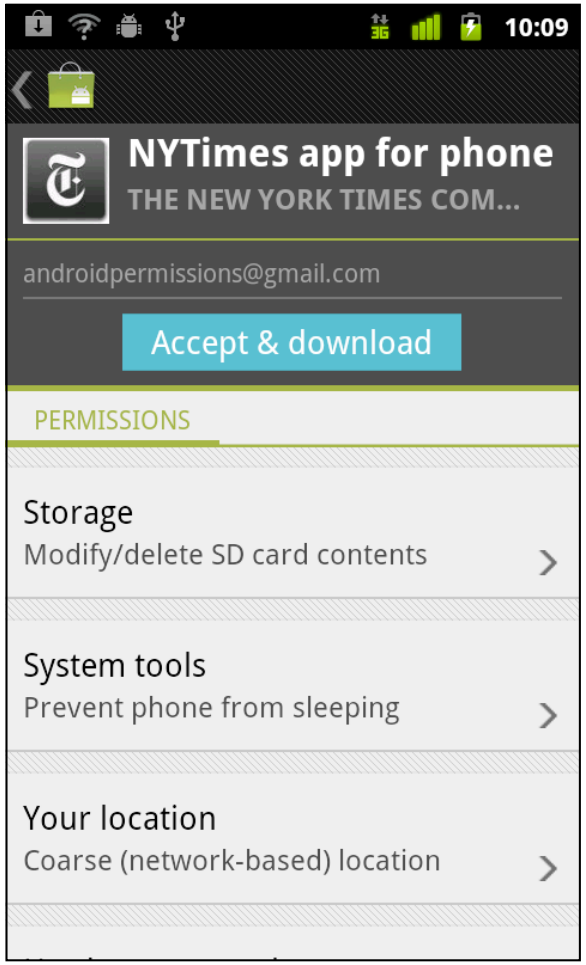
- I think we'll see more of these
- SEO might be under-reported

MALWARE DEFENSES

APPLICATION REVIEW

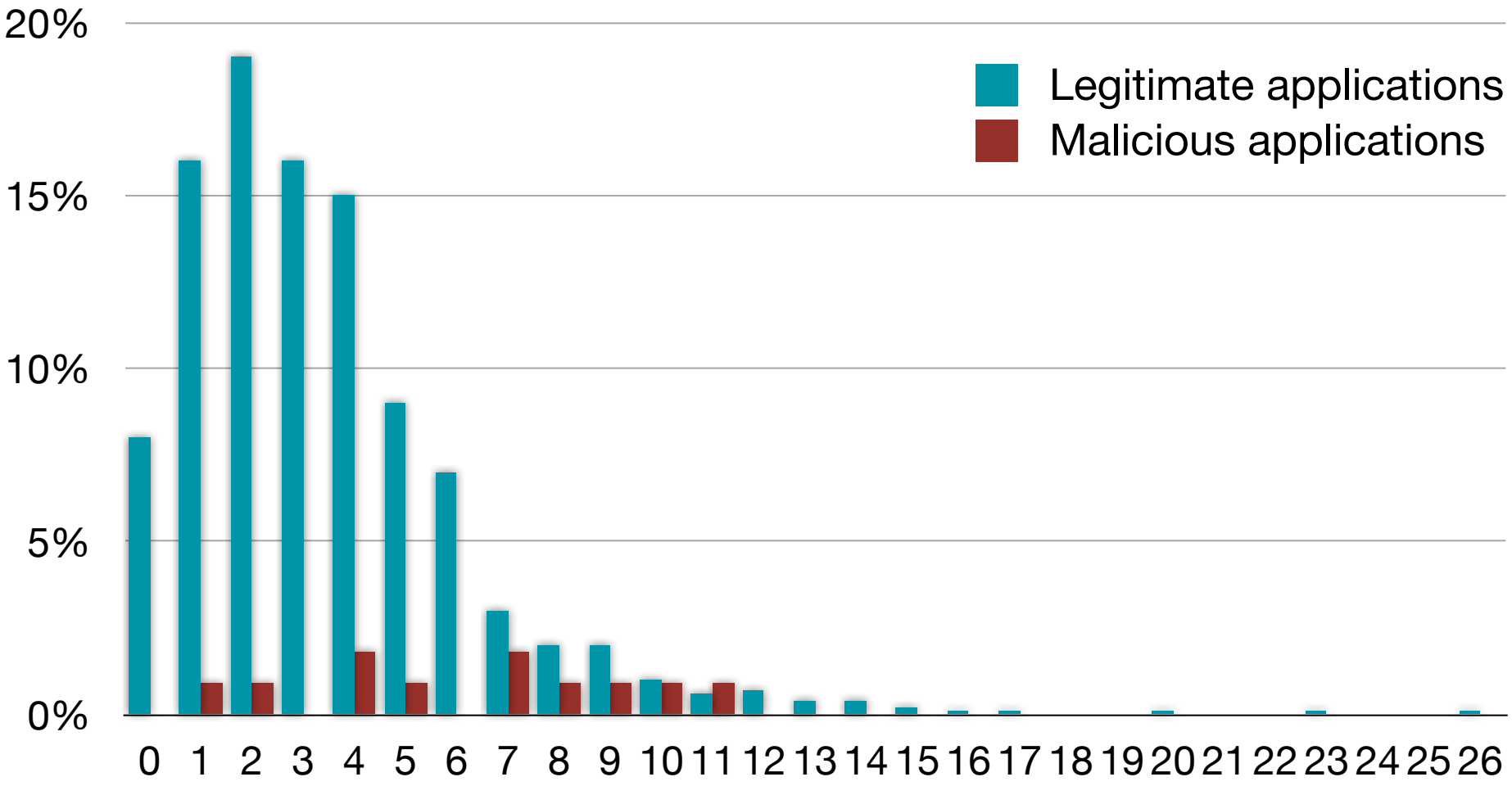
- Do review processes stop malware?
- **0** malware in Apple App Store
- **5** pieces of Symbian Signed malware

ANDROID PERMISSIONS

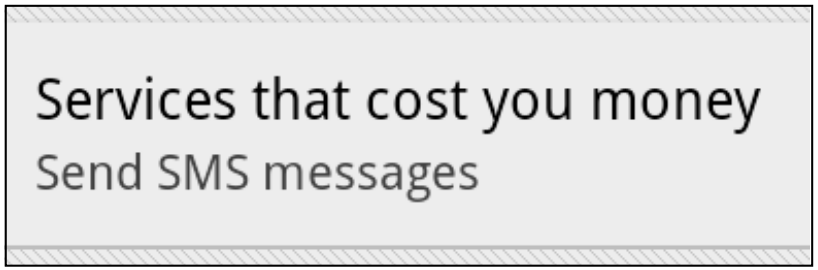


Can they help users (or researchers) identify malware?

OF PERMISSIONS



SMS PERMISSION



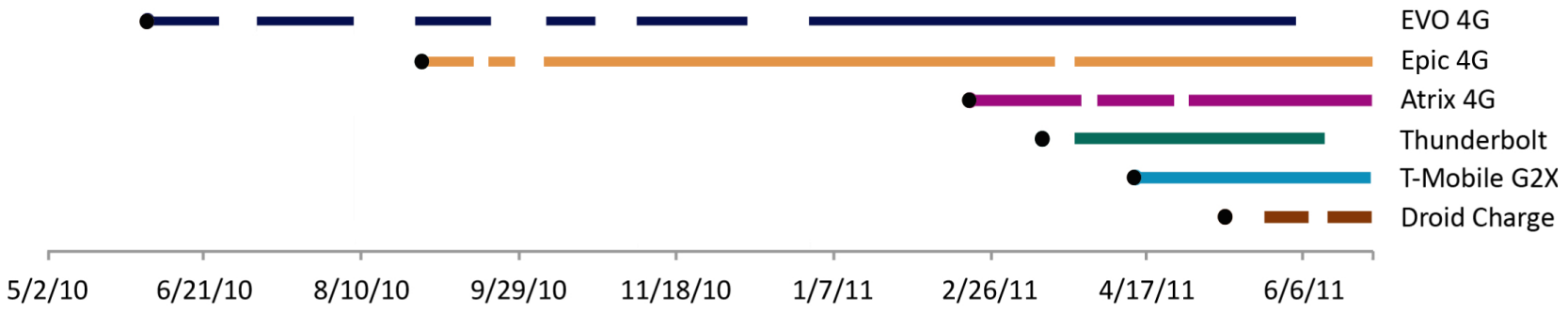
73% of malicious apps
vs
4% of legitimate apps

ROOT EXPLOITS

JAILBREAK

- People want to customize their phones
- So they find and publish **root exploits**
- Malware authors read forums too
  - 4 pieces of malware in our set use them

EXPLOIT AVAILABILITY



Each version remains un-rooted
for an average of 5.2 days

CONCLUSION

- Mobile malware exists, although rare
- Apple's review process is effective; permissions may be useful
- Locking phones indirectly aids malware
- www.cs.berkeley.edu/~afelt/malware.html