UI STATE INFERENCE ATTACK

By: Abhishek Bhole,
Shreyas Bhivandkar

INTRODUCTION

- Team of engineers discovered vulnerabilities were discovered in major operating systems.

MasterMinds
Behind This Research

- Qi Alfred Chen, *University of Michigan*;
  Zhiyun Qian, *NEC Laboratories America*;
  Z. Morley Mao, *University of Michigan*.

- Researchers were able to hack 6 out of 7 popular apps with a whooping 92% success rate.


GUI Security Concerns

- GUI content confidentiality and integrity are critical for end-to-end security.

- URL Spoofing has been a popular example for Integrity comprise.

- Android Malwares which can take screen shots of your android phone compromising confidentiality.

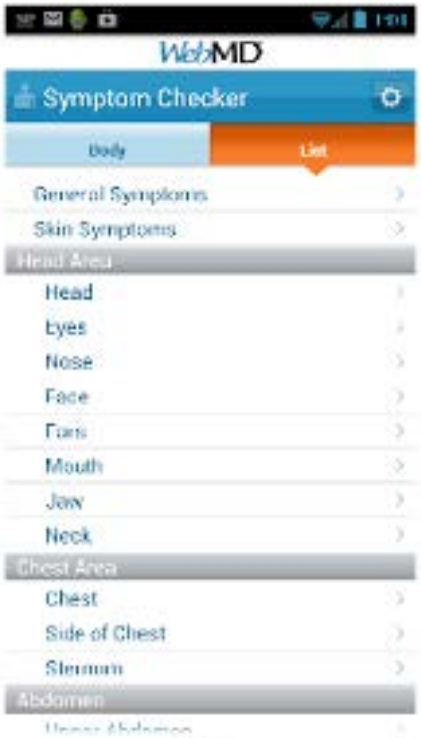

Do you think this was bad enough?
Wait for the Worse!
ANDROID FOUNDRY
ANDROID-FOUNDRY.COM

Define UI State

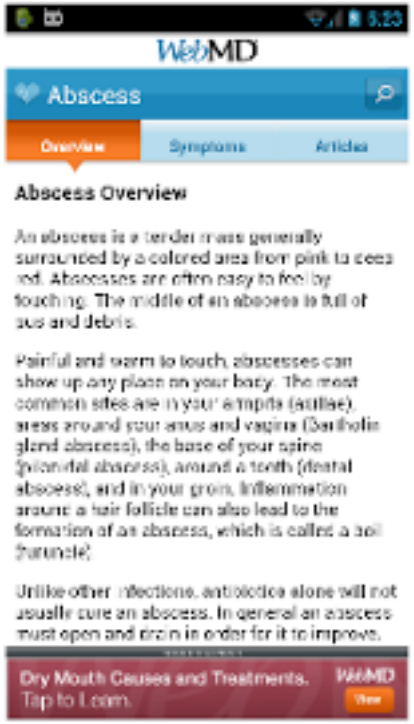
User Interface State (UI State) can be defined as the most consistent UI at window level for certain piece of functionality.

SOME EXAMPLES

Sign-in



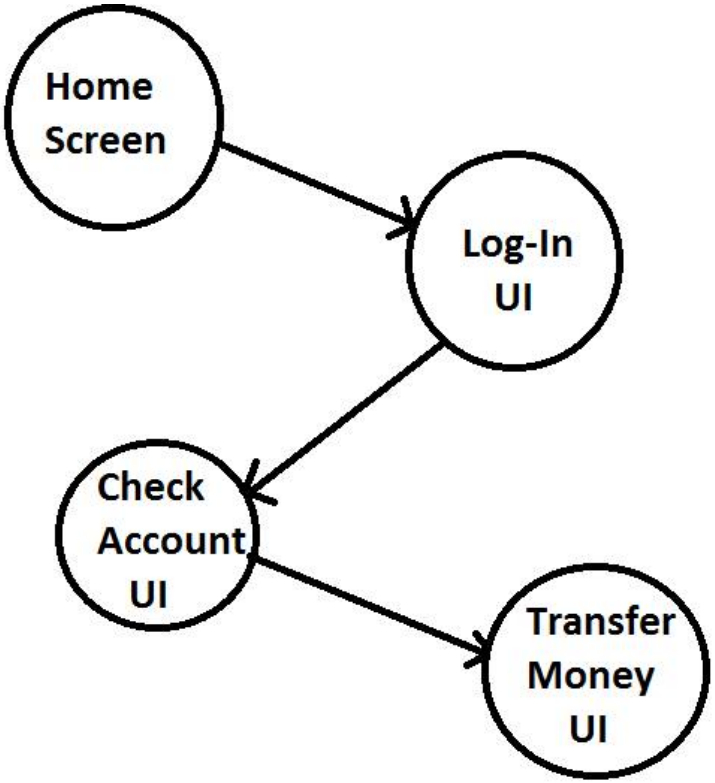
Choose Symptom

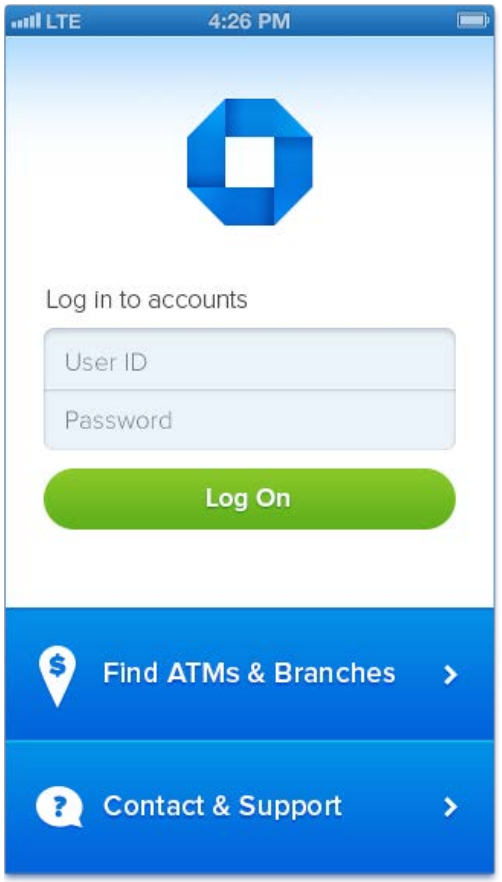


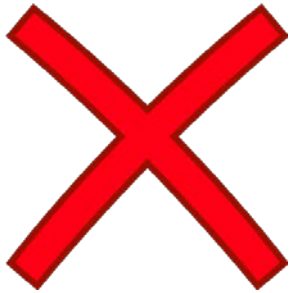
Browse Article

Use UI State, but NOT the Pixels!

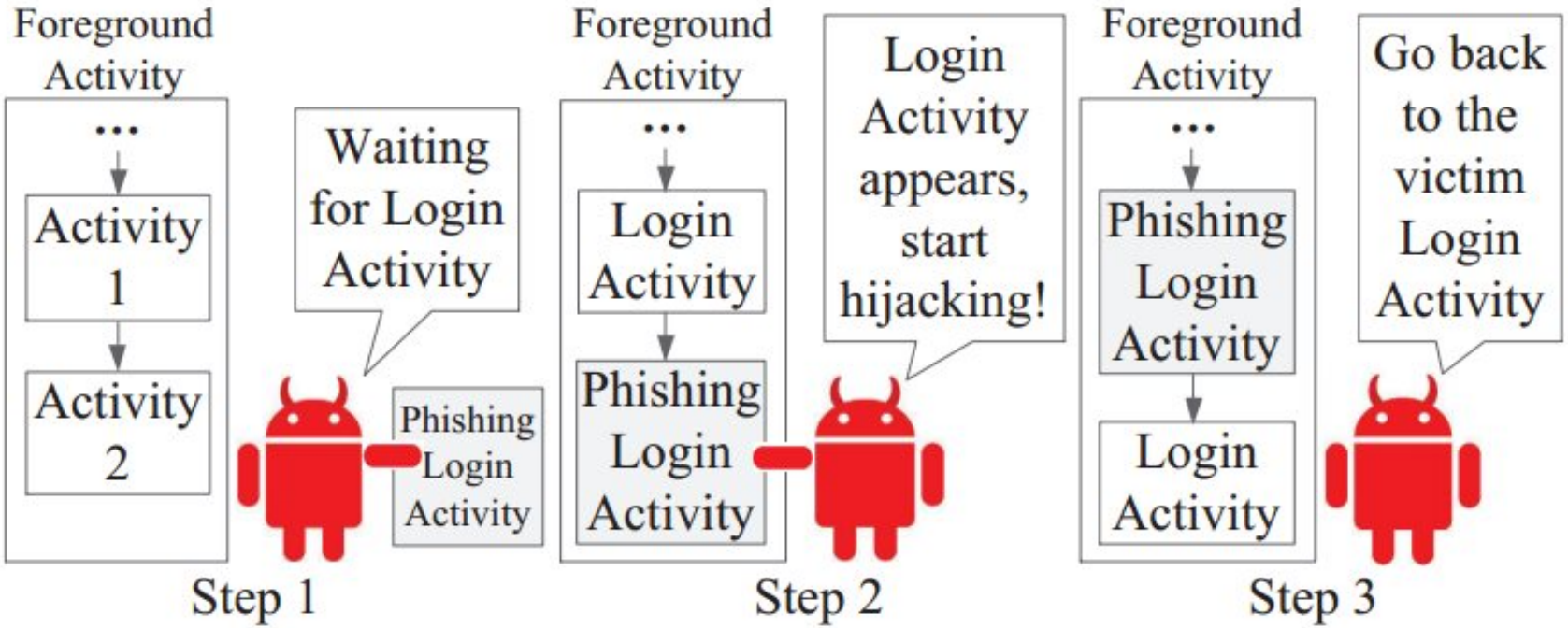
- Attacker can see the UI state, but not read the data from the pixels.

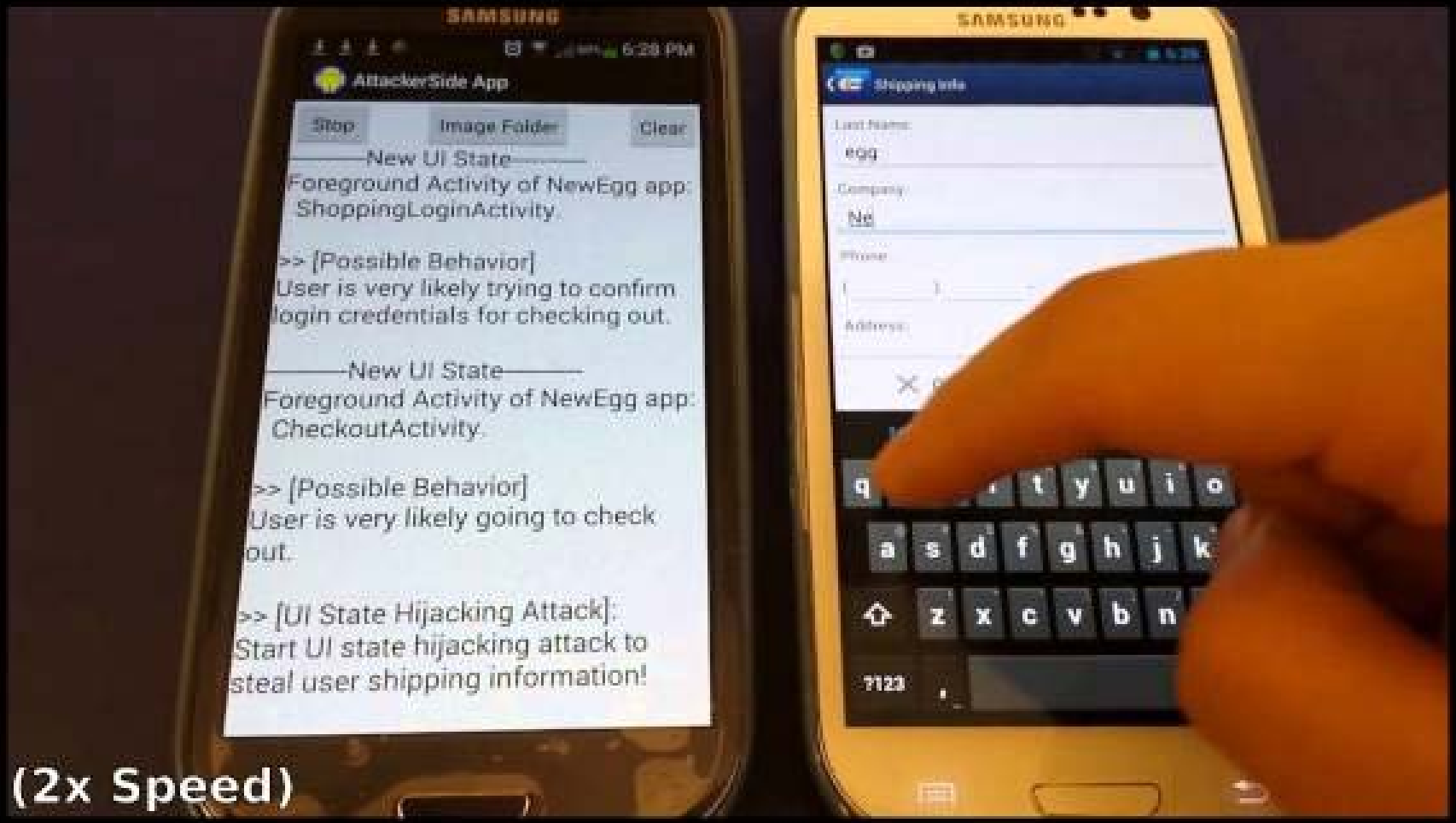

Home Screen
Log-In UI
Check Account UI
Transfer Money UI


LTE
4:26 PM
Log in to accounts
User ID
Password
Log On
Find ATMs & Branches
Contact & Support



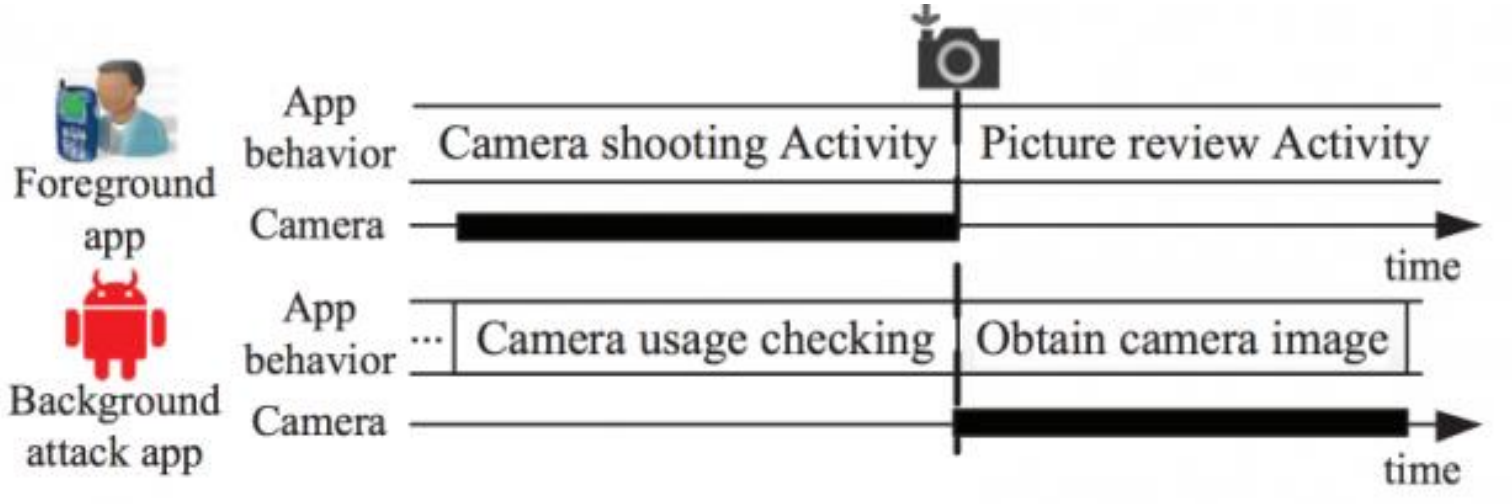
Attack the UI State the App Is In

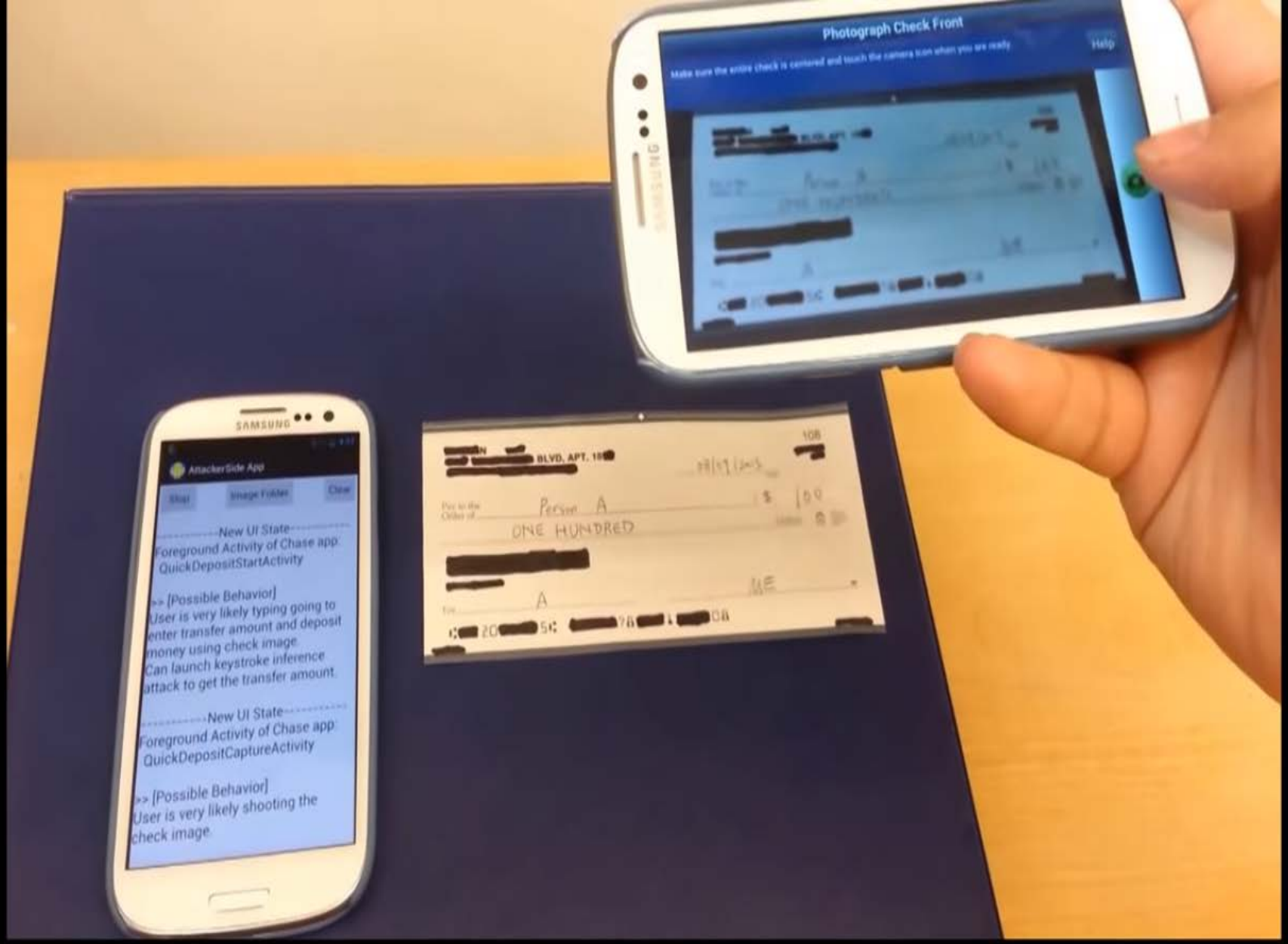




The Activity on the screen now belongs to the attacker.

Camera Peeking





The user is taking photo of the check.

Such kind of Attack which use the UI State to attack is called UI State Inference Attack.

But..

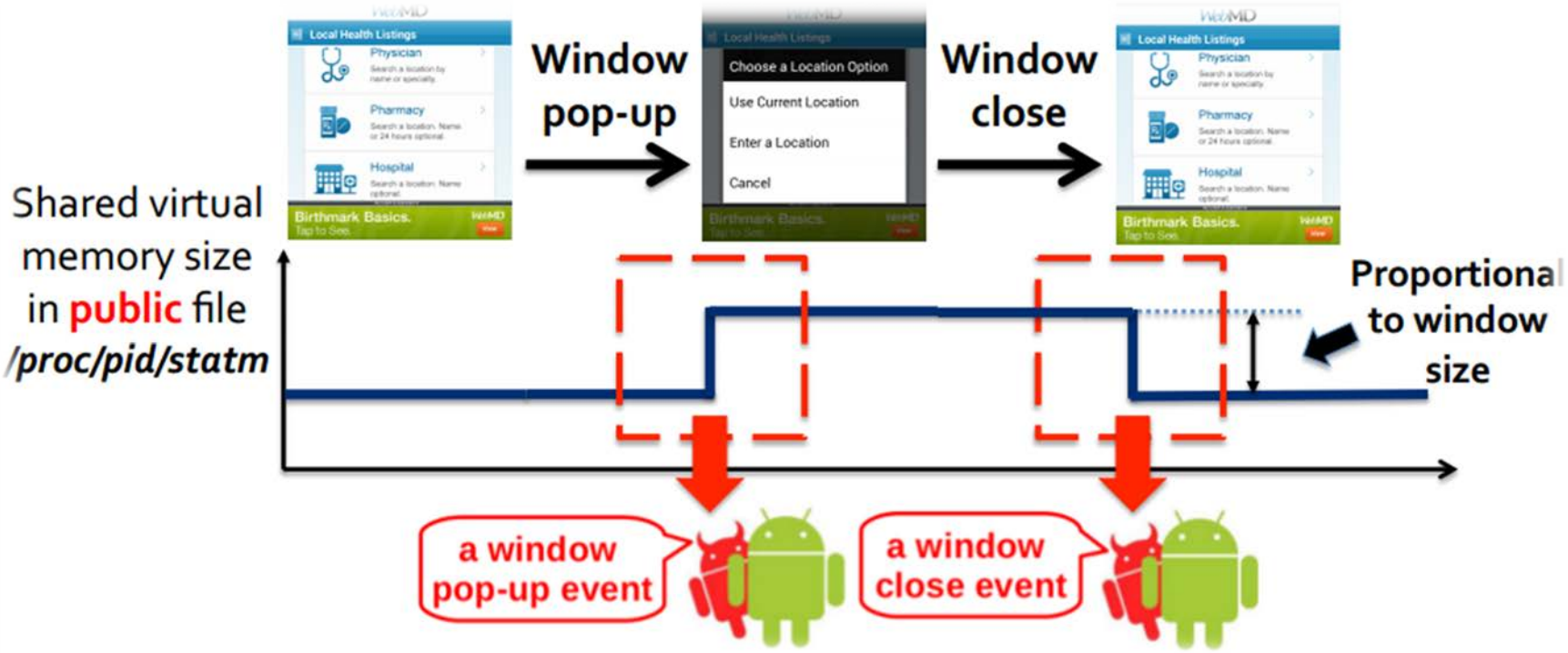
How does it WORK?

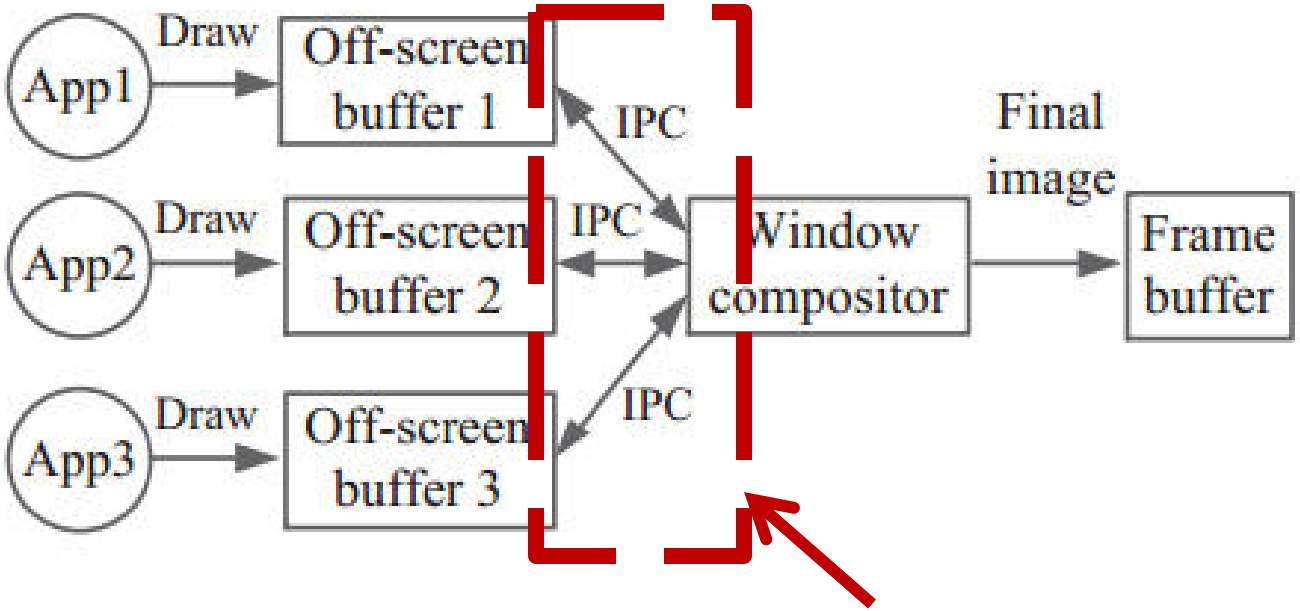
Chen's team detected that-

- An unprivileged app can detect another app's UI state in real time.
- Newly Discovered Shared-Memory Side Channel.
- Hence the Inference Attack which follows requires no Android permission.
- Everyone is Guilty:



Tracing the inference





That's the Problem

For better Performance, most of the OSs uses Shared-Memory as IPC

Broader Security Problems

- These vulnerabilities can lead to identity theft.

QUESTIONS

- **How is UI state interference attack performed?**

- It is performed by creating your own UI state and then infer it in real time from an unprivileged app.

- **What can the hackers get from exploiting this vulnerability?**

- steal users' login details and the social security numbers, address, name, credit card number

- **Which was the only app that the researchers had a hard time hacking into?**

- Amazon with 48% success rate.

Watch these Cool Videos!

- Camera Peeking on Chase App: https://www.youtube.com/watch?v=QZZwiT-Df1U

- Activity Hijacking Attack on H&R Block App: https://www.youtube.com/watch?v=Bbw9AqUVRbc

REFERENCES

- “Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks”, 23rd Usenix Security Symposium, Qi Alfred Chen, *University of Michigan;* Zhiyun Qian, *NEC Laboratories America;* Z. Morley Mao, *University of Michigan, Aug. 2014.*
  < https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/chen>

- "UI State Inference Attack." *UI State Inference Attack*. N.p., n.d. Web. 30 Mar. 2015. <https://sites.google.com/site/uistateinferenceattack/>.

- "Researchers Hack Into Mobile Apps, Find Gmail Most Vulnerable While Amazon Shows Better Resistance." *Headlines Global News RSS*. N.p., 22 Aug. 2014. Web. 30 Mar. 2015. <http://www.hngn.com/articles/39947/20140822/researchers-hack-into-mobile-apps-find-gmail-most-vulnerable-while-amazon-shows-better-resistance.htm>.

- "New Hack Could Steal Personal Information from Gmail, Other Popular Apps." *CBSNews*. CBS Interactive, n.d. Web. 30 Mar. 2015. <http://www.cbsnews.com/news/new-hack-could-steal-personal-information-from-gmail-other-popular-apps/>.