



WILLIAM & MARY

CHARTERED 1693

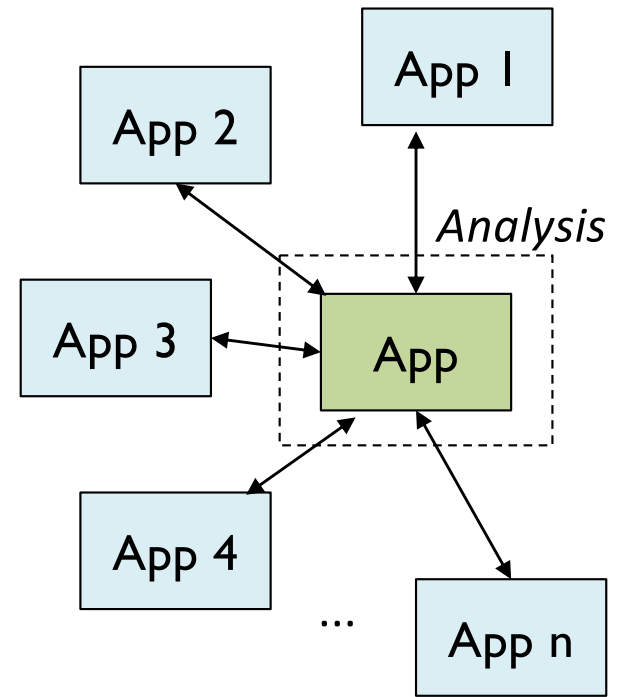
CSCI 445: Mobile Application Security

Lecture 17

Prof. Adwait Nadkarni

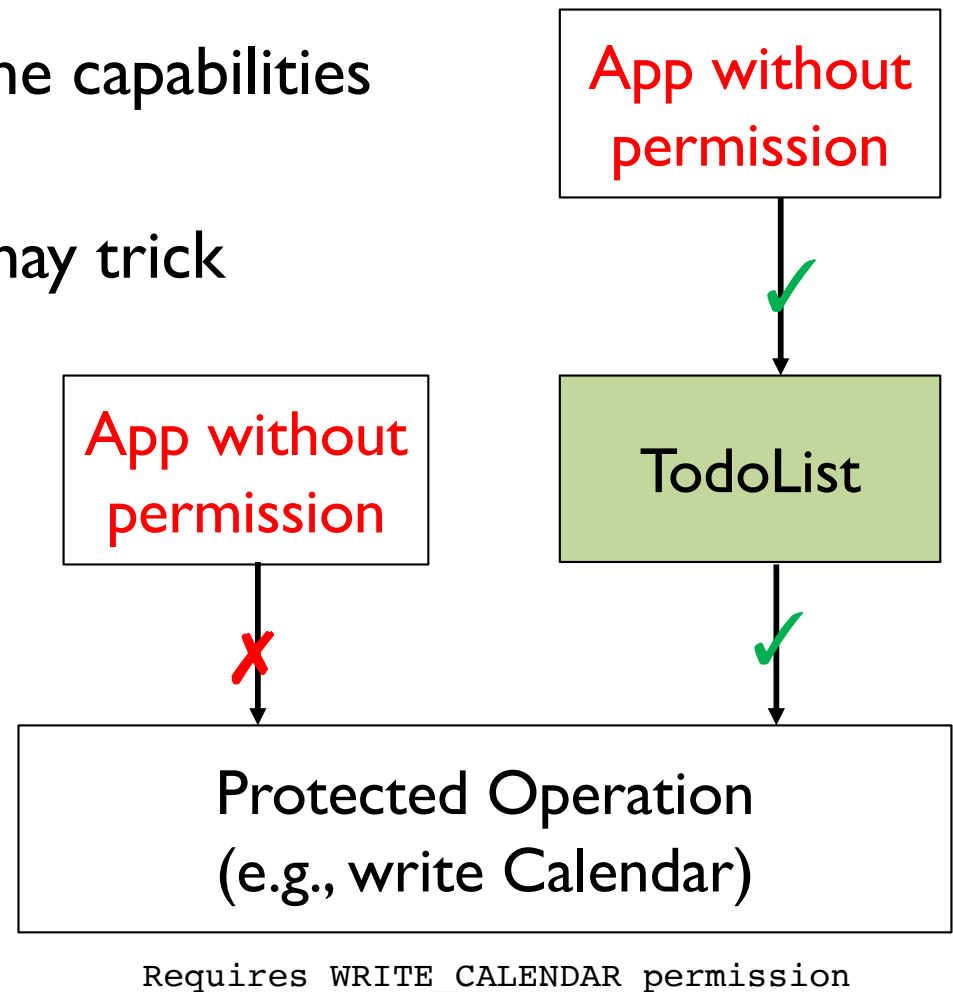
Is permission analysis enough?

- Analyzing the permissions of *one* app
 - Does the app *need* the permissions requested?
 - Does the app request a *high-risk* permission?
 - Or permission combinations?
- *What are we missing?*
 - Multiple untrusted apps
 - Apps communicate!



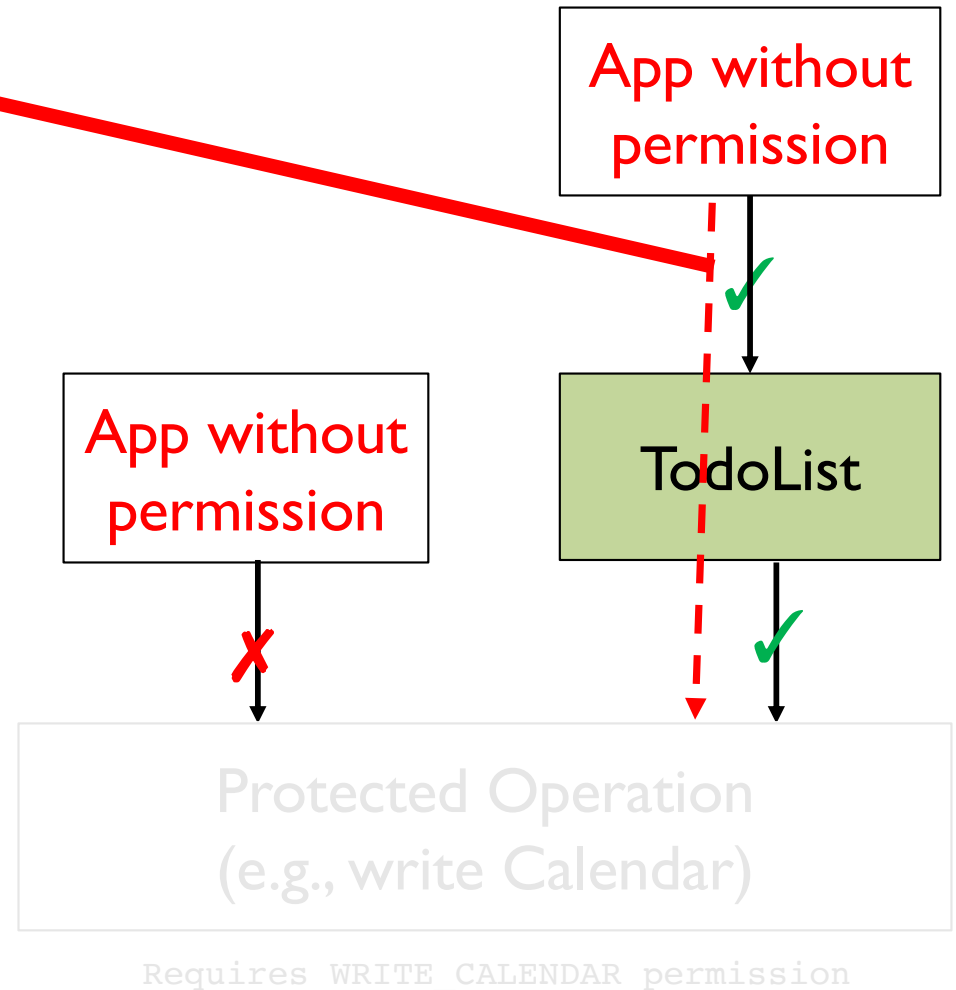
Inter-app communication problems

- *Collusion*: Two apps may combine capabilities (e.g., location + Internet)
- *Confused Deputy*: An attacker may trick vulnerable apps
 - Q: Why does this happen?
 - A: Unprotected interfaces



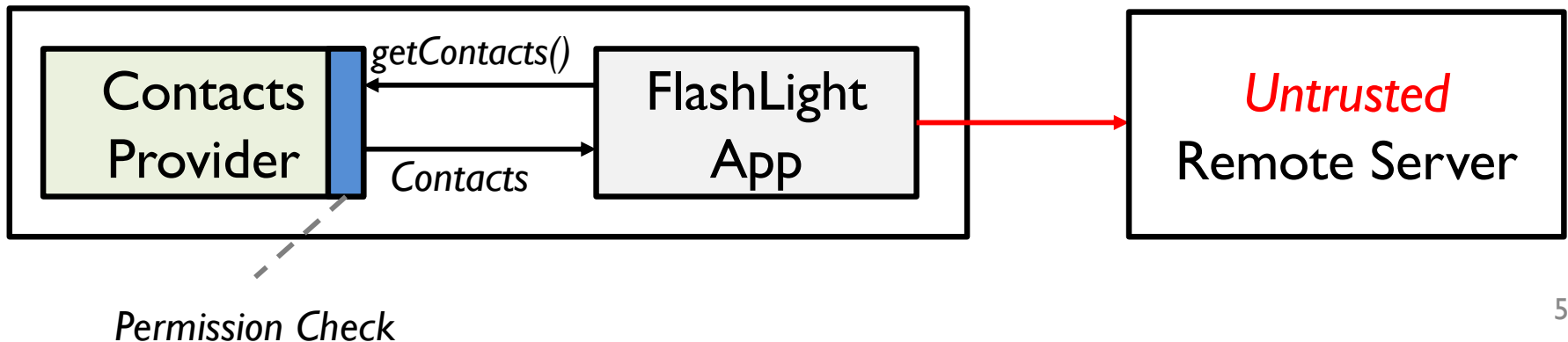
Inter-app communication problems

- Can permissions prevent this *flow*?
 - No; Permissions are *not transitive*
- Can we add transitivity?
 - Enforcing transitivity may result in *over-privilege*



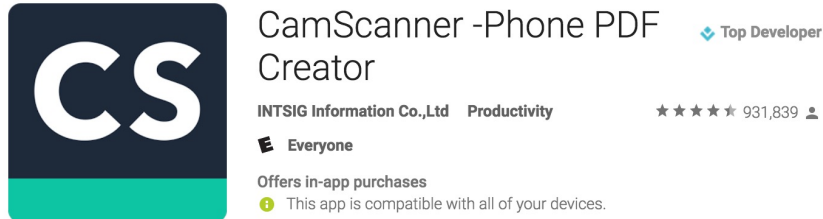
Tracking data leaks

- **Problem:** *An app accesses the user's private data, and exports/leaks it to the network, without the user's consent.*
 - Need to track *information flow*
- **Existing enforcement:** Permissions are only enforced at the first access.
 - Data once accessed is *copied* into the process memory of the receiver.
 - No control over what happens after the copy.



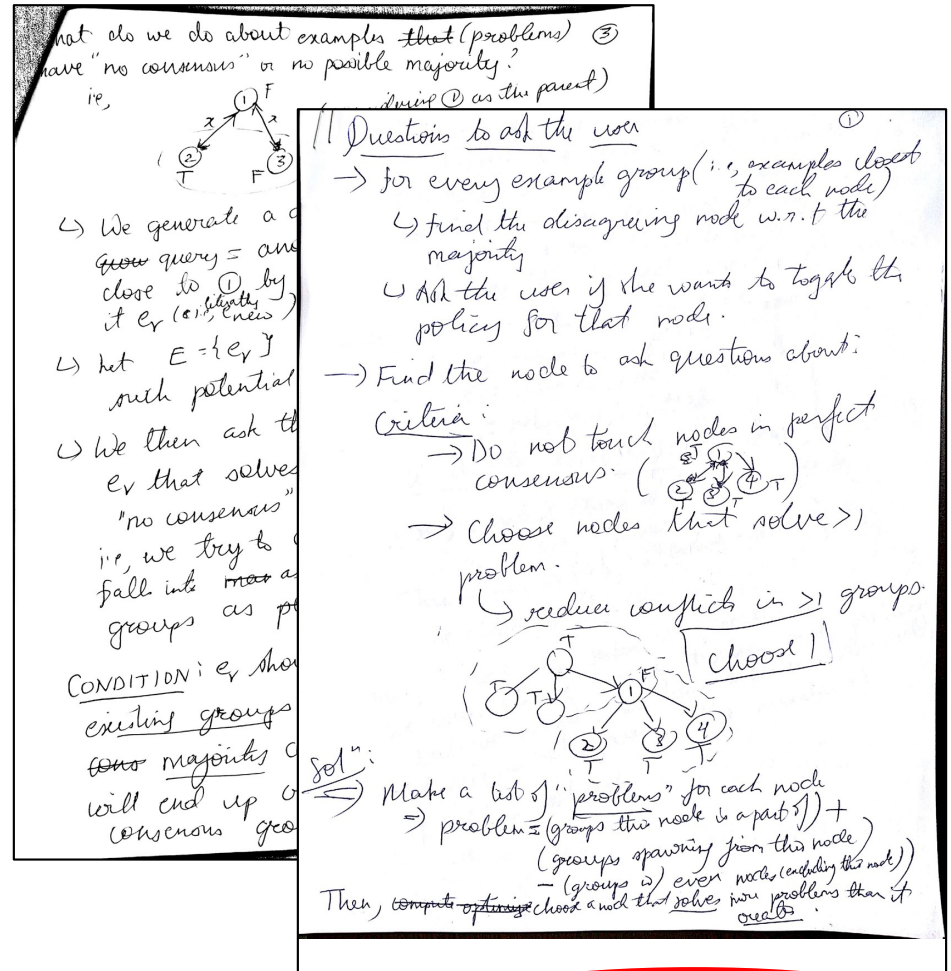
An example

- 2011 - Homework needed to be scanned
- **CamScanner** – Scan with your phone (>50 million Downloads)



CamScanner -Phone PDF Creator
 INTSIG Information Co.,Ltd Productivity Top Developer
 ★★★★★ 931,839
 E Everyone
 Offers in-app purchases
 This app is compatible with all of your devices.

- Premium account, no watermark!



What do we do about examples that (problems) ③
 have "no consensus" or no possible majority?
 i.e.,
 (1) F (2) T (3) F

① Questions to ask the user
 → for every example group (i.e., examples closest to each node)
 ↳ find the disagreeing node w.r.t. the majority
 ↳ Ask the user if she wants to toggle the policy for that node.
 → Find the node to ask questions about:
 Criteria:
 → Do not touch nodes in perfect consensus: (1) F (2) T (3) F (4) T
 → Choose nodes that solve > 1 problem.
 ↳ reduce conflicts in > 1 groups

CONDITION: ev. show existing groups
 no majority
 will end up consensus groups

solⁿ:
 ⇒ Make a list of "problems" for each node
 ⇒ problem = (groups this node is a part of) + (groups spanning from this node) - (groups it even nodes (excluding this node))
 Then, compute ~~optimal~~ choose a node that solves more problems than it creates.

Watermark (free version) →

Scanned by CamScanner

An example

- Premium account removes watermark.
 - Q: What does this have to do with security?
 - A: *“Personal” Cloud Backups*

NC STATE UNIVERSITY

Adwait Nadkarni

U.S. Department of Justice
Immigration and Naturalization Service

Certificate of Eligibility for Nonimmigrant Status - For Academic and Language Study

Please read Instructions on Page 2

For Immigration Official User

Admission number:

North Carolina State University (UNC System)
NC State University

School Official to be notified of student's arrival in U.S. (Name and Title):

UNIVERSITY ADDRESS (INCLUDE ZIP CODE):
OIS
Daniels Hall 320, Box 7222
Raleigh, NC 27695-7222

School code (including 3-digit suffix, if any) and approval date:
ATL214F10206000 approved on 10/14/2002

3. [Redacted] for:

4. [Redacted] issue in the United States:

5. [Redacted] full course of study at this [Redacted]

10. School Certification: I certify under penalty of perjury that all information provided above in items 1 through 9 was complete and is true and correct; I executed this form in the United States after review and evaluation in the United States by me or the student's application, transcripts, or other records of courses taken and proof of financial responsibility, which were reviewed in execution of this form; the school has determined that the above named student's qualifications meet all standards for admission and will be required to pursue a [Redacted] by 8 CFR 214.2(f)(6); I am a designated official of the above named school to issue this form.

Kamon Hester [Redacted] International Admission Specialist 04/15/2011
Name of School Official Signature of Designated School Official Title Date Issued

11. Student Certification: I have read and agreed to comply with the terms and conditions of my admission and those of any other page 2. I certify that all information provided on this form refers specifically to me and is true and correct to the best of my knowledge. I seek to enter or remain in the United States temporarily, and solely for the purpose of pursuing a full course of study at the named school. I also authorize the named school to release any information from my records which is needed by the INS to determine my nonimmigrant status.

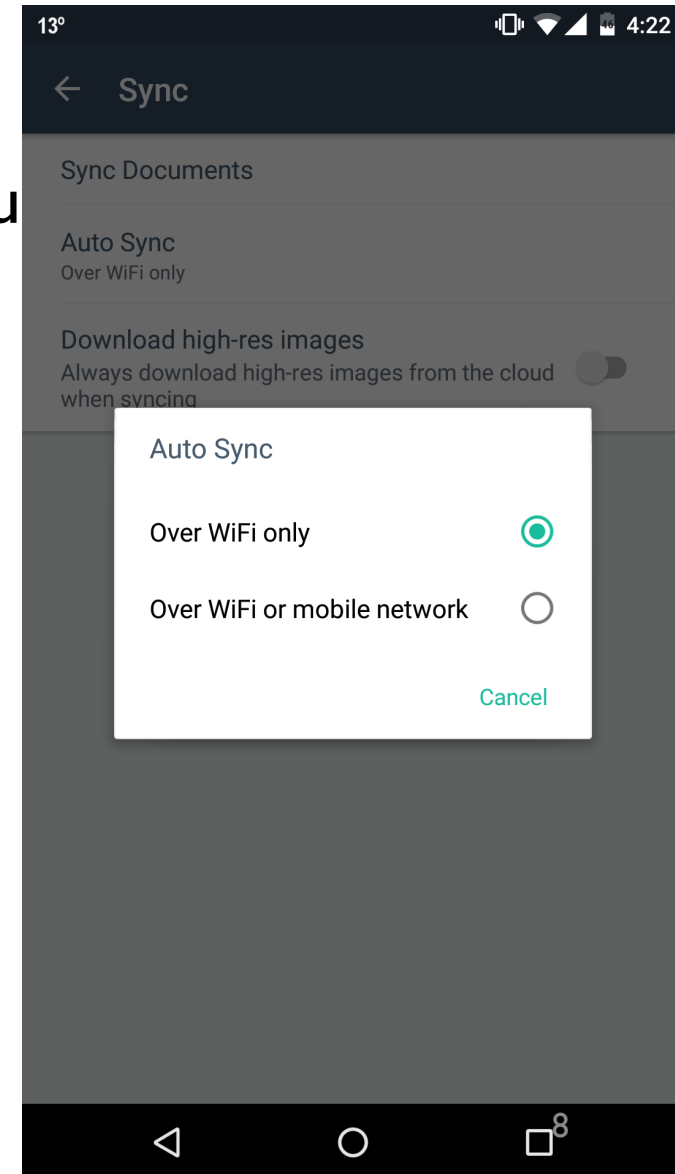
Name of Student [Redacted]

Name of parent or guardian [Redacted] Signature of parent or guardian [Redacted] Address (city) [Redacted] (State or Province) (Country) [Redacted]

Form I-20 A-B (Rev. 04-27-88)N For C

An example

- Premium account removes watermark.
 - Q: What does this have to do with security?
 - A: *“Personal” Cloud Backups*
- Disaster Recovery
 - Disable automatic backup/sync?
 - Not an option



An example

- Premium account removes watermark.
 - Q: What does this have to do with security?
 - A: *“Personal” Cloud Backups*
- Disaster Recovery
 - Disable automatic backup/sync?
 - Not an option
- Takeaway: Users often have to choose between *functionality* and *security*.
 - Sometimes, we may not even be aware of it.



In other news...



AH Android Headlines Android News Tech News Brands Google News

2020 **Android App & Games** Top 10 Best Android Apps & Games

Android App & Games / Massively Popular CamScanner App Delisted Due To Malware

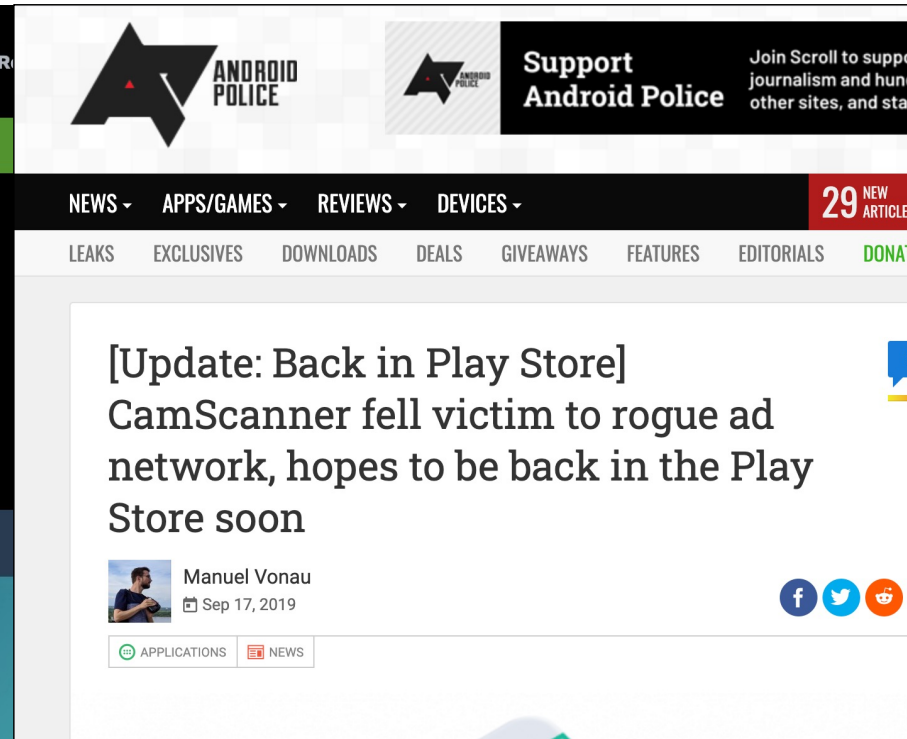
Massively Popular CamScanner App Delisted Due To Malware

By **Daniel Fuller** September 03, 2019

CAM SCANNER Home Download App Pricing Press Media Sign Up Sign In

To address your concerns about the recent controversial reports of CamScanner Android Version, we make the following statement: [View Detail](#)

Mobile Scanner, Easy to use, High quality, Handheld scanner



ANDROID POLICE Support Android Police Join Scroll to support journalism and hunt other sites, and sta

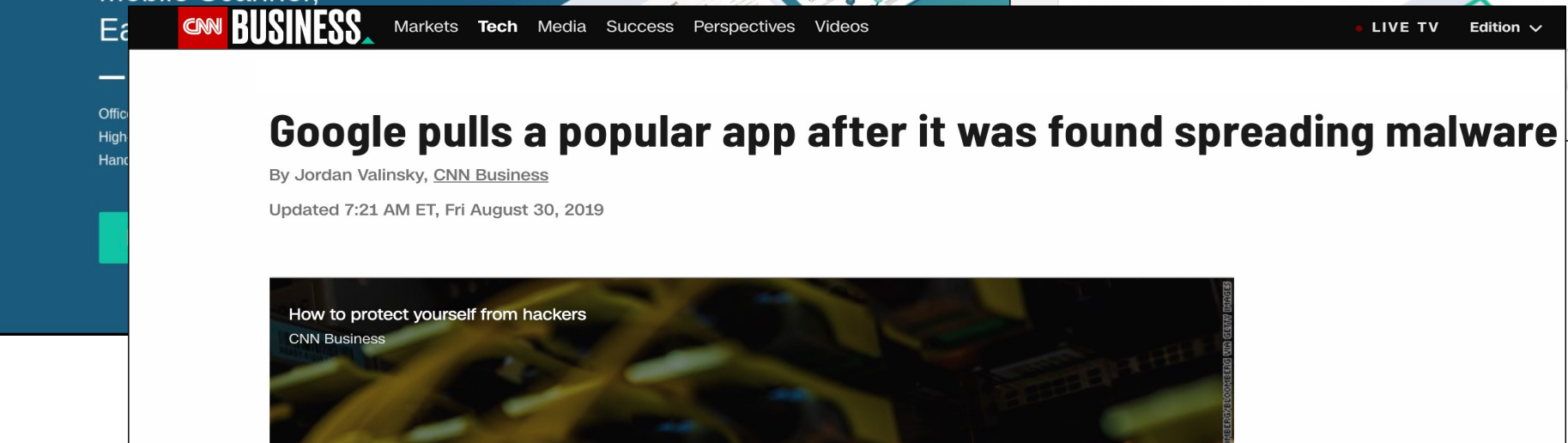
NEWS APPS/GAMES REVIEWS DEVICES 29 NEW ARTICLE

LEAKS EXCLUSIVES DOWNLOADS DEALS GIVEAWAYS FEATURES EDITORIALS DONA

[Update: Back in Play Store] CamScanner fell victim to rogue ad network, hopes to be back in the Play Store soon

Manuel Vonau Sep 17, 2019

APPLICATIONS NEWS



CNN BUSINESS Markets Tech Media Success Perspectives Videos LIVE TV Edition

Google pulls a popular app after it was found spreading malware

By Jordan Valinsky, [CNN Business](#)

Updated 7:21 AM ET, Fri August 30, 2019

How to protect yourself from hackers
CNN Business

Why do apps leak data?

- Malware/ Spyware
- Advertising (aggressive ad libraries may be packaged with apps)
- Accidentally
 - Bug reports
- Unwanted features/ add-ons
 - Without user consent or awareness



Implications of Data Leaks

1. Loss of privacy: Privacy Policy Violations

- E.g., HIPPA (medical data), GLBA (financial data), GDPR, CCPA, ...

2. Loss of confidentiality

- Bring your own device (BYOD): Exfiltration of work data

3. Loss of reputation (for apps)

- E.g.: Facebook lost \$60 billion in valuation

<https://techcrunch.com/2018/03/31/who-gains-from-facebooks-missteps/>

Detecting Data Leaks

Taint Tracking

- Taint analysis/tracking is a technique that tracks information dependencies from an origin
- *For detecting data leaks, we track flows from source → sink*
- Important terms:
 - Taint *source* (e.g., `getIMEI()`)
 - Taint *sink* (e.g., `network_send()`)
 - Taint *propagation*
 - The taint follows the data, *even copies of data*

```
c = taint_source();  
←  
...  
a = b + c  
←  
...  
network_send(a)
```

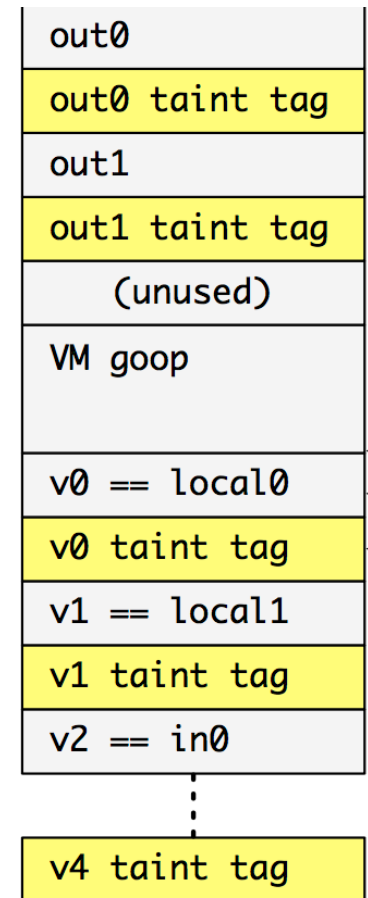
TaintDroid

- *Dynamic, variable-level* taint tracking
- Tracks export of private data to the network
- Sources: *Sensitive API calls* (e.g., *get IMEI, location*)
- Sinks: Network API (e.g., creating sockets)
- Modification to the firmware
 - Adds taints when sensitive APIs are first called
 - Tracks taints at runtime
 - Raises alarm when tainted data is exported

```
c = getDeviceID();  
←  
...  
a = b + c  
←  
...  
network_send(a)
```

Variable-level Tracking in VM

- TaintDroid modifies the Dalvik VM interpreter to *store* and *propagate* taint tags (a taint bit-vector) on variables. *Why use a bit vector?*
 - A 32-bit vector can store 32 taint values
- *Local Variables/args*: Taint tags are stored adjacent to the variable on the internal execution stack
- *Class fields*: Similar to locals, but inside static and instance field heap objects
- *Arrays*: One taint tag per array. Why?
 - To minimize performance overhead













Taint Propagation Logic

- Can also represent bit vector as a *set*
 - i.e., if bits/taints for IMEI and Contacts are “set” in label L_X for variable X , then $L_X = \{\text{IMEI}, \text{Contacts}\}$
- Consider variables A ($L_A = \{\}$) and B ($L_B = \{\text{IMEI}\}$)
- Consider the assignment: $A := B$; what is L_A now?
 - $L_A = \{\text{IMEI}\}$
- Consider C ($L_C = \{\text{LOC}\}$), & the assignment $A += C$; what is L_A ?
 - $L_A = L_A \cup L_C = \{\text{IMEI}\} \cup \{\text{LOC}\} = \{\text{IMEI}, \text{LOC}\}$
- This is known as *floating labels* (the labels/taints float with the data, i.e., propagate in the direction of the flow of data)

Privacy Study (TaintDroid)

- Selected 30 applications with bias on popularity and access to *Internet*, *location*, *microphone*, and *camera*

applications	#	permissions
The Weather Channel, Cetos, Solitarie, Movies, Babble, Manga Browser	6	
Bump, Wertago, Antivirus, ABC --- Animals, Traffic Jam, Hearts, Blackjack, Horoscope, 3001 Wisdom Quotes Lite, Yellow Pages, Datelefonbuch, Astrid, BBC News Live Stream, Ringtones	14	 
Layer, Knocking, Coupons, Trapster, Spongebot Slide, ProBasketBall	6	  
MySpace, Barcode Scanner, ixMAT	3	
Evernote	1	  

- Of 105 flagged connections, only 37 clearly legitimate*

Tradeoffs

- **Advantages:** *Precise analysis* (mostly): If an alarm is raised, its very likely a true positive
 - Excluding cases where the export is legitimate
 - Precision is mostly due to the fine-grained variable-level tracking, as well as the dynamic nature of the analysis.
- **Limitations:**
 - *Soundness: False negatives* due to the challenges in executing all possible code paths
 - Variable-level granularity dynamic analysis may not detect *implicit* flows (more on the next slide)
 - Cannot protect against a *malicious* adversary

Other Limits to precision

- Persistent Storage: Tracked at the *file-level*
 - How does this impact precision? → False positives for fine-grained database accesses
- Native code: Apps execute *native methods* through the Java Native Interface (JNI)
 - Method-level tracking: Propagate taint to method call, and then to the return value.
 - How does this affect precision? → coarse-grained tracking of native code

Implicit Flows

- Data may be inferred from from *control flows*

```
//'a' contains a secret
```

```
b = false;
```

```
if (a == 0) {
```

```
    b = true;
```

```
}
```

- *b* has the value of *a*, but not tainted

- Can we use static analysis *in conjunction* to detect implicit flows?

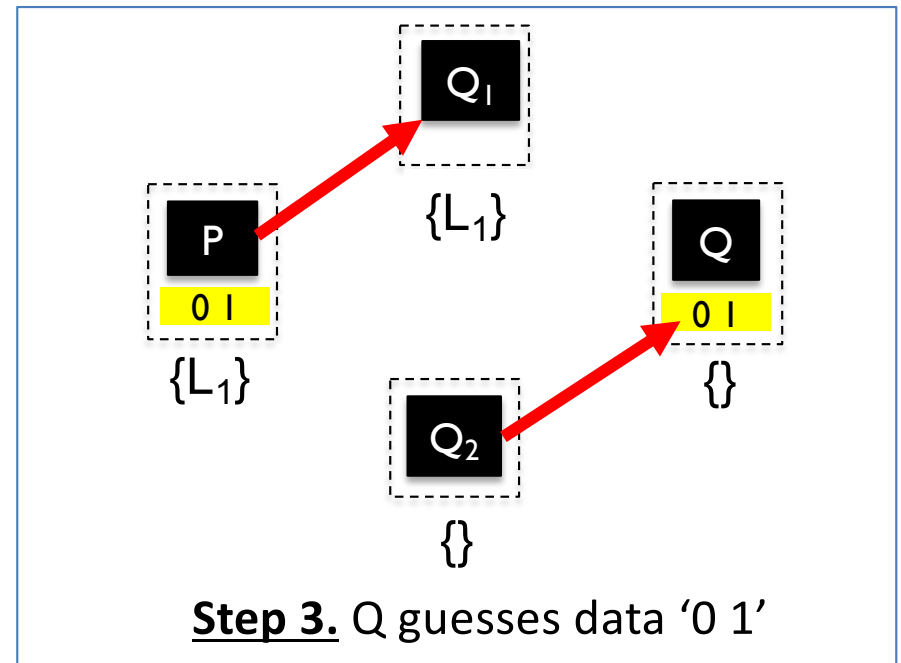
More Implicit Flows

Denning, 1976

```
1 //a is secret
2 b := c := false
3 if ~a then c := true
  if ~c then b:=true
```

$a \rightarrow b$ without label
propagation: *because either $c:=true$ or $b:=true$ were not executed*

Krohn & Tromer, 2009



Attack Setup:

- P sends a message to Q_i if the i^{th} bit is '0'
- All the Q_i s send Q a message at a fixed time interval, *unless* they have received a message from P

FlowDroid, Argus, ...

- *Fine-grained, static, data flow* analysis
- Model's Android's Lifecycle. Why?
 - There is no single *main* method
 - Support various *entry points*: lifecycle callbacks, UI callbacks, etc.
- Q: Can we detect implicit flows with FlowDroid?
- A: Yes!
- What do we lose?
 - Precision: Some flows may not execute in reality
 - Inter-app flows: Need the user's context, which is only available at runtime

The End