ReCon: Revealing and Controlling PII Leaks in Mobile Network Systems

Jingjing Ren, Martina Lindorfer, Ashwin Rao, Arnaud Legout, David Choffnes
(MobiSys ‘16)

Presented by : Umar Farooq
CS 563
Fall 2018
Mobile Phones today..

- Offer ubiquitous connectivity
- Equipped with a wide array of sensors
- Examples: GPS, camera, microphone etc.
Problems

- Personally identifiable info. (PII) leakage
  - Device Identifiers (IMEI, MAC address, etc.)
  - User Information (name, gender, contact info, etc.)
  - Location (GPS, zip code)
  - Credentials (?)

- Device Fingerprinting
- Cross Platform tracking
User Identifier (email, name, gender etc.)
Contact Info
Location
Credential (username, password)
Device Identifier (IMEI, Advertiser ID, MAC etc.)

App Store  Google Play  WP Store
Goals for this work

- Identify PII leakage without a priori information
- Provide users a platform to view potential PII leaks (i.e. increase user visibility and transparency)
Approach..

- **Opportunity:** Almost all devices support **VPNs**
- Have a trusted third party system to audit network flows
  - Tunnel traffic to a controlled server (trusted server)
  - Measure, modify, shape or block traffic with user opt in
Why should this work?
So, what does a PII look like?

GET
/index.html?id=12340;foo=bar;name=CS563@Illini;pass=jf3jNF#5h

How can we identify a PII leak?
Naïve approach: Pattern matching.
ReCon:

A system using supervised ML to accurately identify and control PII leaks from network traffic with crowdsourced reinforcement.
Automatically Identifying PII leaks

Hypothesis: PII leaks have distinguishing characteristics

- Is it just simple key/value pairs (e.g. “user_id=563”)
  - Nope, leads to high FPR (5.1%) and high FNR (18.8%).

Need to learn structure of PII leaks.

Approach: Build ML classifiers to reliably detect leaks.

- Doesn’t require knowing PII in advance
- Resilient to changes in PII formats over time.
Initial Training

- Manual test: top 100 apps from each official store
- Automatic test: top 850 Android apps from a third party store
Initial Training

- Feature extraction: bag of words
3.3 Protecting User Privacy

We deployed heads [44]. We are also in discussions with Telefonica to provide immediate cross-platform support with low overhead.

3.2 Deployment Model and User Adoption

When it comes to deploying ReCon, we leveraged information flow analysis techniques to improve its environment. For example, information flow analysis [21] may be used to filter and identify PII leaks. To achieve this, we train a classifier (bottom). Periodically, we update our classifier with results from new network flows. Based on user feedback, we retrain our classifier (top), then use this model to predict whether new network flows are leaking PII. Based on user feedback, we retrain our classifier (top), then use this model to predict whether new network flows are leaking PII. When a leak is detected, we can use thresholds to remove infrequent or too frequent words.

- Feature extraction: bag of words
- Use thresholds to remove infrequent or too frequent words
- Ground truth from the controlled experiments
- C4.5 decision tree
- Per-domain and per-OS classifier
ReCon architecture

Figure 1: Initial Training

Figure 2: Features

Flow contains /user/

Flow contains session

Flow contains deviceId

Initial Training

Initial Training

Flows

Features

Training

Model

Negative

Positive

Negative

Positive

Negative

Negative

Positive

Negative

Positive
3.3 Protecting User Privacy

Attracted thousands of users.

3.2 Deployment Model and User Adoption

We are also in discussions with Telefonica to provide immediate cross-platform support with low overhead service on ISP, or on mobile devices. We are currently hosting this service on a home router, a dedicated server in an enterprise, on the device itself, or VM in the cloud. One can also selectively leverage information flow analysis techniques to improve its coverage, as we demonstrate in §5.3. Importantly, because there is no standard token (e.g., a PII leaks and actions that appears in a flow is set to 1, and each word that does not flow, we produce a vector of binary values where each word thing between those separators to be words. Then for each problem, we choose certain characters as separators and consider any-

4. RECON IMPLEMENTATION

4.1 Machine Learning Techniques

We now discuss key aspects of our implementation. We choose certain characters as separators and consider any-

Figure 2: Initial Training [Image]

Figure 1: Continuous training with user feedback

An important concern with a user study is privacy. Using an IRB-approved protocol [6], we encrypt and anonymize all captured flows before storing them. We have demonstrated how they hold up "in the wild" via a user study, our system requires only that a user has root on a Linux OS.

Because the stability of our results (see §5), we encrypt and anonymize all captured flows before storing them. We have demonstrated how they hold up "in the wild" via a user study, our system requires only that a user has root on a Linux OS.
Evaluation – Accuracy (CCR)

- DT outperforms Naïve Bayes
- Time: DT based ensembles take more time than a simple DT
- More than 95% accuracy per-domain-and-per OS
- Greater than the General Classifier
- 60% DTs zero error.
Evaluation – Accuracy (AUC)

- Area under the curve (AUC) [0,1]
  - Demonstrates the predictive power of the classifier
- Most (67%) DT-based classifiers have AUC = 1
Evaluation – Accuracy (FNR and FPR)

Most DT based classifiers have zero FPs (71.4%) and FNs (76.2%)
Evaluation – Comparison with IFA

Information flow analysis (IFA)

- Resilient to encrypted / obfuscated flow
  - Dynamic IFA: Andrubis
  - Static IFA: Flowdroid
  - Hybrid IFA: AppAudit

Susceptible to false positives, but not false negatives
ReCon vs. static and dynamic analysis

The chart compares ReCon with other analysis methods for identifying device, user identifier, contact info, and location. The methods include:

- FBvDroid (Static IFA)
- Andrubis (Dynamic IFA)
- AppAudit (Hybrid IFA)
- ReCon

The y-axis represents the percentage, ranging from 0% to 1200%. The x-axis lists the aspects being analyzed: Device Identifier, User Identifier, Contact Info, and Location.
3.3 Protecting User Privacy

attracted thousands of users.

deploy heads [44]. We are also in discussions with Telefonica to
provides immediate cross-platform support with low over-

service on ISP, or on mobile devices. We are currently hosting this

ment models,

3.2 Deployment Model and User Adoption

flows from arbitrary devices without requiring OS modifica-

allows us to identify and block unobfuscated PII in network

coverage, as we demonstrate in §5.3. Importantly,

leverage information flow analysis techniques to improve its
identify PII leaks not revealed by

ronment. For example, information flow analysis [21] may

how their PII is leaked, validate the suspected PII leaks, and create custom

Figure 2: 

Figure 1: 

Because

(a) PII leaks and actions

(b) Map view of location leaks

ReCon

architecture

Continuous training with user feedback

User Feedback

Initial Training

initially select features and train a model

We use the

with parsing network flows, then passing each flow to a ma-

An important concern with a

weka
data mining tool [25] to train classifiers

An important concern with a

Meddle

Rewriter

User Interface

Users can view

anonymize all captured flows before storing them. We have

An important concern with a

occurred) and users consent via an online form. The secret key

An important concern with a

Feature extraction.

Feature extraction.

For example, a

is set to 0.

is set to 1, and each word that does not

thing between those separators to be words. Then for each

choose certain characters as separators and consider any-

problem,

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

the stability of our results (see §5).

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

weka
data mining tool [25] to train classifiers

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.

Feature extraction.

An important concern with a

for accuracy. This process is repeated

the classifier, and the remaining

flow contains PII is similar to the document classification

Feature extraction.
ReCon:

- The retraining phase is important
  - FP decreased by 92%
  - FN increased by 0.5%
ReCon in the wild

- 239 users in March 2016 (IRB approved)
- 137 iOS, 108 Android devices
- 14,101 PII found and 6,747 confirmed by users
- 21 apps exposing passwords in plaintext
  - Used by millions (Match, Epocrates)
  - Responsibly disclosed
Discussion

Challenges

- Encrypted Traffic (totally reliant on plaintext traffic)
- 10-fold cross validation, does it help?
  - 2.2% FP and 3.5% FN, but what about overfitting?
  - Network flows too diverse, is the model generalizable?
- Can miss out on PII leaks (FN) if model not trained for that class of PII. Standard program analysis susceptible to false positives, but not false negatives
Discussion - continued

- Can we use this approach for IoT devices?
  - Device Identification?
  - PII leakage?
  - Monitor if IoT devices “talk” to themselves?
Questions?