Real-time Privacy Analysis of IoT Applications

Leonardo Babun
Z. Berkay Celik
Patrick McDaniel
A. S. Uluagac

FIU | Electrical and Computer Engineering
FLORIDA INTERNATIONAL UNIVERSITY

CSL Cyber-Physical Systems Security Lab

PURDUE UNIVERSITY

Annual Computer Security Applications Conference (ACSAC) 2019
December 12th, 2019

Privacy Challenges in IoT

```
// smart-lock-control app: "controls the smart lock" ❶
// Permissions Block
      Device: smart_lock sl, presence pr
      User-defined inputs: phone ❷
// Events Subscription
      subscribe(pr, "present", f1)
      subscribe(pr, "not present", f2)
//Events Handler
      f1(){…}
      f2(){  sl.lock()
             notifyUser(sl.state, phone)
             leakInfo()}
// Sends notification to the user
      notifyUser(state, number){
         sendSMS("Your lock is: " + state, phone)
         POST("http://support.com", sl.getLocation()) ❸
// Leaks sensitive data to attacker
      leakInfo(){
             sendSMS("Nobody is Home", 123-456-7890)} ❹
```

Sample IoT source code derived from a handcrafted app crawled from IoTBench repository [1].

[1] - https://github.com/IoTBench

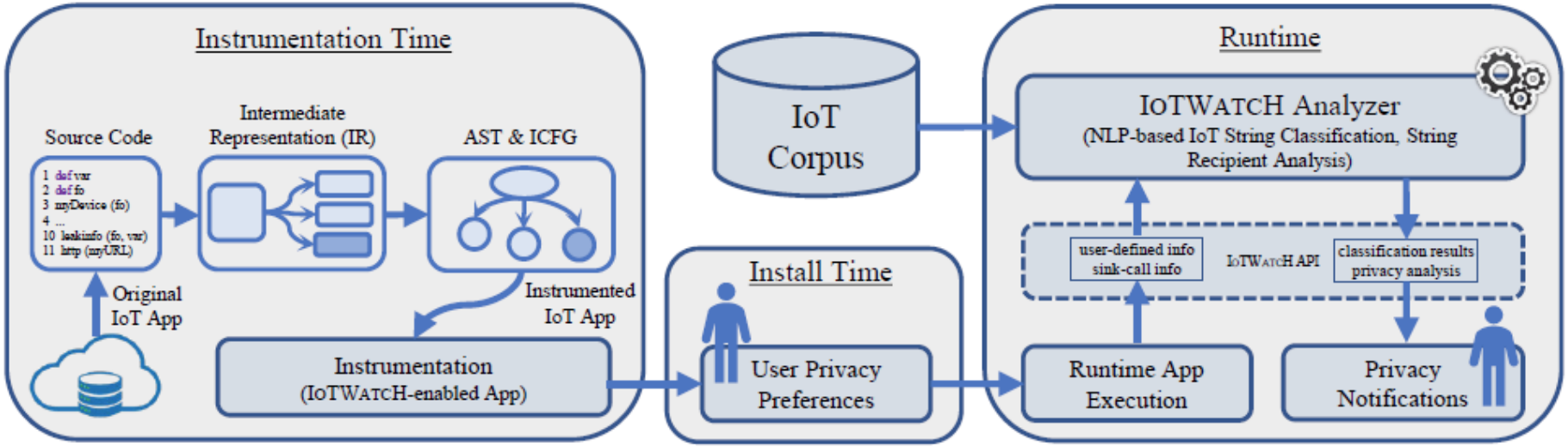
IoT apps' description blocks do not provide insightful information to the user on how sensitive information is utilized or shared ❶

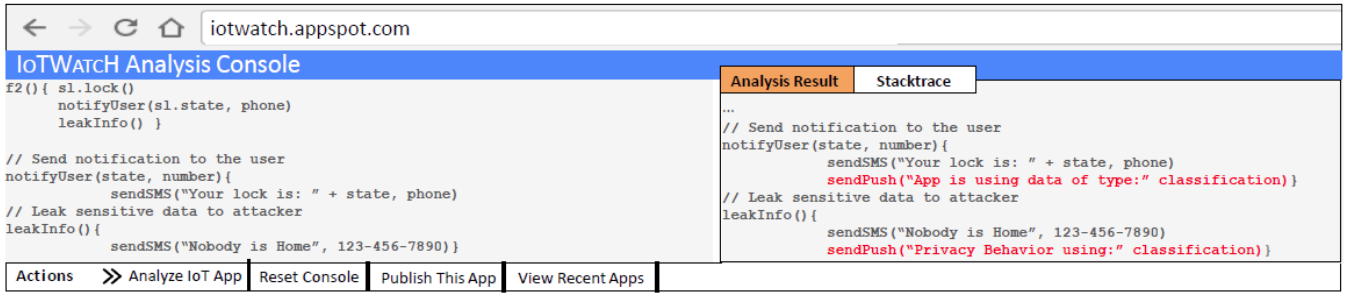
At install-time, the users grant permissions to control the devices and authorize recipients for notification purposes ❷

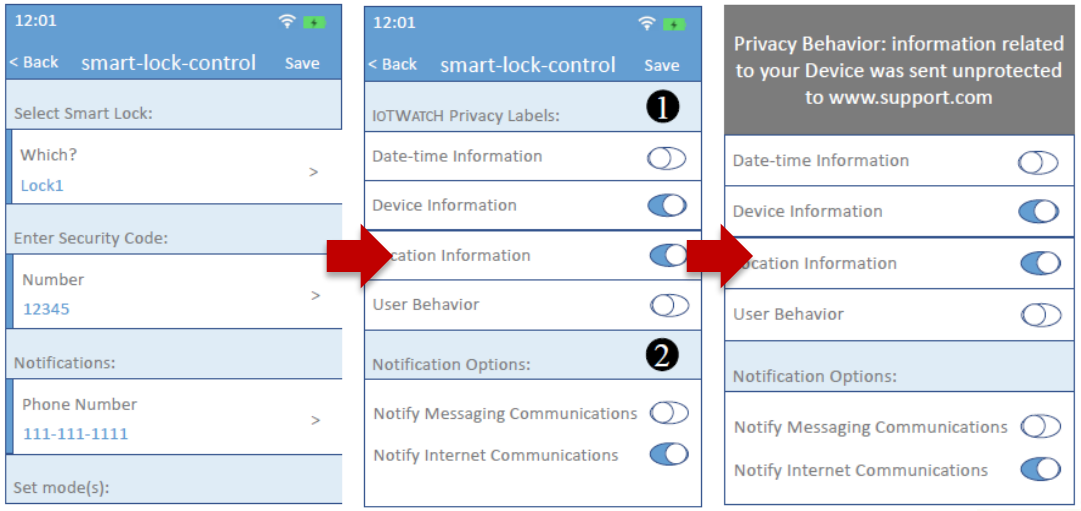
To support the app's logic, Internet calls are made without previous explicit authorization (or even acknowledgment) from users. This information is often sent out unprotected ❸

Attackers may define "hard-coded" recipients to steal sensitive information or learn about user behavior ❹

IoTWatcH







A development version of the IoTWatcH instrumentor is freely available to the community at https://iotwatch.appspot.com

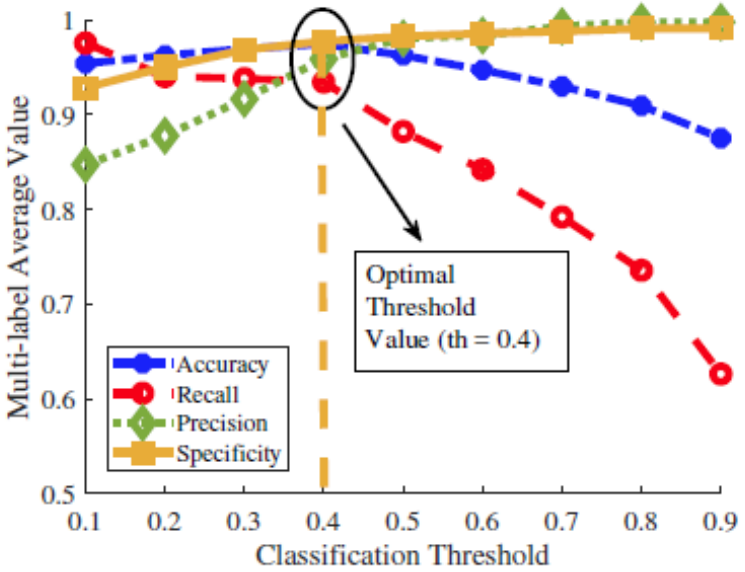
Performance Evaluation

- IoTWatcH classified 146 IoT strings into privacy preferences with an average accuracy of 94.25% and precision of 95%
- It also flagged 62 sensitive leakages (29 via messaging and 33 via Internet communications) to unauthorized parties in 35 IoT apps
- IoTWatcH introduced, on average, 105 ms latency to an app's execution

App Type	Total Apps Analyzed	Messaging Ccommunications Analyzed	No. of Data Leaks	No. of Privacy Concerns	IoTWatcH Effectiveness
Market	120	54	0	–	–
Malicious	40	58	29	–	100%
Total	160	112	29	–	100%

App Type	Total Apps Analyzed	Internet Communications Analyzed	No. of Data Leaks	No. of Privacy Concerns	IoTWatcH Effectiveness
Market	120	12	11	3†	100%
Malicious	40	22	22	3‡	100%
Total	160	34	33	6	100%

† Includes one privacy concern that does not constitute a data leak and two privacy concerns that were also flagged as data leaks.
‡ Includes three privacy concerns that were also flagged as data leaks.



Conclusions

- IoT platforms do not offer real-time privacy analysis that informs the users about how the IoT apps use the sensitive information
- We proposed IoTWatcH, a privacy analysis tool that applies NLP techniques to uncover privacy risks from IoT apps in real time
- IoTWatcH classified IoT strings to privacy labels with 94.25% accuracy and flagged 35 apps that leak data

Thank You!

Stop by our poster presentation to learn more and ask questions!

Name: Leonardo Babun

Email: lbabu002@fiu.edu

Project Link: https://arxiv.org/abs/1911.10461

Personal Website: http://leobabun.wixsite.com/leo-babun-phd

Lab Website: https://csl.fiu.edu/