
# Enforcing Privacy Policies for Hybrid Mobile Applications

Aishwarya Marghatta Nandeesh

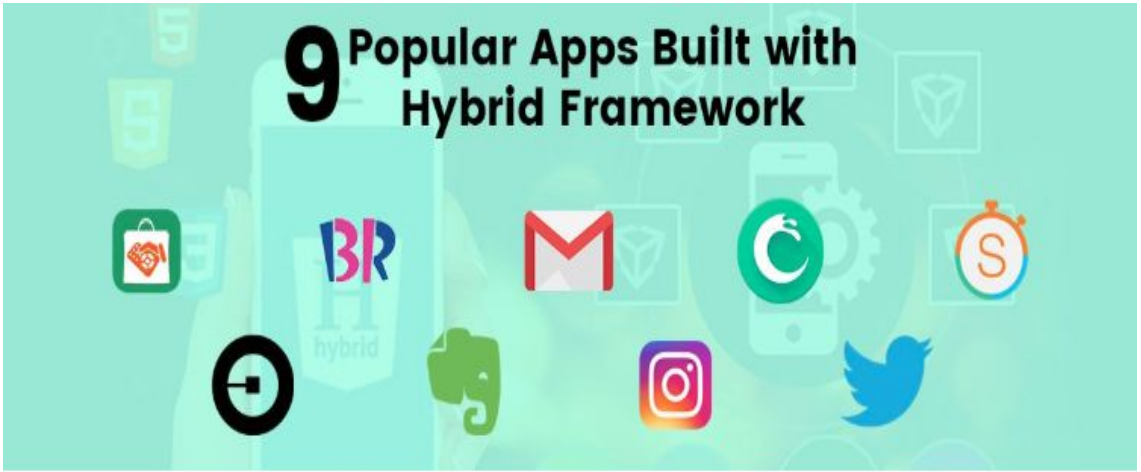
Advisor
Dr. Phu H. Phung

https://isseclab-udayton.github.io/
Intelligent Systems Security Lab
Department of Computer Science

# Hybrid Mobile Applications

Mobile applications that combine the elements of both native applications and web applications.

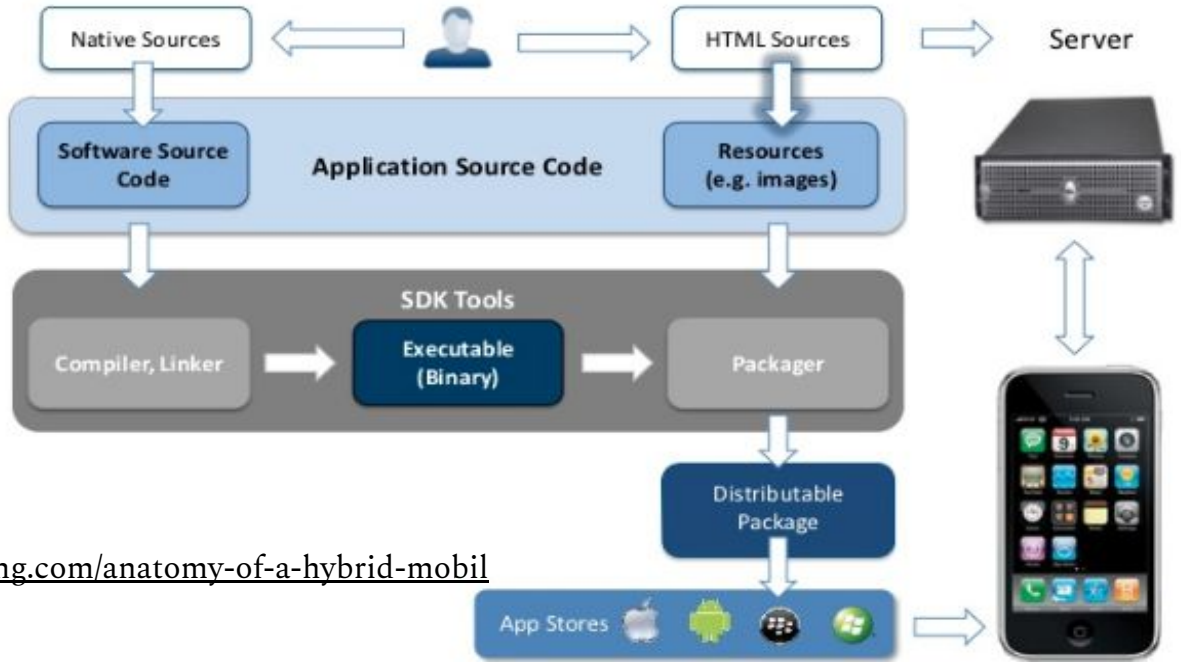
# Few popular Hybrid Mobile Applications




Source: http://blog.venturepact.com/8-high-performance-apps-you-never-knew-were-hybrid/

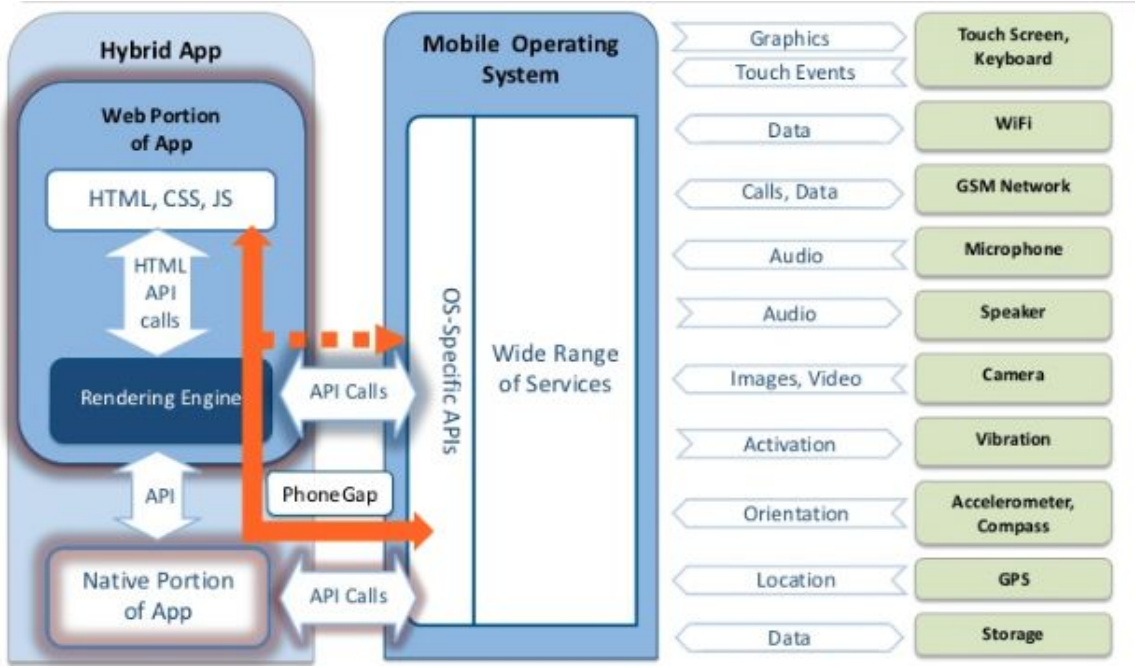
# Advantages of Hybrid Application Development

## Write-once-run-everywhere




Sourcehttp://geospatialtraining.com/anatomy-of-a-hybrid-mobile-gis-application/

# Hybrid Mobile App Architecture




Source : http://geospatialtraining.com/anatomy-of-a-hybrid-mobile-gis-application/

# Vulnerability in Hybrid App

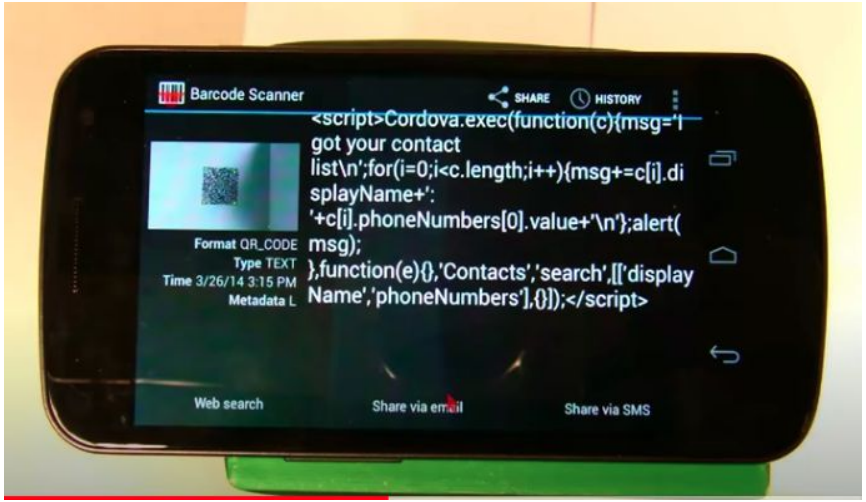
- Hybrid apps are more vulnerable to attack than mobile apps written in native binary code because vulnerabilities on the web is written in **JavaScript** and **HTML**.
- Once the vulnerabilities say malicious code gets executed, attacker can launch the attack and steal the information.

# An Attack Example

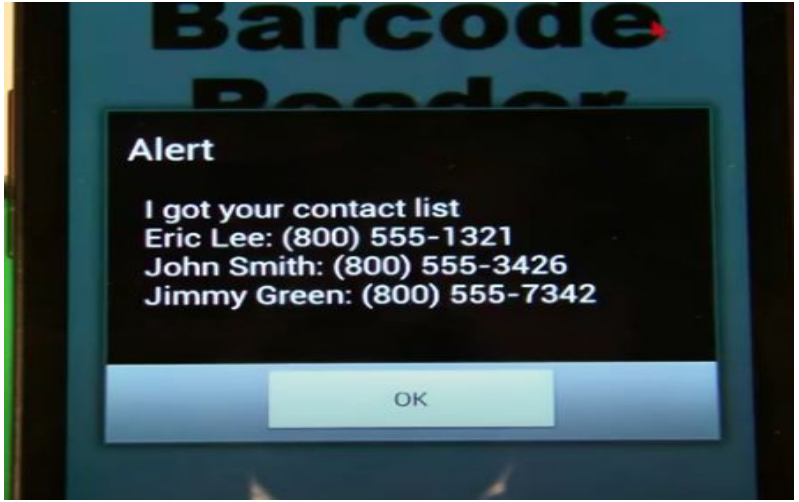
- An example of two applications used to scan a 2D barcode which is inserted with a piece of Malicious code.
- One of the apps is written in native(Java code) and the other app is written in HTML5 based technology.
- Let’s compare the both the apps how it works after scanning the barcode.

# Scanned Barcode result

## Native App:




## Hybrid App:



# Hacking in Hybrid apps

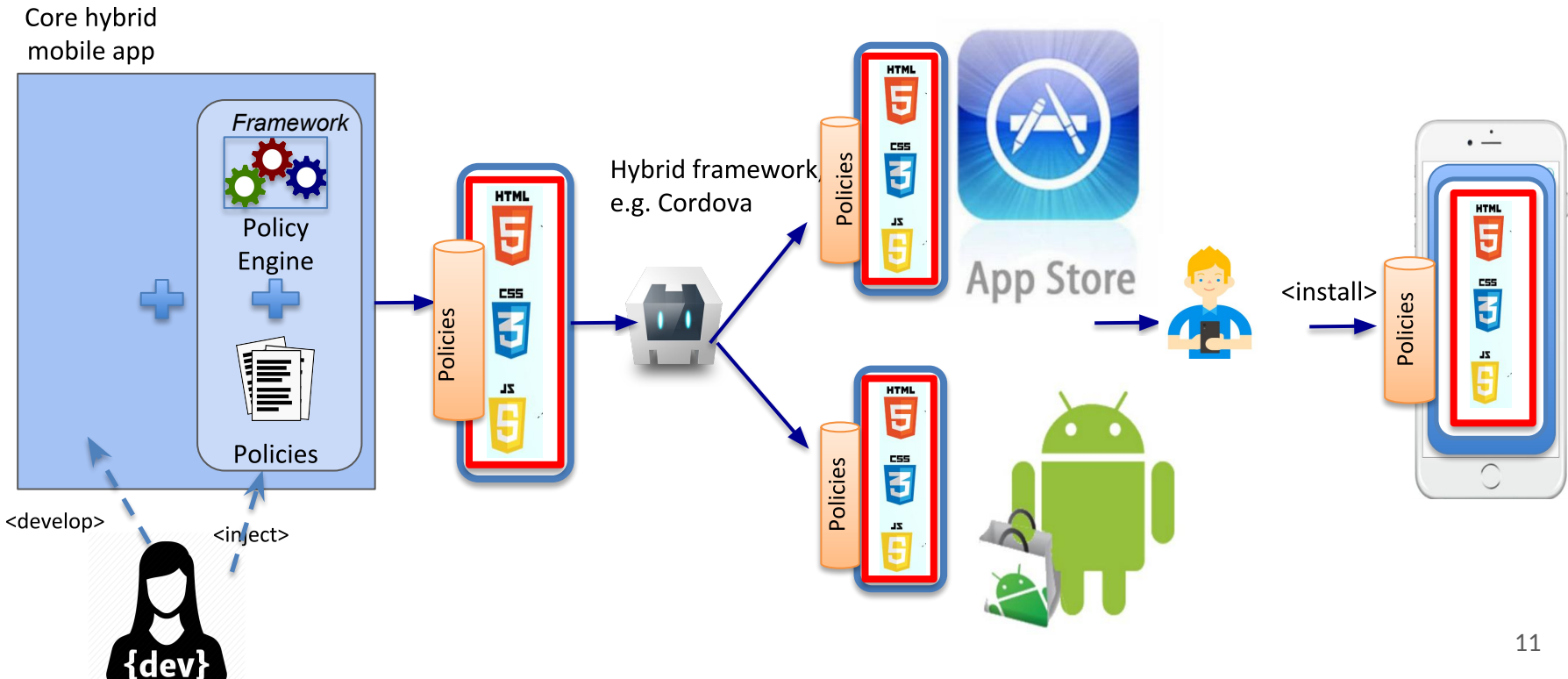
Thus, on Native application the code is not executed it is just displayed, Whereas on HTML5 technology based application the malicious code is executed and launch its attack for stealing the information.

# Talk Outline

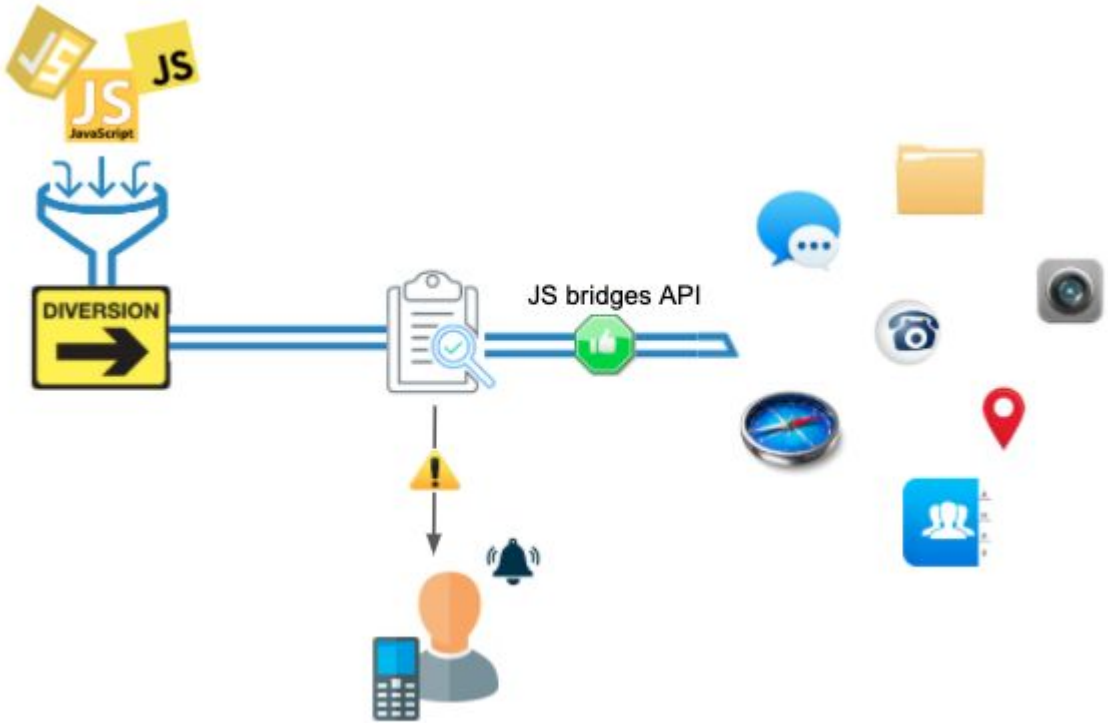
- Hybrid Mobile Apps and Security
- Existing solutions in our Intelligent Systems Security Lab and their limitations
- Motivations for this work
- Proposed Solutions
- Conclusions

# The HybridGuard Framework

[Phung et al., MOST'2017, Phung et al., JCS'2020]

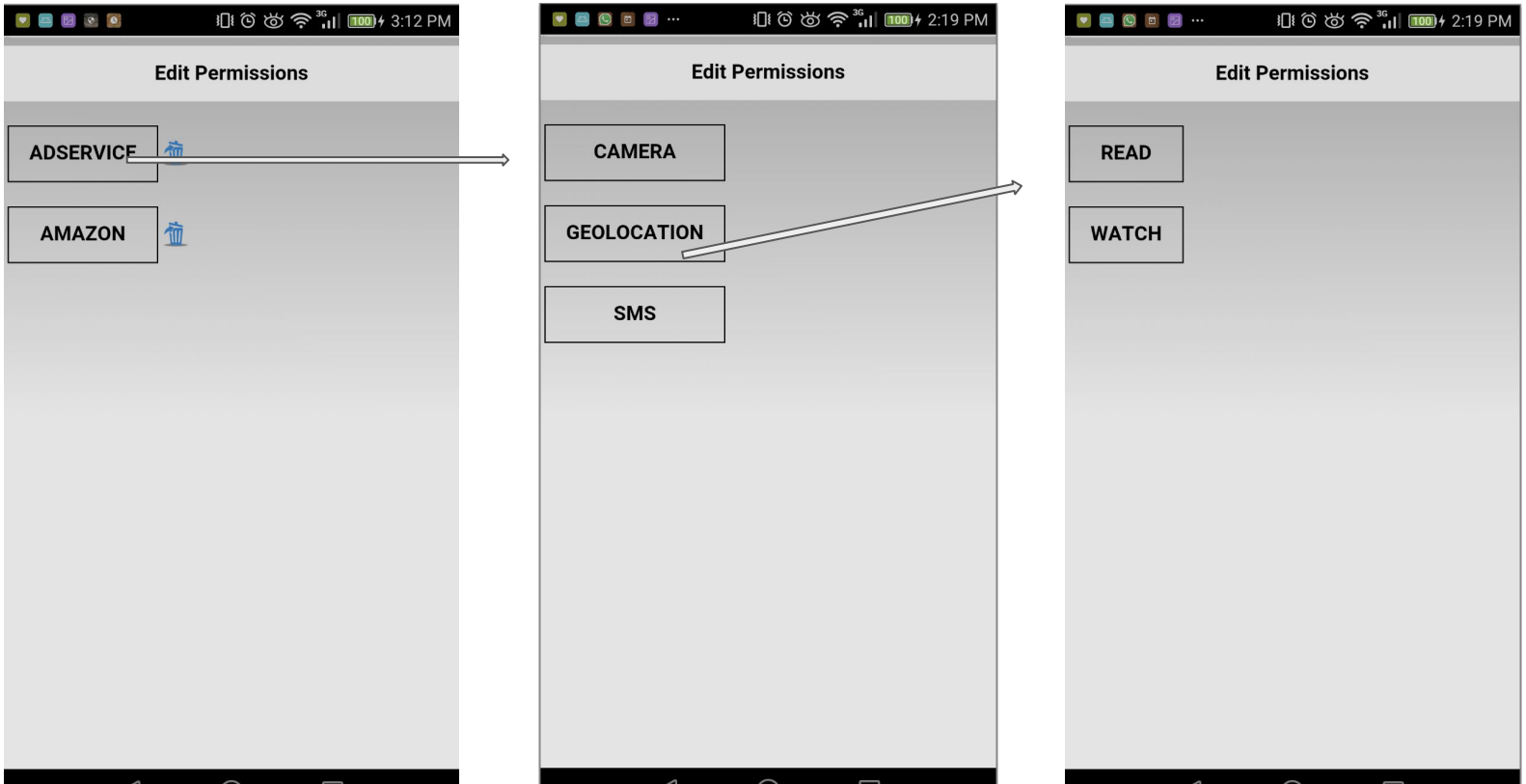


# Hybrid Guard Policy Enforcement



# Extended HybridGuard Fine-grained Policies

## [Rakesh Reddy, Master thesis 2019]

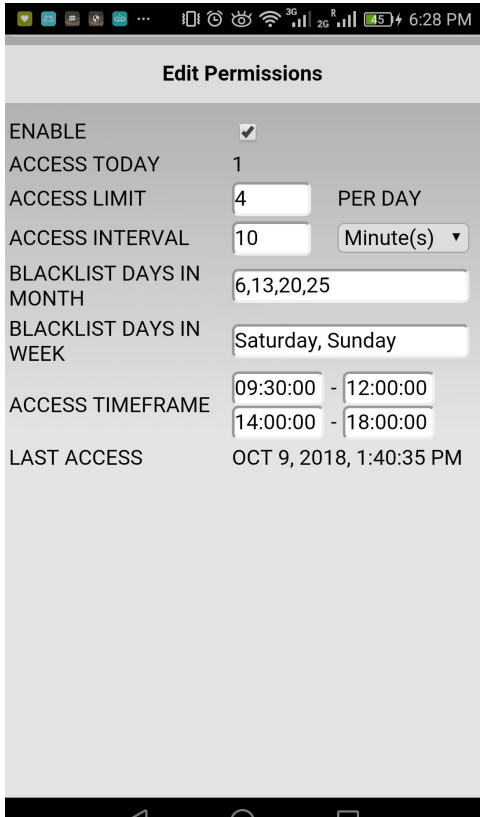


# Policy Categorised on Current Solution

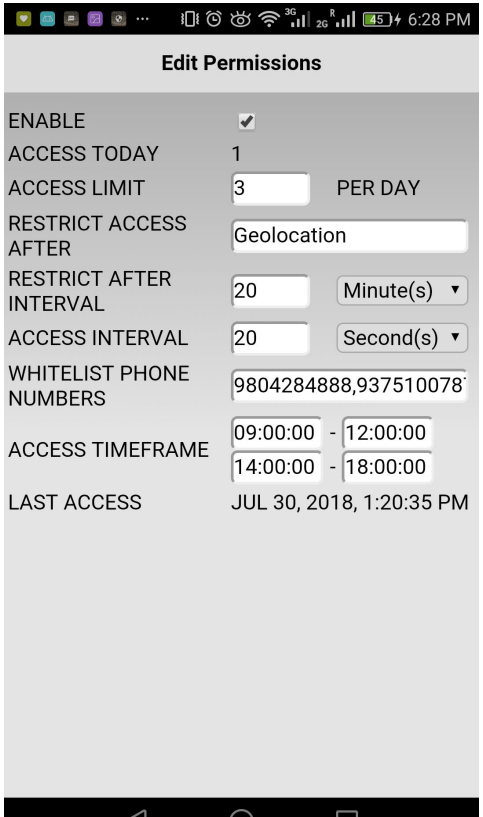
- Volume-based policy
- Interval-based policy
- Timeframe-based policy
- Blacklist-based policy
- Whitelist-based policy
- Sequence-based policy

# Fine-grained Policy Examples

location.read




Sms.send



# Limitations of current solution and Motivation of this work

- Can enforce security policies in general but not privacy specific
  - Privacy enforcement is more important in the mobile revenue and ecosystem.
- No user experience study
  - Whether users want to enforce stricter policies
  - User concerns about their privacy

These limitations are the motivations for our current work

# Research questions

- Are these policies useful for the users?
- How do we build the privacy awareness to the mobile users?
- Are these policies helpful for users on real-time?
- Are we reaching the users expectations for authorizing advanced features and alerting from malicious activity?

# Proposal

- To customize the policy for the end-users such that the privacy requirements should take control over the device resource utilization.
- To reach the users expectations of privacy features by implementing and injecting more security policies into the mobile applications.

# Summary

- The research work aims at reaching users expectations for data privacy and calibrates the security for hybrid mobile apps.
- The research work adds more customized policies for reaching the users expectations on privacy requirement against malicious activities.

# References


- Phung, Phu H. , Reddy, Rakesh S.V., Cap, Steven, Pierce, Anthony, Mohanty, Abhinav and Sridhar, Meera. ‘A Multi-party, Fine-grained Permission and Policy Enforcement Framework for Hybrid Mobile Applications’. Journal of Computer Security, vol. 28, no. 3, pp. 375-404, 2020
- Phung, Phu H. , Abhinav Mohanty, Rahul Rachapalli, and Meera Sridhar, “HybridGuard: A Principal-based Permission and Fine-Grained Policy Enforcement Framework for Web-based Mobile Applications”, Mobile Security Technologies (MoST) 2017
- Claudio Rizzo, Lorenzo Cavallaro, and Johannes Kinder. “Babelview: Evaluating the impact of code injection attacks in mobile Webviews”. In I*nternational Symposium on Research in Attacks, Intrusions, and Defenses*, pages 25–46. Springer, 2018.
- Colli, MG 2009, *Bilbao_6 Guggenheim Museum Bilbao,* photograph, viewed January 2012, <http://www.flickr.com/photos/52355315@N08/5757476385/>.
- *Nefertari with Isis,* n.d. photograph, viewed 4 January 2012, <http://en.wikipedia.org/wiki/File:Ankh_isis_nefertari.jpg>.
- Colli, MG 2009, Bilbao_6 Guggenheim Museum Bilbao, photograph, accessed January 2012, <https://www.flickr.com/photos/52355315@N08/5757476385/>. CC BY 2.0
- https://developer.android.com/guide/topics/permissions/overview

# Thank you!

Aishwarya Marghatta Nandeesh

https://isseclab-udayton.github.io/
Intelligent Systems Security Lab
Department of Computer Science