

Android Security Improvement by Visualization of Application Behavior

Rika Hayashi
Institute of Information Security

I love Android

I love Android.



I love Android. But ...

I love Android.



If I give him everything ...

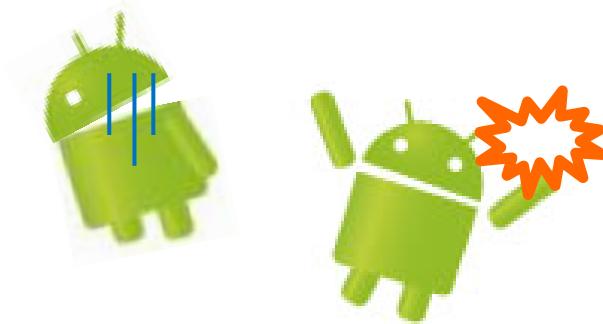


I love Android. But ...

If I give him everything ...

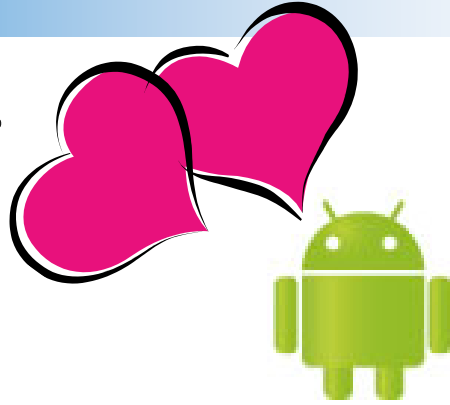


He would become ill.



I love Android. So ...

I love Android.



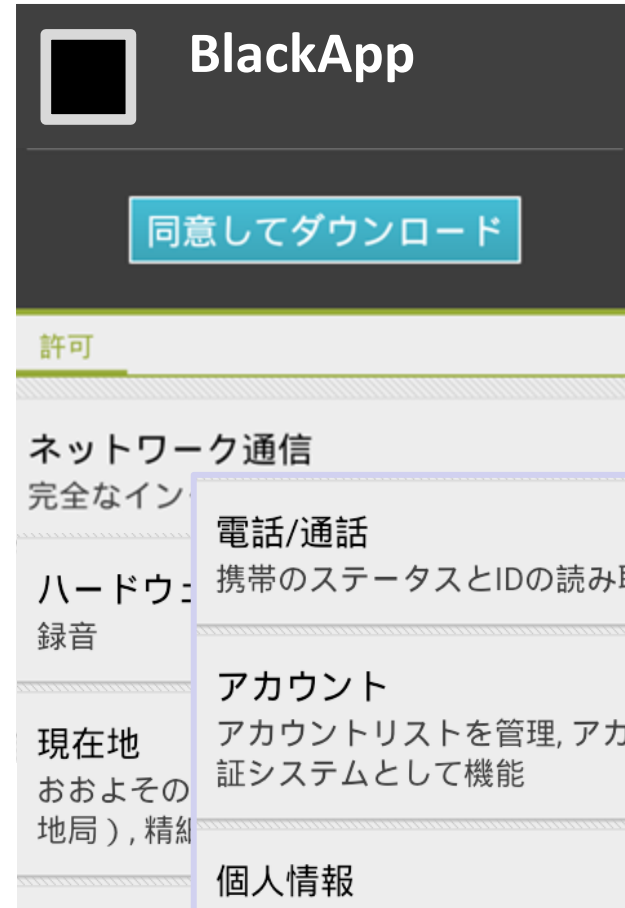
So I have to select what I give him.



Select what I give him

example : Application to show the map where I am

Applications requires 'permissions' before installation.



Select what I give him

example : Application to show the map where I am
Applications requires 'permissions'
before installation.



INTERNET

RECORD
AUDIO

ACCESS
LOCATION

READ
PHONE_STATE

AUTHENTICATE
_ACCOUNTS

ACCESS
PERSONAL_INFO

Select what I give him

example : Application to show the map where I am
Applications requires 'permissions'
before installation.



INTERNET

RECORD
AUDIO

ACCESS
LOCATION

READ
PHONE_STATE

AUTHENTICATE
_ACCOUNTS

ACCESS
PERSONAL_INFO

Select what I give him

example : Application to show the map where I am

Applications requires 'permissions'
before installation.



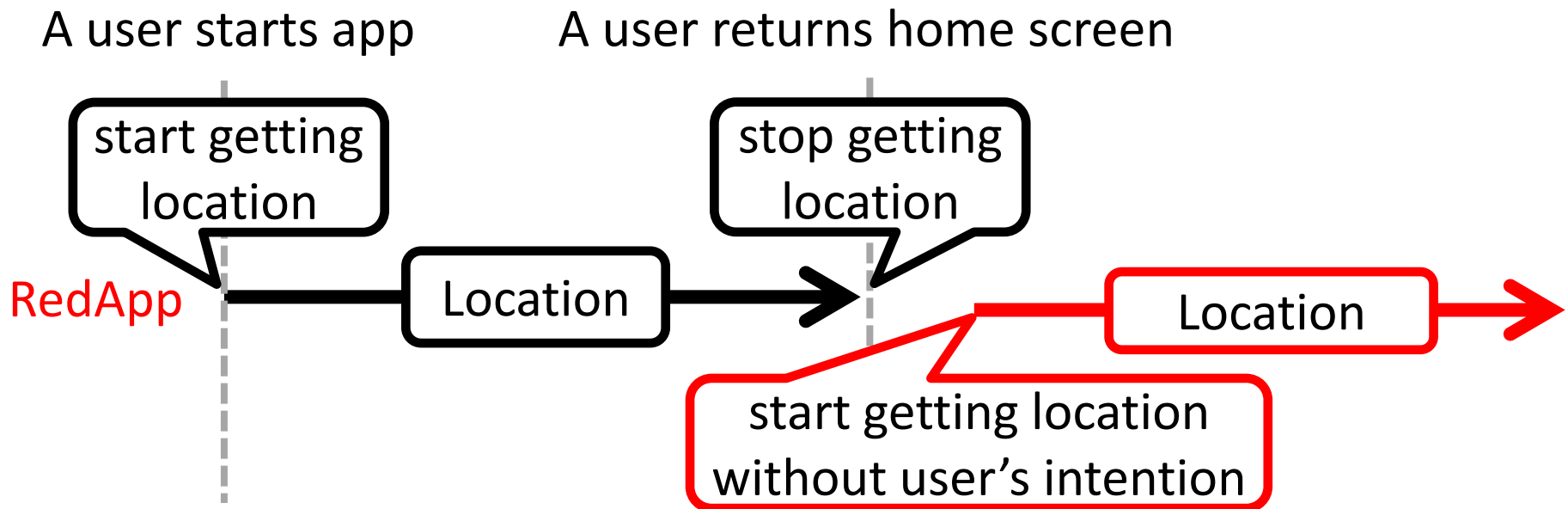
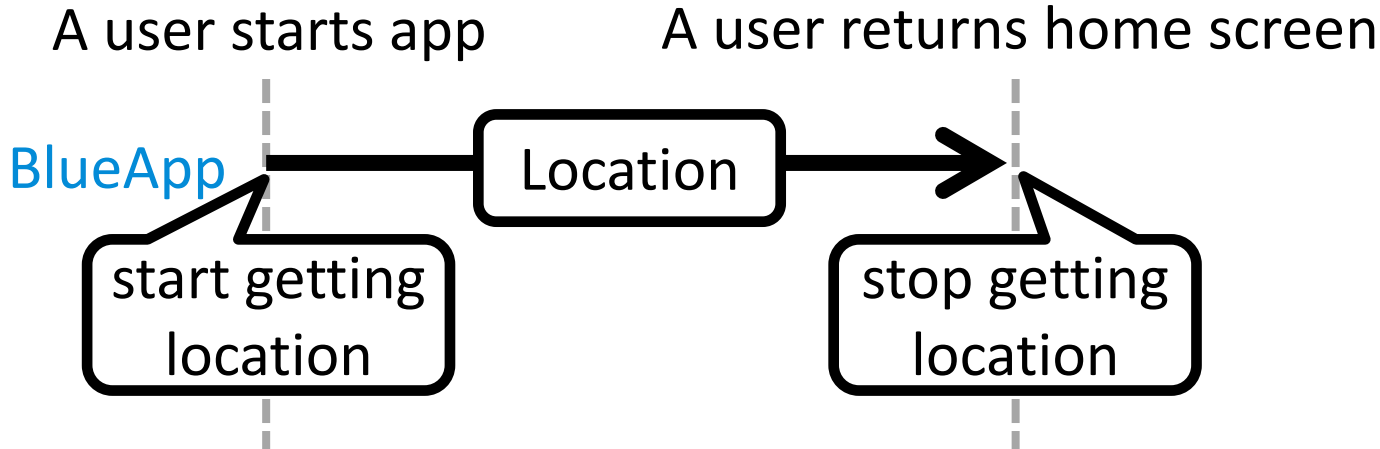
INTERNET

ACCESS
LOCATION

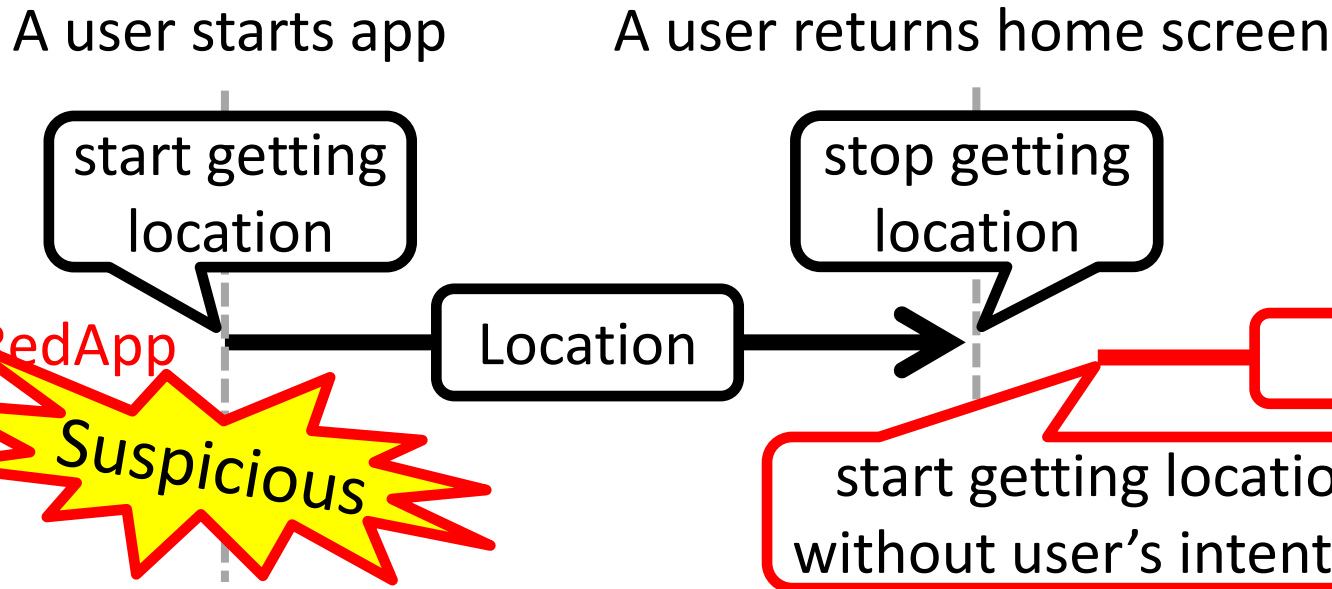
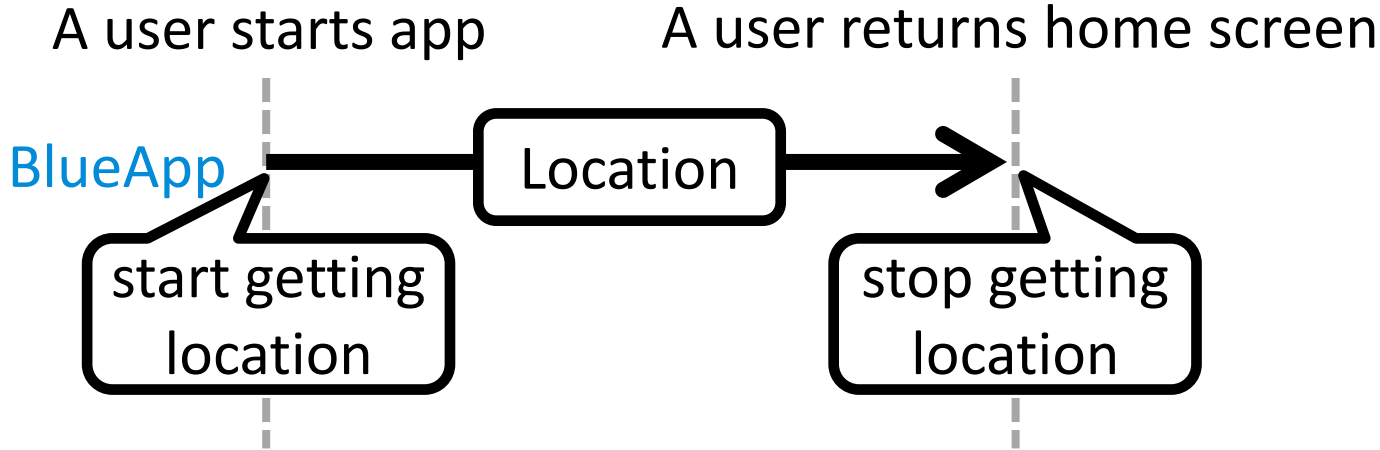


Permissions are reasonable...

Select what I give him

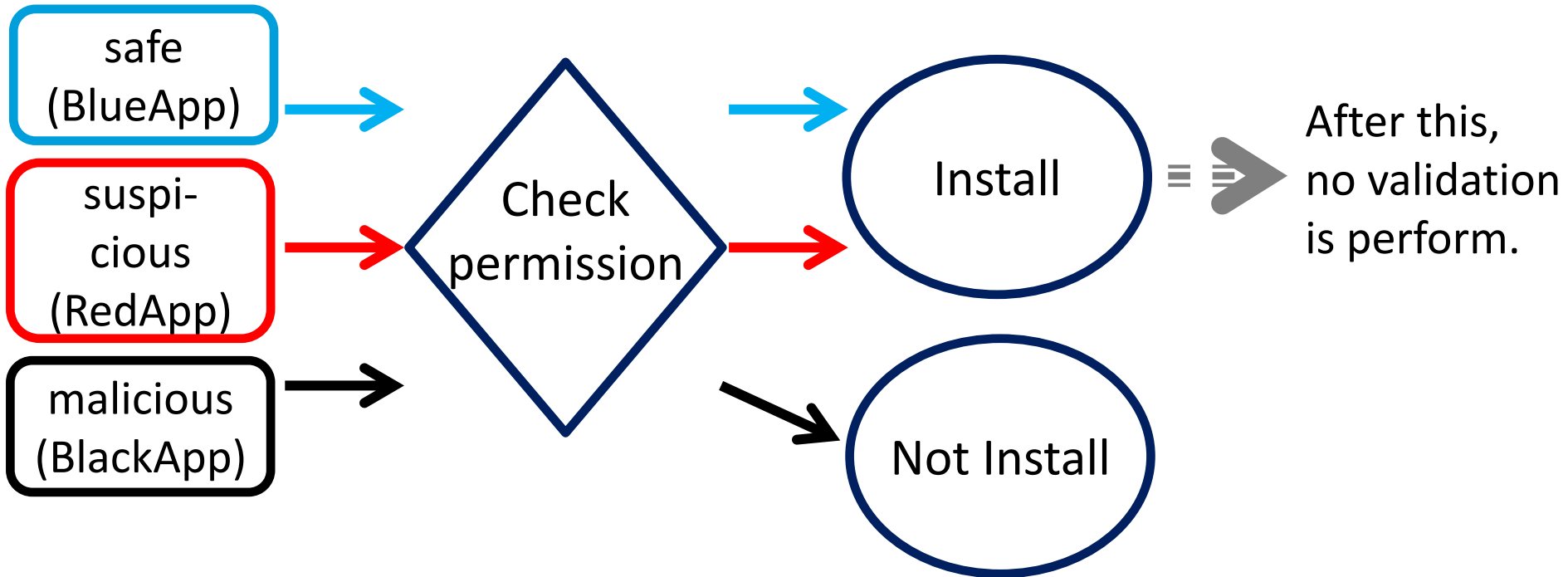


Select what I give him



Select applications

[now]



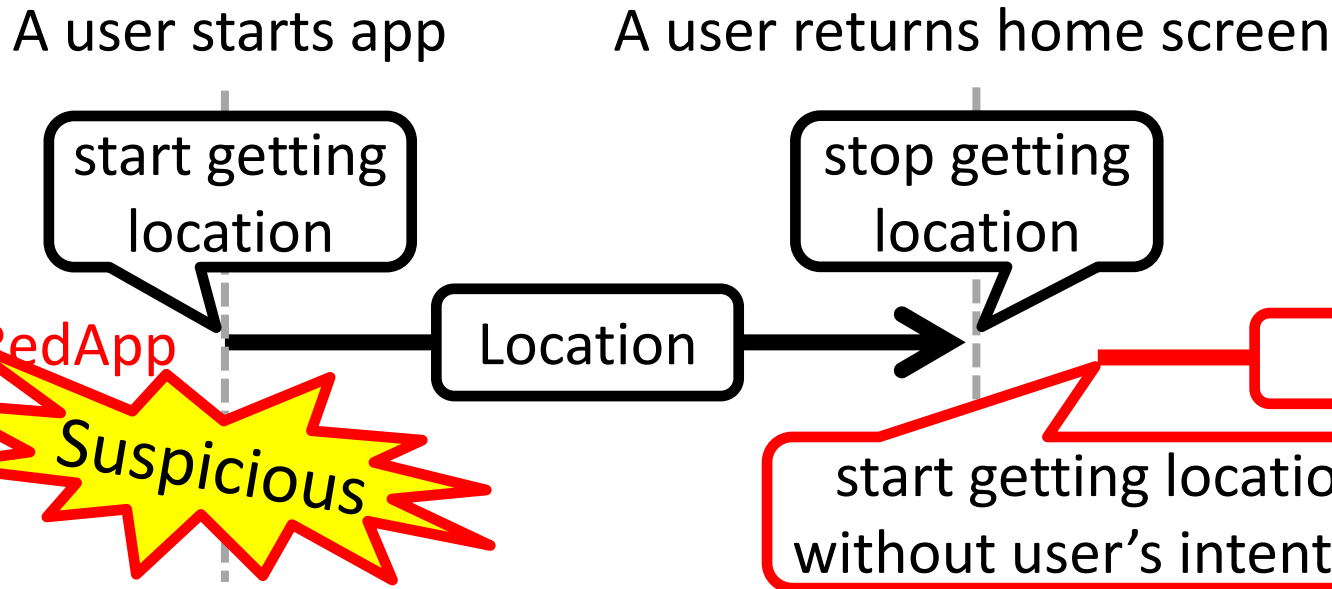
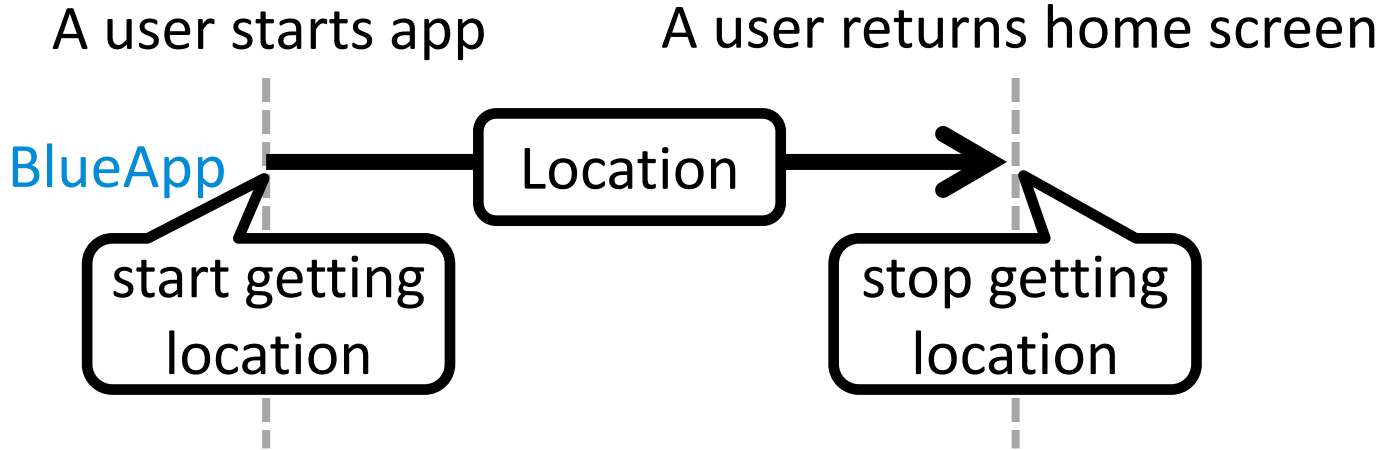
Select what I give him

example : Application to show the map where we are

Applications requires 'permissions' before installation.



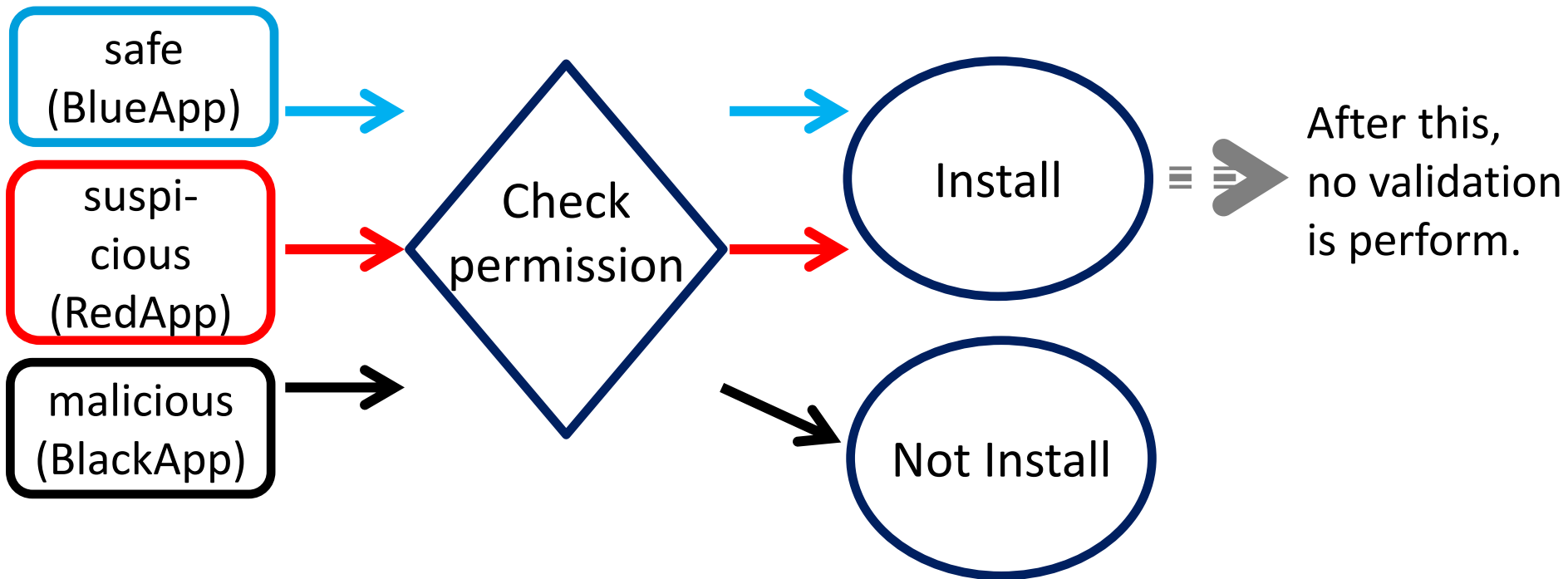
Select what I give him



To keep safety by users' own selves

— Select application

[now]



[now]

To judge whether applications are malicious, safe or **suspicious**, users can only verify the '**permissions**' required by them before installation.

So users can't notice suspicious applications.



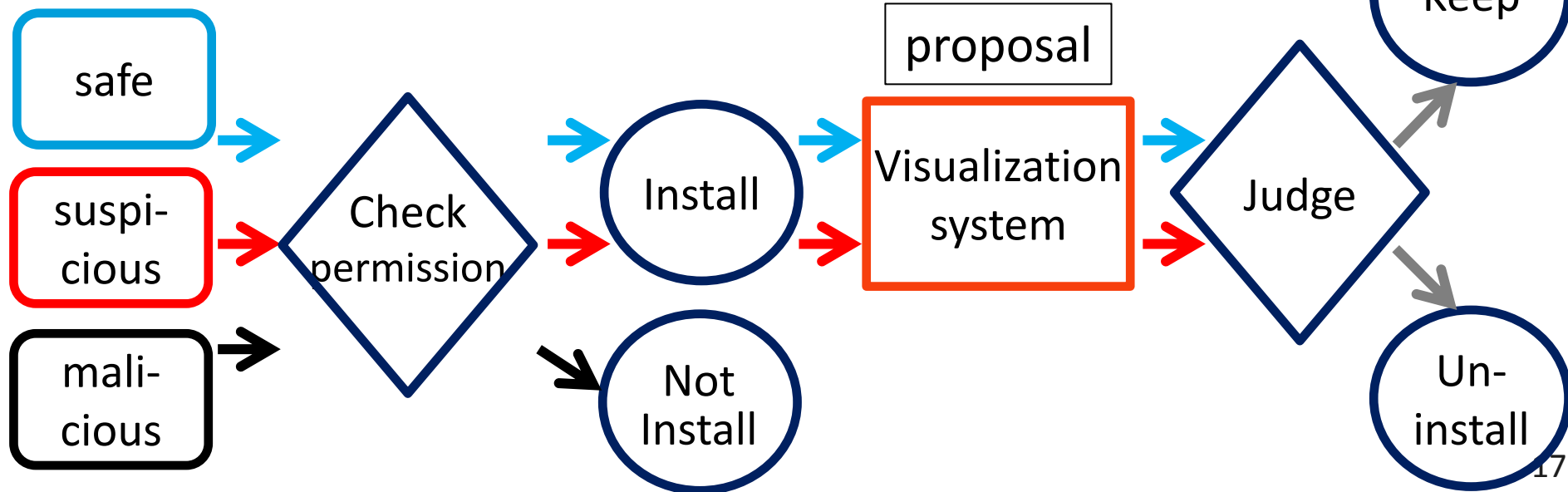
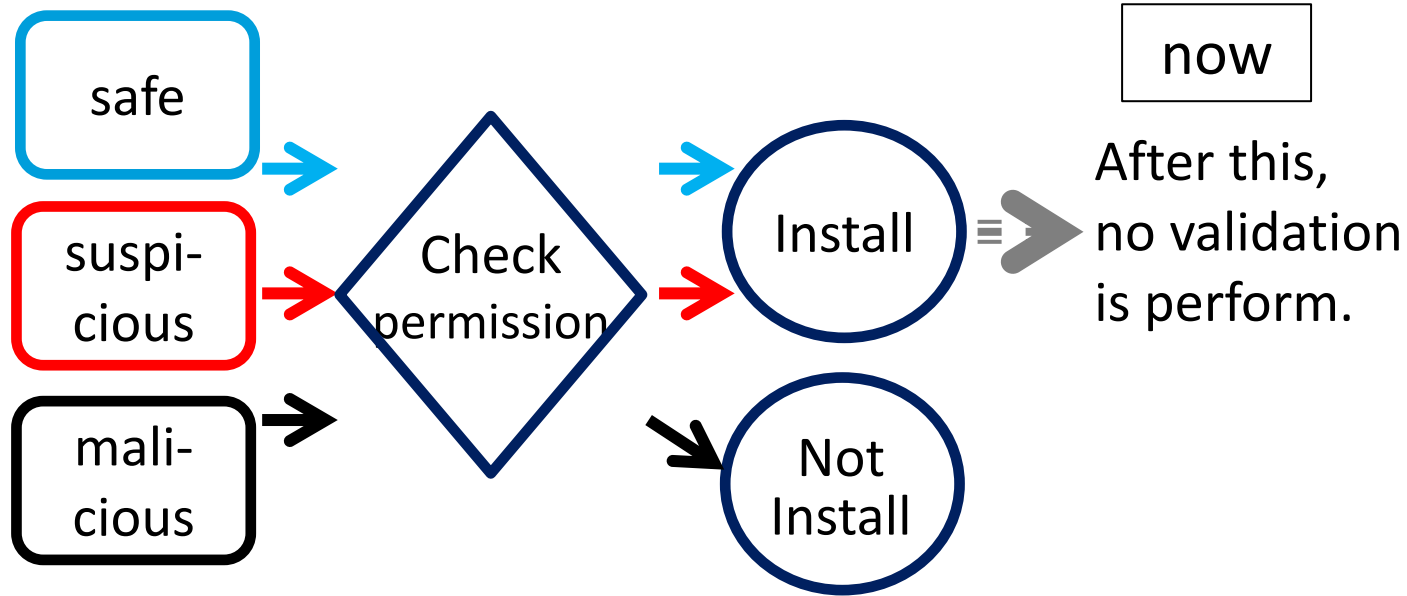
[propose]

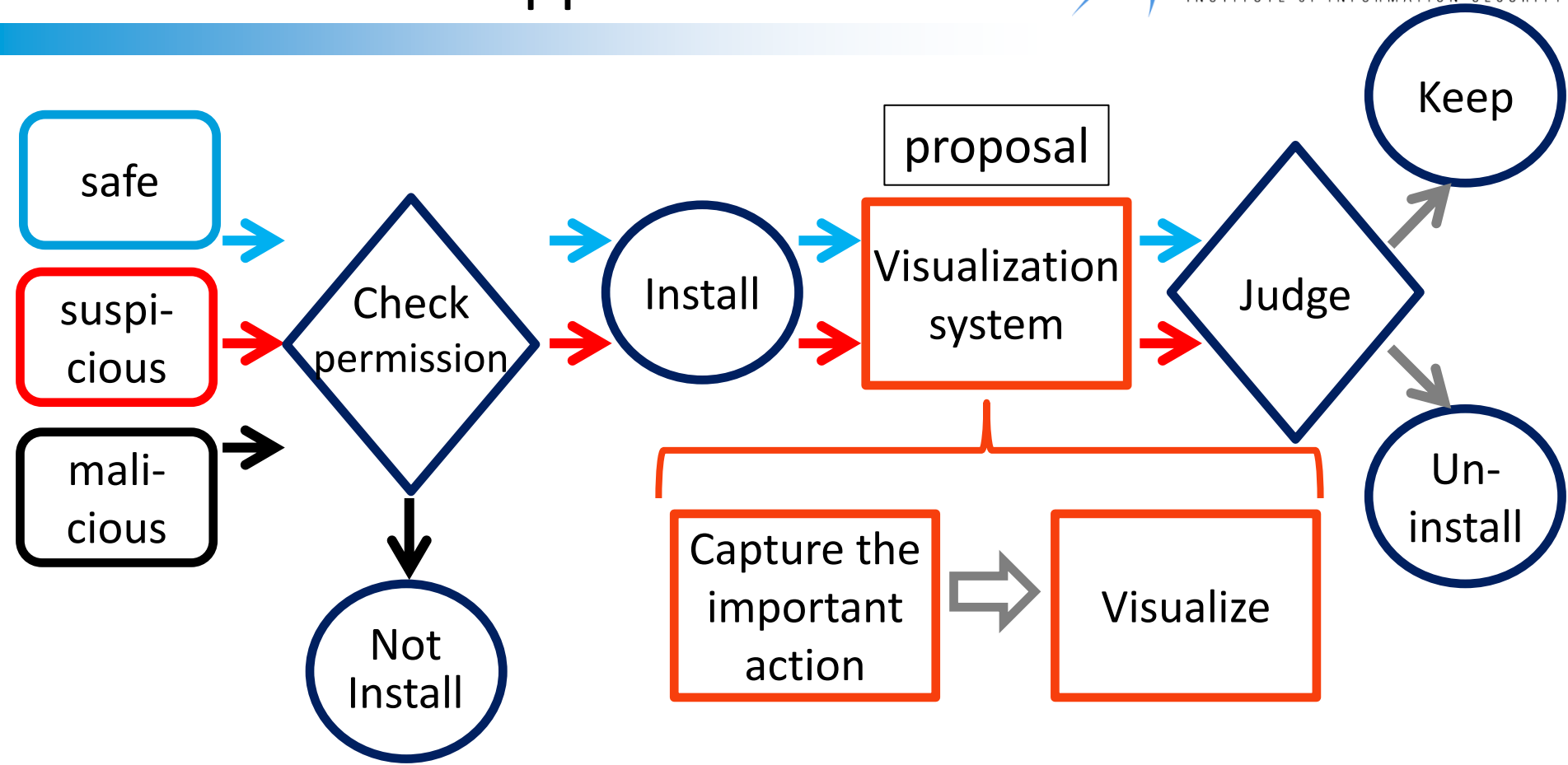
I provide users with information to judge whether applications are safe or **suspicious**, even **after installing** them.

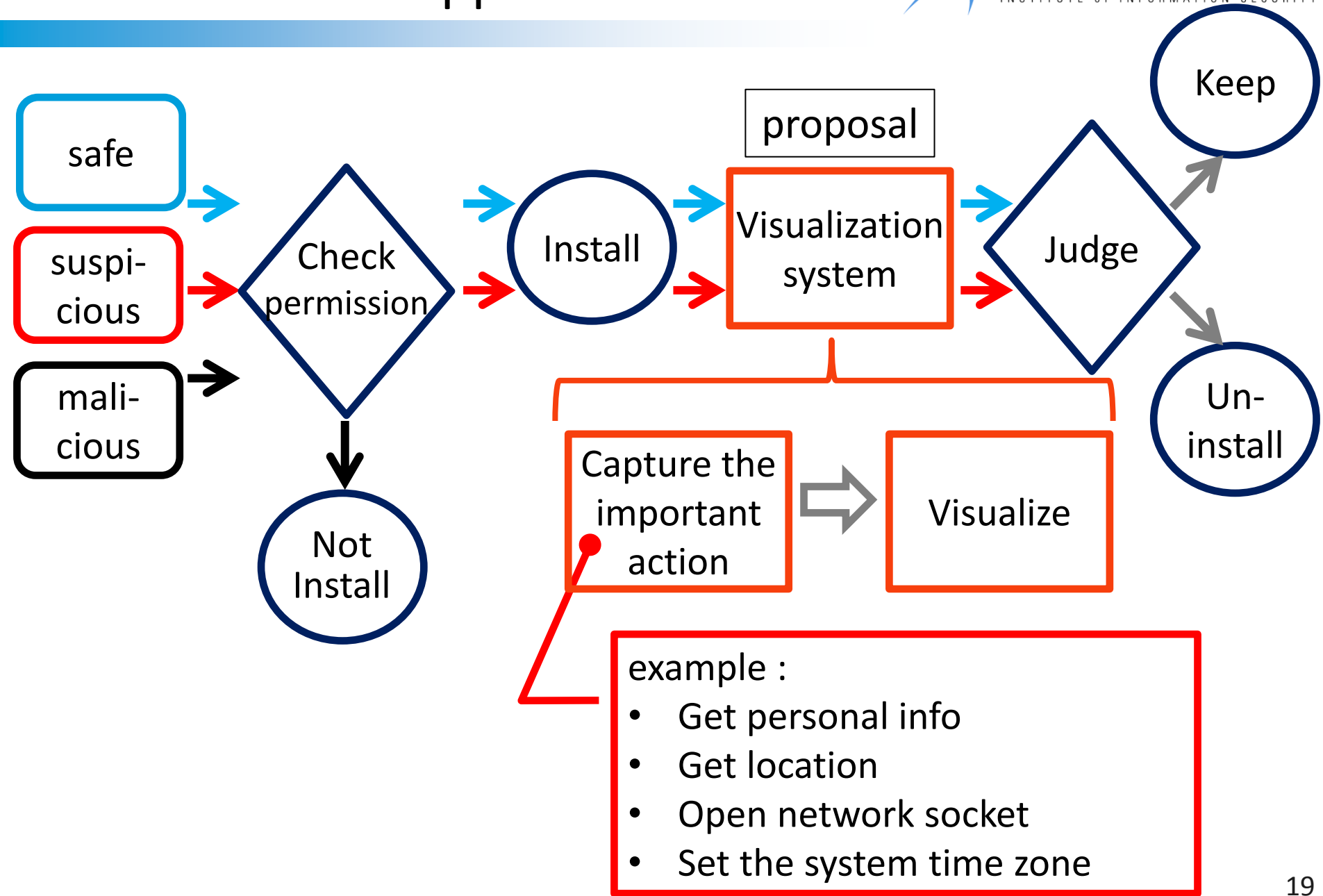
I propose the **visualization system** to show application behavior.

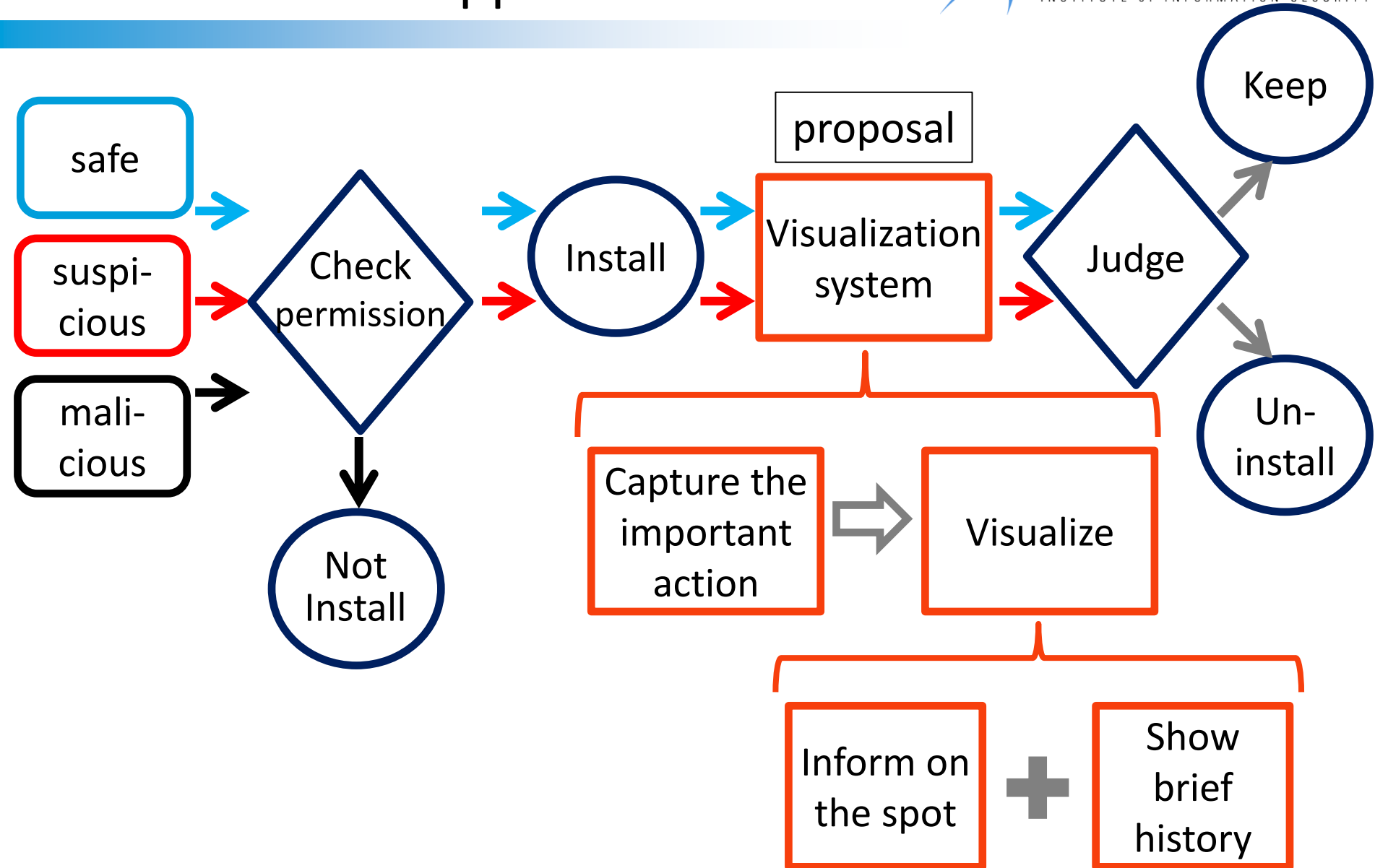


Proposal



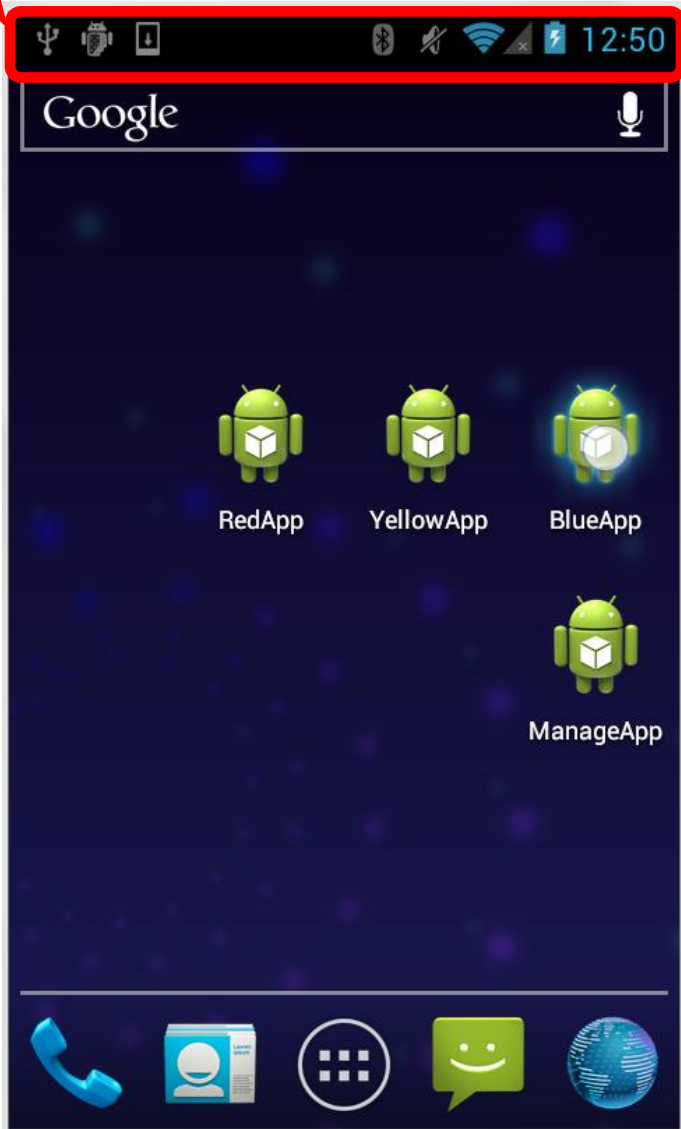






Inform on the spot

Status bar



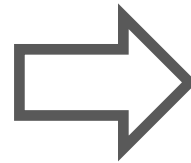
Inform users that application takes an important action

位置情報取得開始

BlueApp

現在地は

An application takes an important action.



Inform on the spot

Permit application to take an important action ⇒ Tap the notification area

Reject application to take an important action ⇒ Ignore it

< If permitting >



If permitting,
tap here.

Notification
area



Show brief history

Show users the brief history of important actions taken by applications.

ManageApp

アプリ名: B 表示

The brief history that BlueApp got location.

日時	動作	判定
2012-09-21 09:50:59	位置取得開始	
2012-09-21 09:51:10	位置取得終了	
2012-09-21 11:11:26	位置取得開始	
2012-09-21 11:11:43	位置取得終了	
2012-09-21 12:14:47	位置取得開始	
2012-09-21 12:15:05	位置取得終了	

ManageApp

アプリ名: R 表示

The brief history that RedApp got location.

日時	動作	判定
2012-09-21 09:51:44	位置取得開始	
2012-09-21 09:52:00	位置取得終了	
2012-09-21 09:52:05	位置取得開始	
2012-09-21 11:13:08	位置取得開始	×
2012-09-21 11:13:25	位置取得終了	
2012-09-21 11:13:30	位置取得開始	×
2012-09-21 12:15:41	位置取得開始	×
2012-09-21 12:16:25	位置取得開始	
2012-09-21 12:17:13	位置取得終了	
2012-09-21 12:17:18	位置取得開始	×
2012-09-21 12:19:58	位置取得開始	
2012-09-21 12:20:05	位置取得終了	
2012-09-21 12:20:10	位置取得開始	×

start getting location

stop getting location

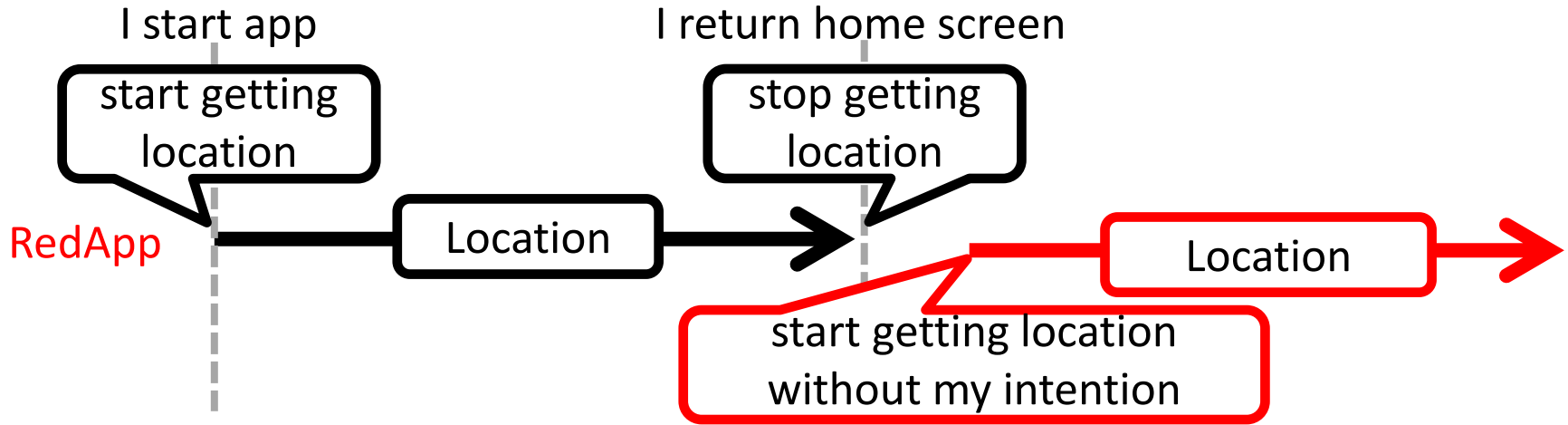
User rejects starting getting location

♣ Implement Visualization system as application experimentally.

I want to modify the API in the Application Framework of Android platform, but I haven't yet ...

Demonstration

RedApp is the application to show the location where I am



Permit the action ⇒ Tap the notification area

Reject the action ⇒ Ignore it



If permitting,
tap here.



Add two features to visualize the application behavior.

<feature1> Inform on the spot

♣ Inform users that application takes an important action on the spot.

Users can judge whether the timing of the action is exactly what users intend.

+α ... Users can permit or reject the action as intended.

<feature2> Show brief history

♣ Show users the brief history of important actions taken by applications.

Users can judge whether there are any application

- whose timing of the action is not exactly what users intend
- which took improper duration or repetition of the action.

<feature1> Inform on the spot

♣ Inform users that application takes an important action on the spot.

Users can judge whether the timing of the action is exactly what users intend.

+α ... Users can permit or reject the action as intended.

<feature2> Show brief history

♣ Show users the brief history of important actions taken by applications.

Users can judge whether there are any application

- whose timing of the action is not exactly what users intend
- which took improper duration or repetition of the action.



Users can judge whether applications are safe or **suspicious**, even **after installing** them.

Fin.
Thank you.