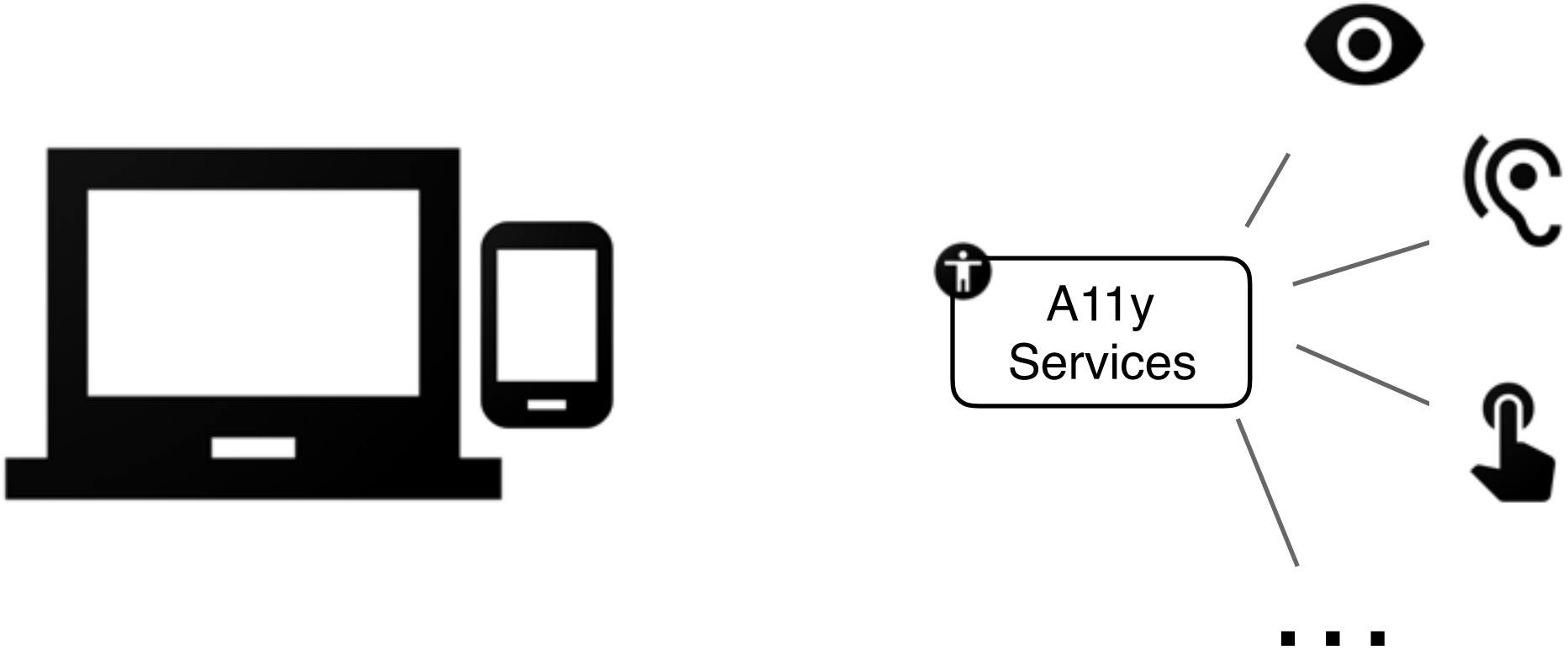
A11y and Privacy don’t have to be mutually exclusive: Constraining Accessibility Service Misuse on Android

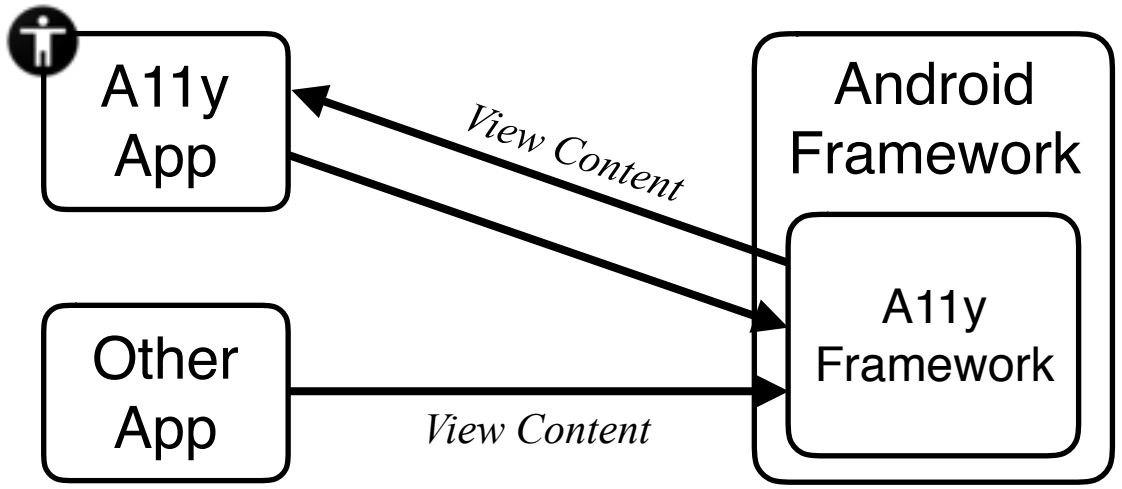
Jie Huang, Michael Backes, and Sven Bugiel
CISPA Helmholtz Center for Information Security

Motivation

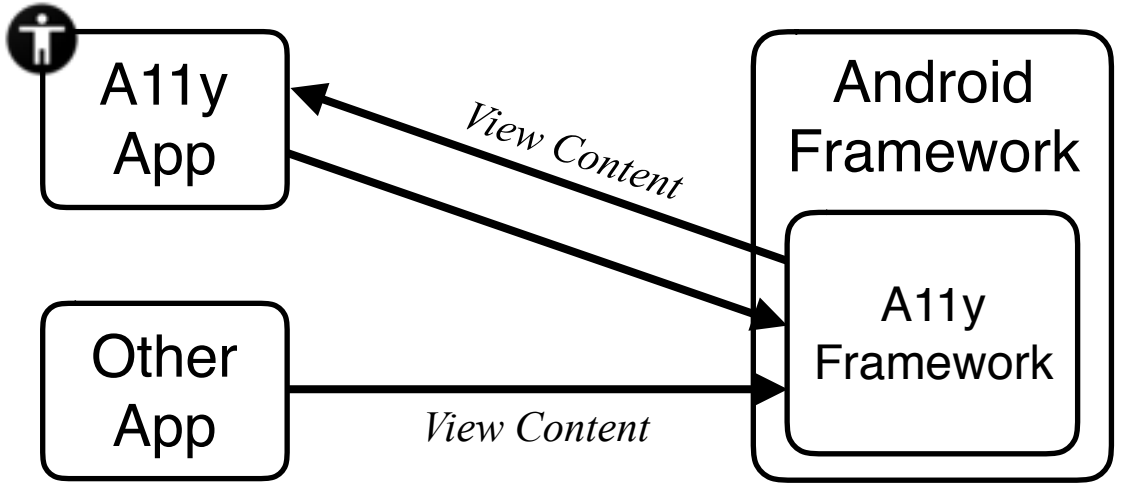


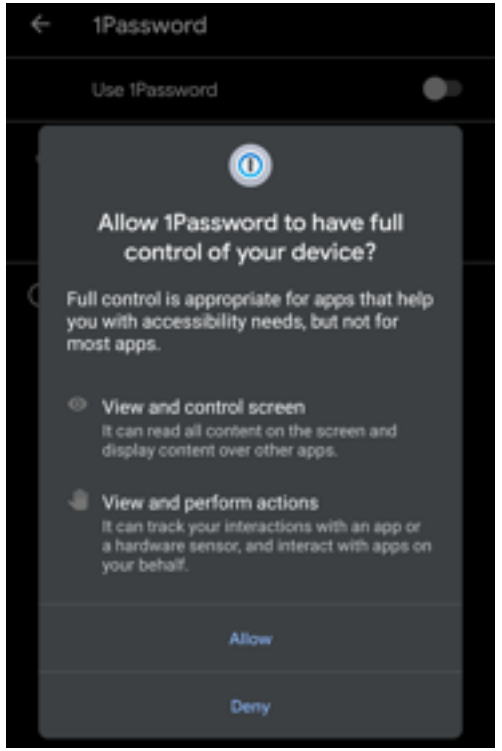
a11y is the abbreviation of a**ccessibility**

Motivation


A11y App
Other App
View Content
View Content
Android Framework
A11y Framework

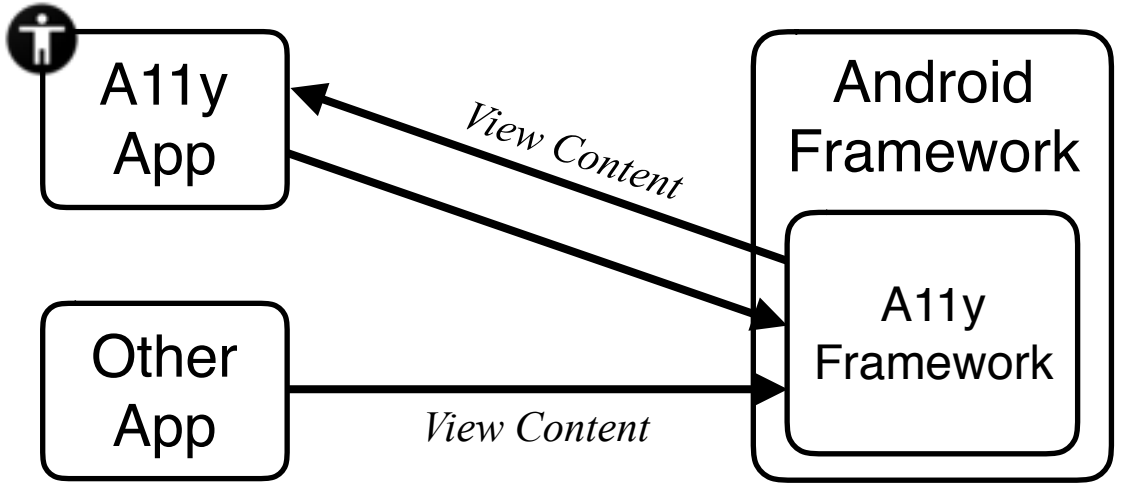
Motivation





permission.BIND_ACCESSIBILITY_SERVICE

Motivation



LastPass

Cleaner

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

How to not make a11y and privacy mutual exclusive?

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

How to not make a11y and privacy mutual exclusive?

How to distinguish good from bad behaviour?

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)

	#Apps	#AccessibilityService	Source
Malicious	55	57	GitHub
Utility	35	36	Google Play
A11y	5	8	Google Play
Sum	95	101	

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)

Distinguish based on configuration?

No!

Similarities

- all monitoring broadly
- similar configuration

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO

Distinguish based on API usage?

No!

Similarity

- same API usage pattern

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO
- Distinguish based on API usage? NO

Distinguish based on complete accessibility pipelines?

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click specific buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click specific button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen navigation
	Gesture Access	Finger gesture	Screen navigation
	Voice Access	Microphone detection	Screen navigation&text editing
	Switch Access	Hardware keyboard	Screen navigation&text editing

Similarities

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click specific buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click specific button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen navigation
	Gesture Access	Finger gesture	Screen navigation
	Voice Access	Microphone detection	Screen navigation&text editing
	Switch Access	Hardware keyboard	Screen navigation&text editing

Similarities

- self-determined triggers

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click specific buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click specific button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen navigation
	Gesture Access	Finger gesture	Screen navigation
	Voice Access	Microphone detection	Screen navigation&text editing
	Switch Access	Hardware keyboard	Screen navigation&text editing

Similarities

- self-determined triggers
- overlapped intended operations

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click specific buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click specific button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen navigation
	Gesture Access	Finger gesture	Screen navigation
	Voice Access	Microphone detection	Screen navigation&text editing
	Switch Access	Hardware keyboard	Screen navigation&text editing

Similarities

- self-determined triggers
- overlapped intended operations
- require raw data processing

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click specific buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click specific button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen navigation
	Gesture Access	Finger gesture	Screen navigation
	Voice Access	Microphone detection	Screen navigation&text editing
	Switch Access	Hardware keyboard	Screen navigation&text editing

Similarities

- self-determined triggers
- overlapped intended operations
- require raw data processing

Differences

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click **specific** buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click **specific** buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click **specific** button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen **navigation**
	Gesture Access	Finger gesture	Screen **navigation**
	Voice Access	Microphone detection	Screen **navigation**&text editing
	Switch Access	Hardware keyboard	Screen **navigation**&text editing

Similarities

- self-determined triggers
- overlapped intended operations require raw data processing

Differences

- more powerful function (a11y)

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click **specific** buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click **specific** buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click **specific** button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen **navigation**
	Gesture Access	Finger gesture	Screen **navigation**
	Voice Access	Microphone detection	Screen **navigation**&text editing
	Switch Access	Hardware keyboard	Screen **navigation**&text editing

Similarities

- self-determined triggers
- overlapped intended operations
- require raw data processing

Differences

- more powerful function (a11y)
- different final data destination

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click **specific** buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click **specific** buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click **specific** button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen **navigation**
	Gesture Access	Finger gesture	Screen **navigation**
	Voice Access	Microphone detection	Screen **navigation**&text editing
	Switch Access	Hardware keyboard	Screen **navigation**&text editing

Similarities

- self-determined triggers
- overlapped intended operations
- require raw data processing

Differences

- more powerful function (a11y)
- different final data destination
- perform silent operations (malicious)

Study of Accessibility Service Usage

	Scenario	Trigger	Intention
Malicious	Content Eavesdropping	Auto enabled	Send to remote
	Phishing	Target app operation	Load a phishing page
	Process Persistence	Target app operation	Back home
	Silent Installation	Ad click	Click specific buttons in specific app
	Silent Privilege Elevation	Auto enabled	Click **specific** buttons in specific app
	E-Banking Fraud	Auto enabled	Text input&click **specific** button in specific app
A11y	Screen Reader	Finger select	Read text aloud
	Speech to Text	Auto enabled	Enable shortcut button
	Facial Access	Camera detection	Screen **navigation**
	Gesture Access	Finger gesture	Screen **navigation**
	Voice Access	Microphone detection	Screen **navigation**&text editing
	Switch Access	Hardware keyboard	Screen **navigation**&text editing

Similarities

- self-determined triggers
- overlapped intended operations
- require raw data processing

Differences

- more powerful function (a11y)
- different final data destination
- perform silent operations (malicious)
- against user intention (malicious)

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO
- Distinguish based on API usage? NO

Distinguish based on complete pipeline?

YES!

Findings

- different data destination
- explicit **vs.** silent
- user intended **vs.** against user intention

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO
- Distinguish based on API usage? NO
- Distinguish based on complete pipeline? YES

associate UI operations with user intentions

Findings

- different data destination
- explicit **vs.** silent
- user intended **vs.** against user intention

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO
- Distinguish based on API usage? NO
- Distinguish based on complete pipeline? YES

Findings

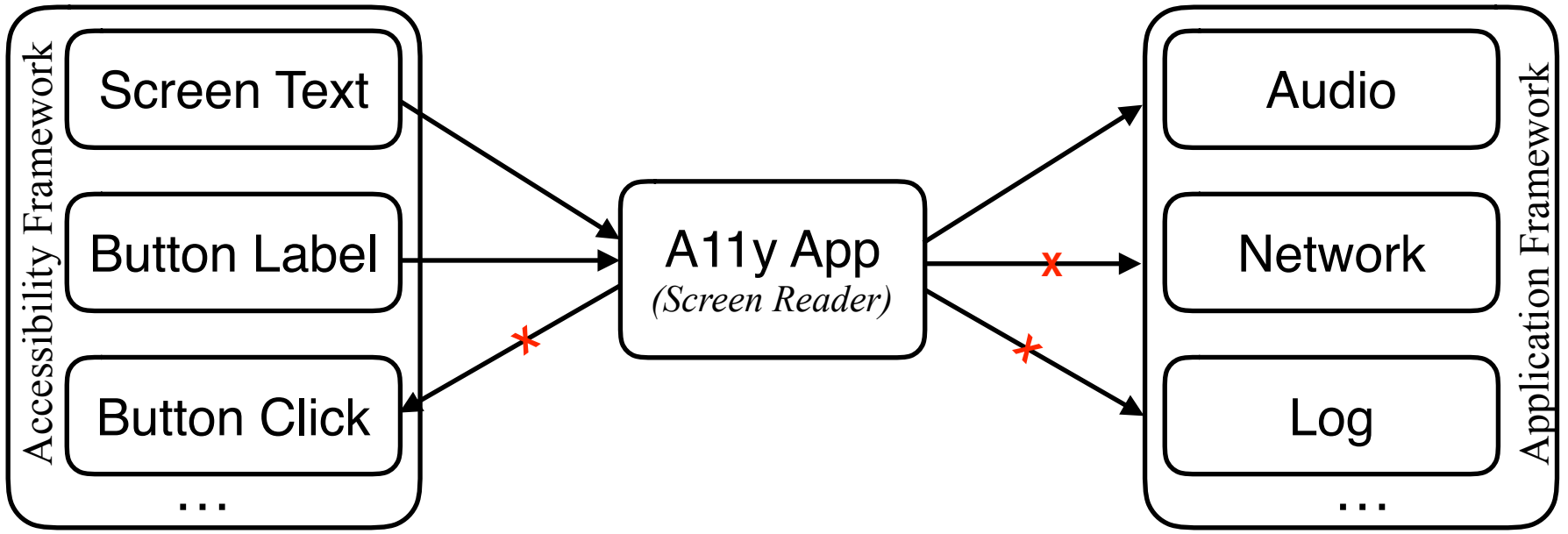
secure on-screen information of apps ← different data destination

associate UI operations with user intentions ← explicit **vs.** silent

user intended **vs.** against user intention

Study of Accessibility Service Usage

- Accessibility App Sample Set (57 malicious, 36 utility, 8 a11y)
- Distinguish based on configuration? NO
- Distinguish based on API usage? NO
- Distinguish based on complete pipeline? YES



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

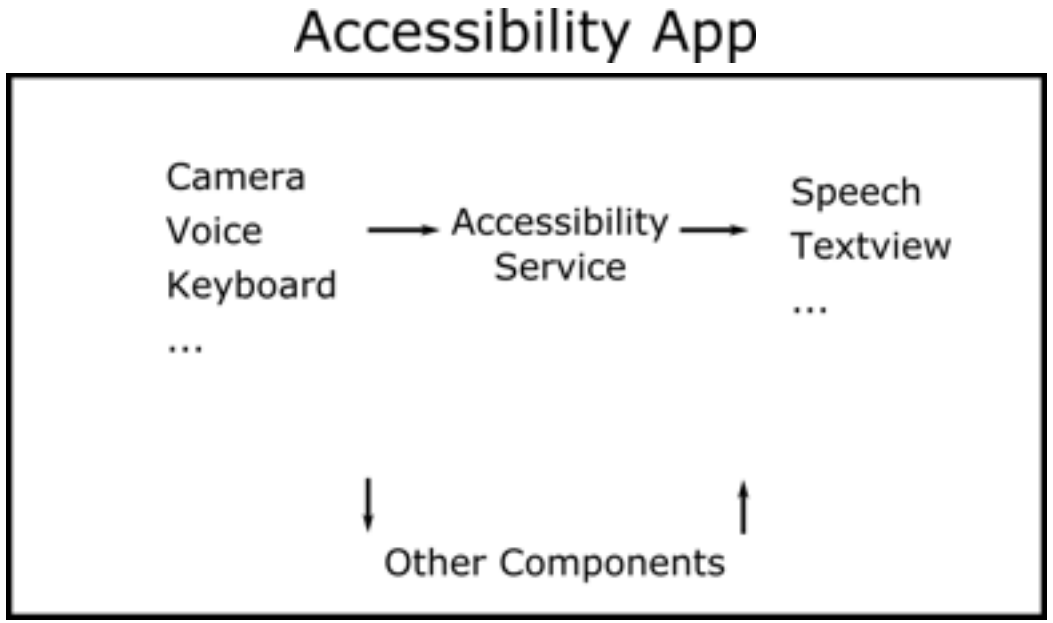
- Ac
- Dis
- Dis
- Dis

Our Solution

- treat the accessibility **pipeline** as a sequence of **steps**
- **redesign** the accessibility framework such that
  - those steps are made **explicit**
  - each step's privileges and I/O can be individually governed by a **least-privilege privacy policy**
  - the content of each step is treated as a **blackbox**

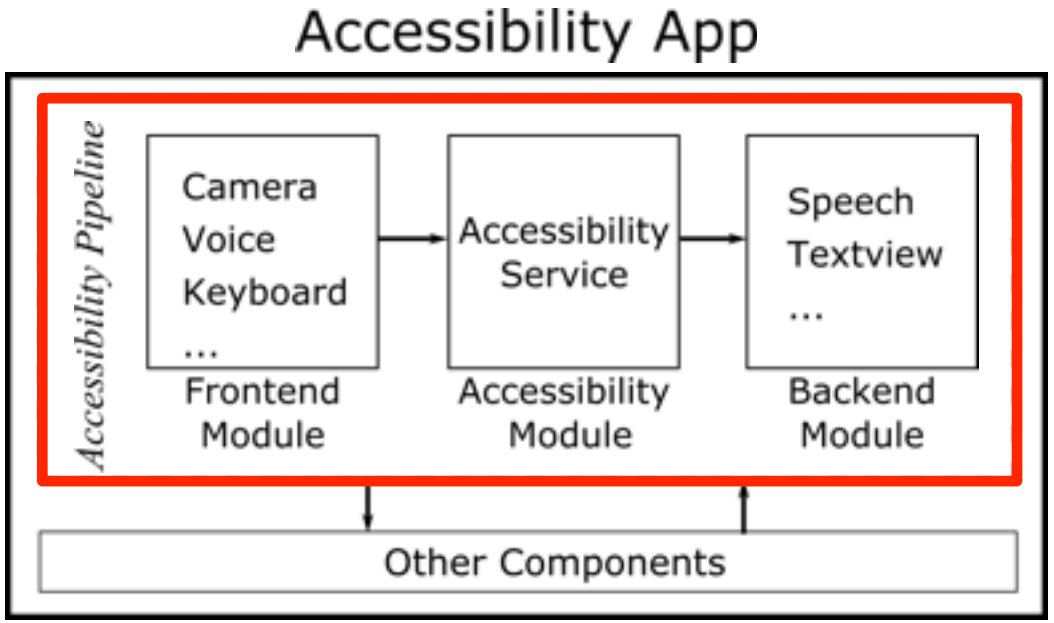
Privacy-Enhanced Accessibility Framework

- Accessibility Pipeline



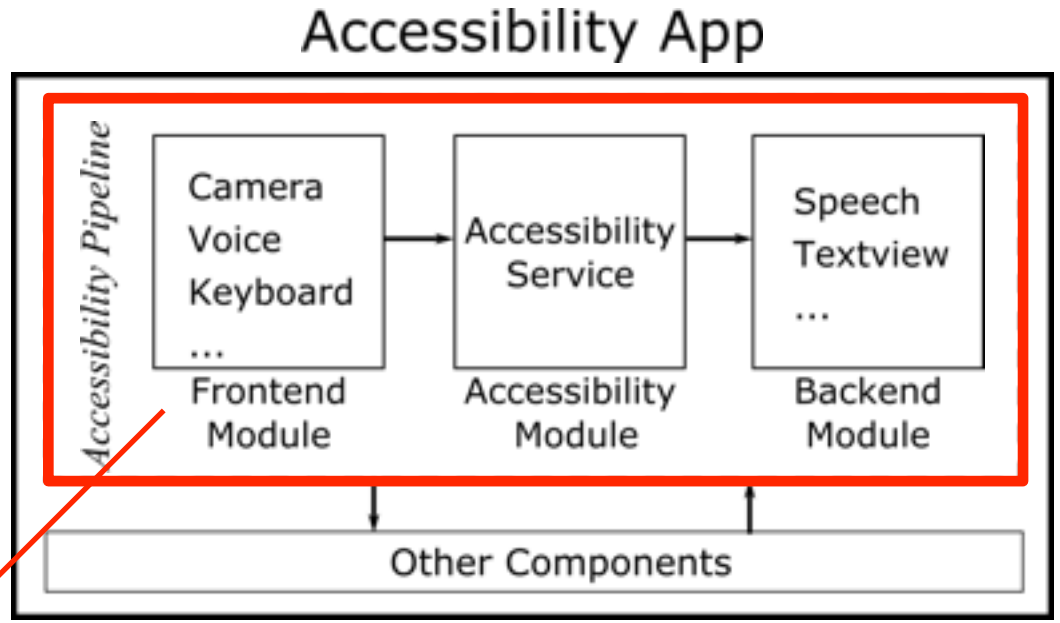
Privacy-Enhanced Accessibility Framework

- Accessibility Pipeline



Privacy-Enhanced Accessibility Framework

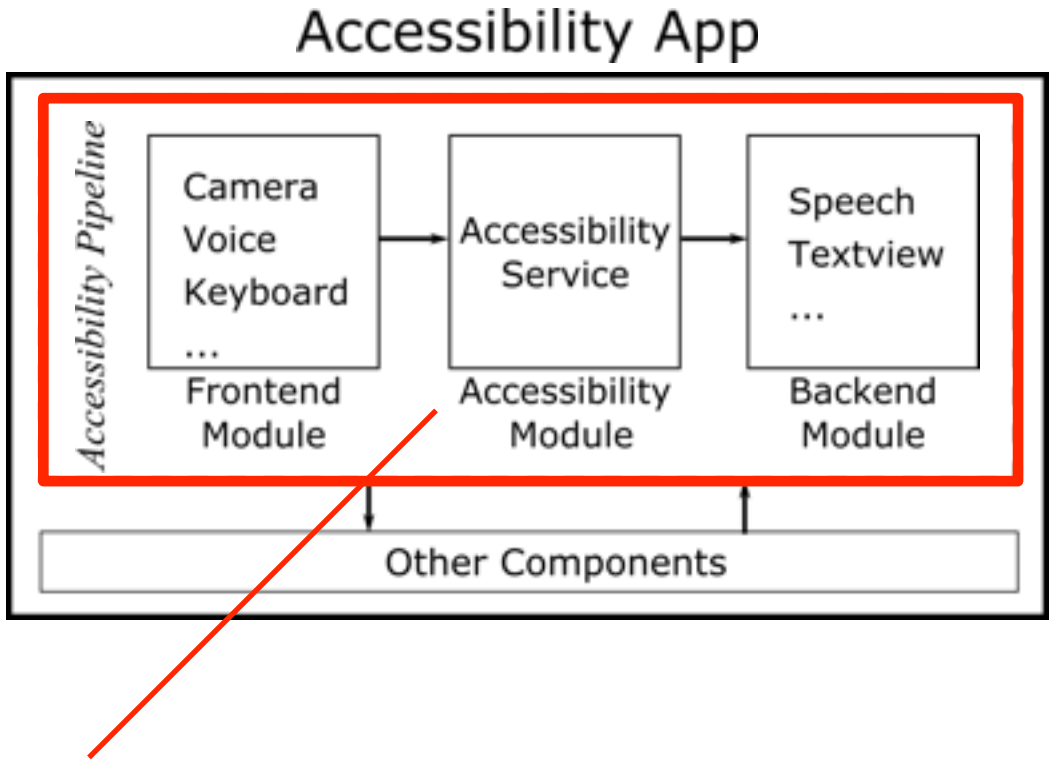
- Accessibility Pipeline
  - Frontend Module



gather user **intentions** from sensors or peripherals

Privacy-Enhanced Accessibility Framework

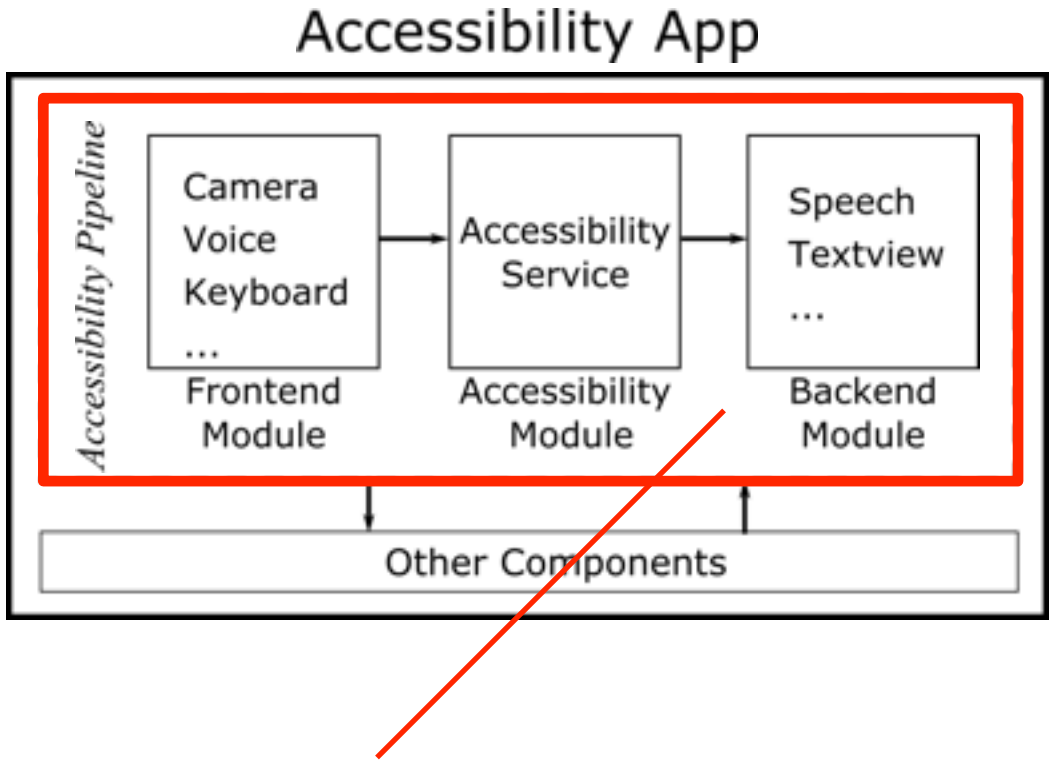
- Accessibility Pipeline
  - Frontend Module
  - Accessibility Module



perform UI operations or retrieve sensitive information via accessibility framework

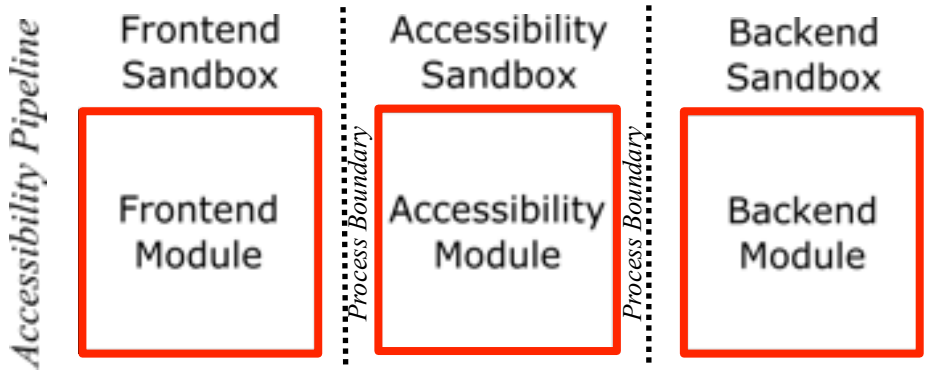
Privacy-Enhanced Accessibility Framework

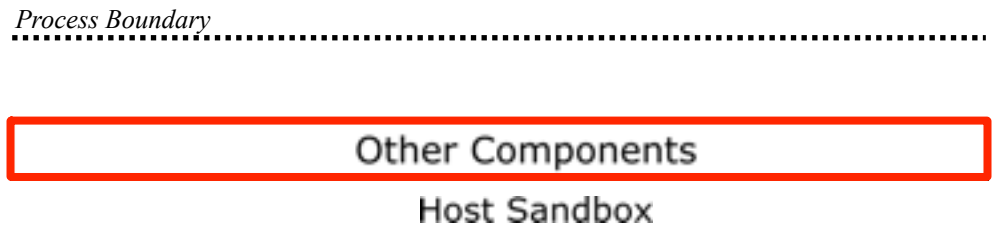
- Accessibility Pipeline
  - Frontend Module
  - Accessibility Module
  - Backend Module



Privacy-Enhanced Accessibility Framework

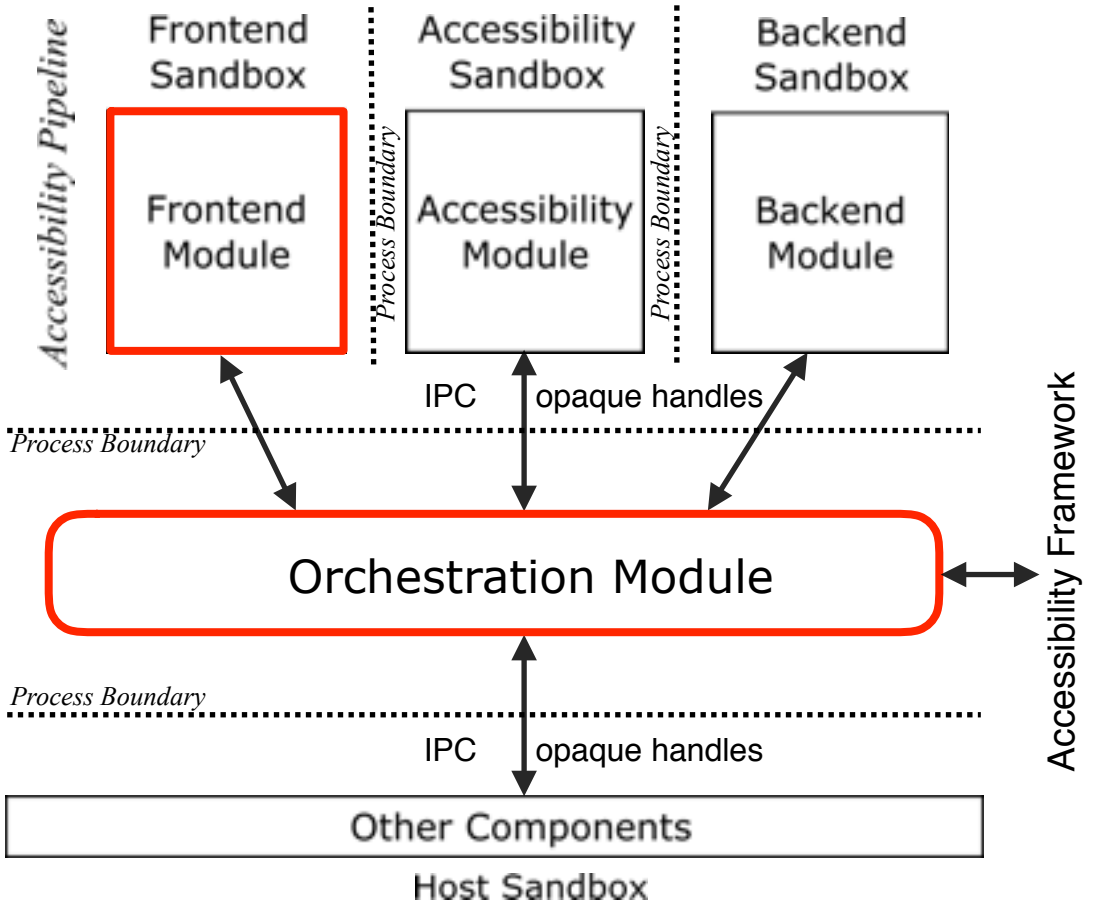
- Accessibility Pipeline
  - Frontend Module
  - Accessibility Module
  - Backend Module
- Least-privilege Privacy Policy
  - Separate Sandboxes [SEC'12, ASIACCS'12, CCS17]





Privacy-Enhanced Accessibility Framework

- Accessibility Pipeline
  - Frontend Module
  - Accessibility Module
  - Backend Module
- Least-privilege Privacy Policy
  - Separate Sandboxes [SEC'12, ASIACCS'12, CCS'17]
  - Information Flow Control
    - opaque handles [SEC'16]
  - Recognizers [SEC'13]

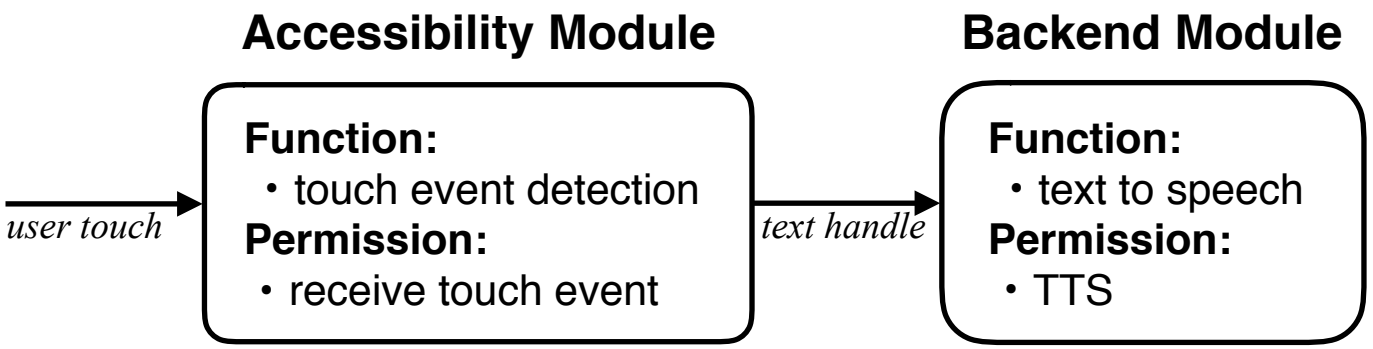


Evaluation

- Case Study 1: TalkBack

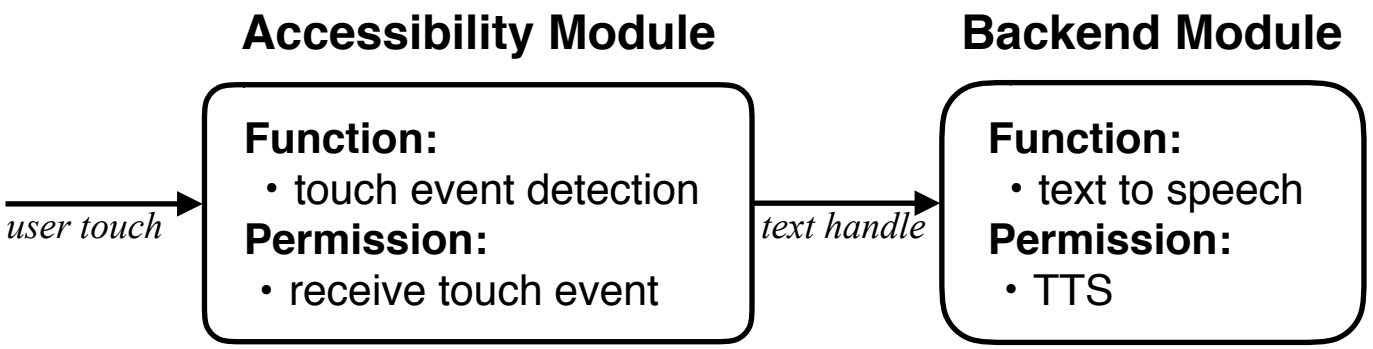
Evaluation

- Case Study 1: TalkBack



Evaluation

- Case Study 1: TalkBack



- Case Study 2: EVA Facial Mouse

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Problem

The accessibility service is so powerful and unconstrained that it is easy to be misused.

All the existing solutions make accessibility and privacy mutually exclusive.

Our Solution

We treated the accessibility pipeline as a sequence of explicit steps and tried to control data flows between steps.

Contribution

We made the first step towards making A11y and privacy not mutually exclusive anymore.

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Thank you!

Q&A

jie.huang@cispa.saarland