TÉCNICO LISBOA

University of Lisbon

inesc id lisboa

A Case for Enforcing App-Specific Constraints to Mobile Devices by Using Trust Leases

Nuno Santos

Nuno O. Duarte, Miguel B. Costa, and Paulo Ferreira

HotOS'15

Sometimes, Your Mobile Must Be Restricted

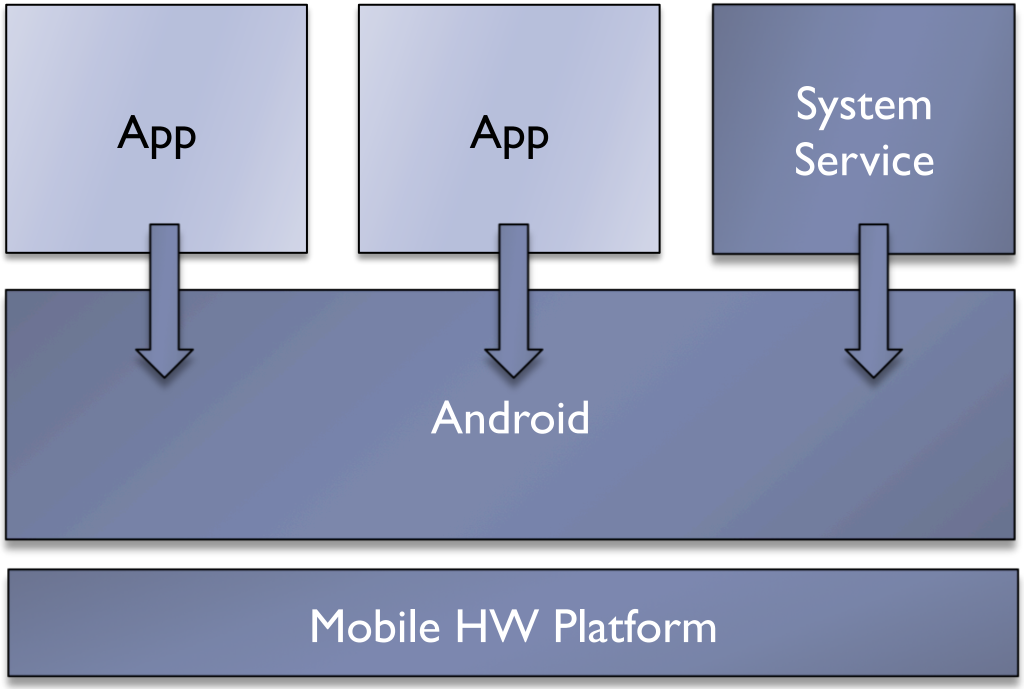
- Example: in movie theaters, people forget to turn off phones

More Motivating Examples

- In business meetings, prevent info leaks by spyware
  - Need to block untrusted apps in background
- Improve security of photo sharing apps (e.g., Snapchat)
  - Need to prevent taking screenshots
- Allow students to fill out exams on their devices
  - Need to ensure that students don’t cheat

Typical Mobile Security Architecture

- Hard to constrain the functionality of device



- Users can:
  - Install apps
  - Execute apps
  - Grant permissions
  - Configure system

Our Wish List

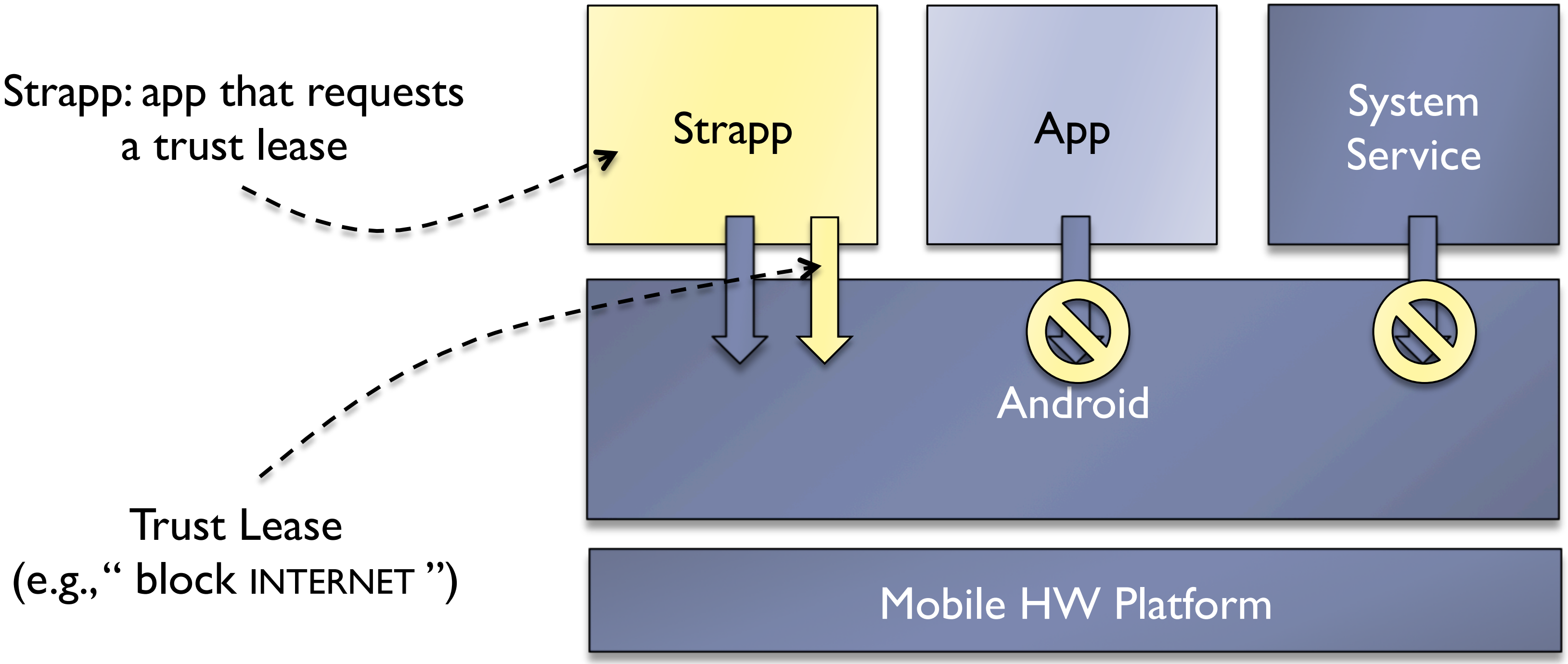
- Enable apps to globally restrict access to resources

- Find a sweet spot between user / app control

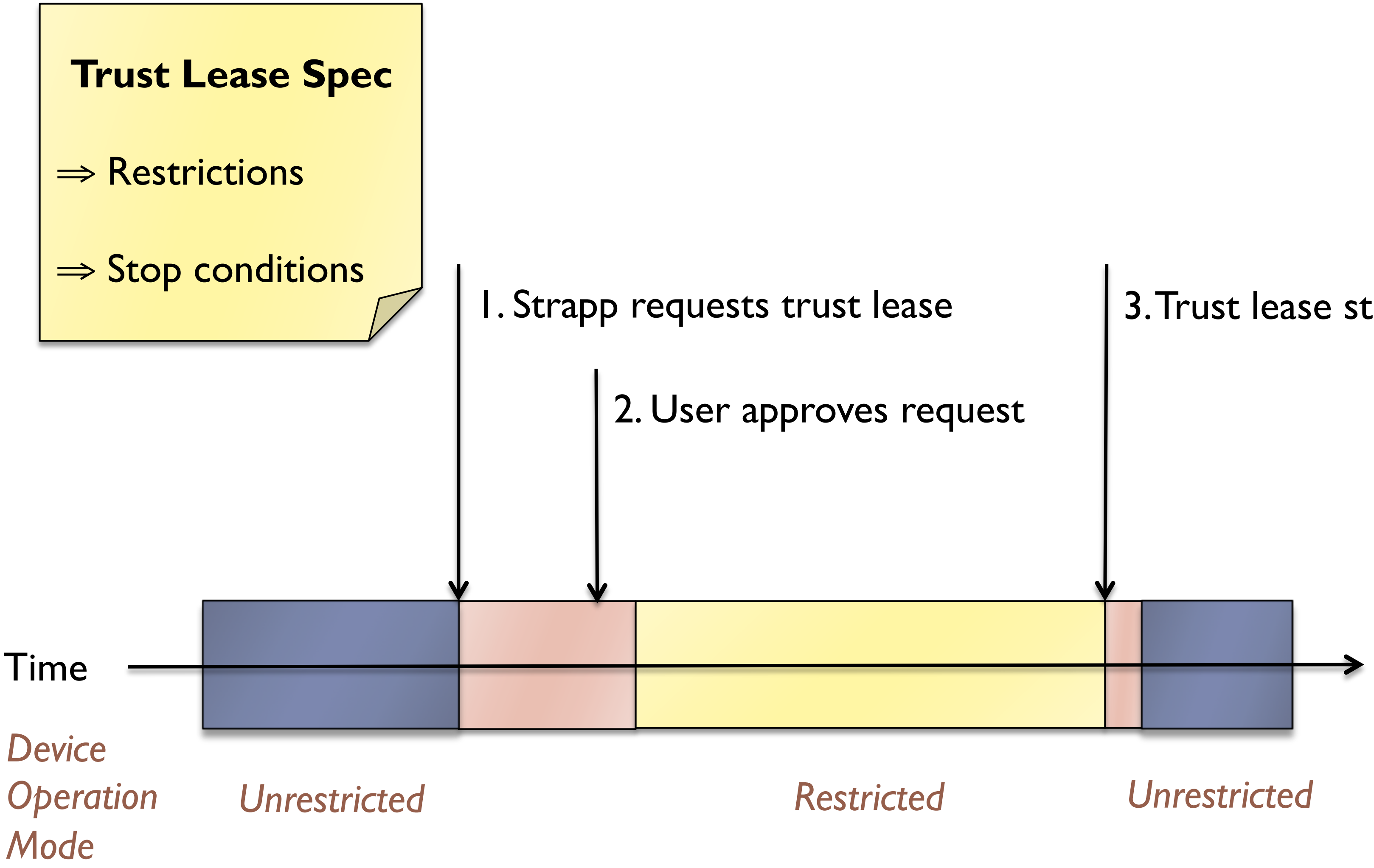
- Able to give to third-parties guarantees of enforcement

Trust Lease

- Novel OS primitive to let apps restrict device functionality


Strapp: app that requests a trust lease
Strapp
App
System Service
Android
Trust Lease (e.g., " block INTERNET ")
Mobile HW Platform

Trust Lease: Contract between Strapp and User



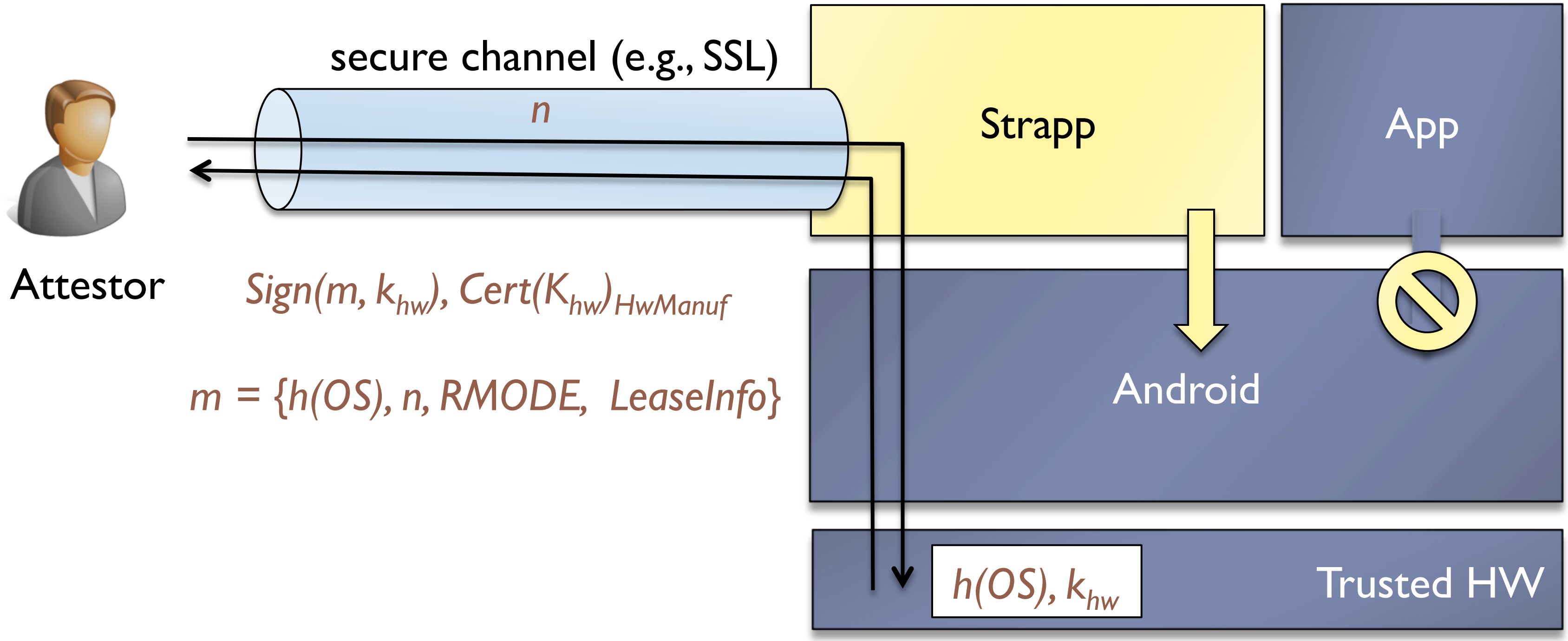
Trust Lease: Restrictions and Stop Conditions

- Restrictions:
  - Access to resources (e.g., network, camera, etc.)
  - Changes to system configurations (e.g., enable the sound)
  - Execution of applications

- Stop conditions:
  - Timeout
  - Voluntary termination
  - Others triggered by environment events (e.g., location based)

Trust Lease: Remotely Check Lease Enforcement

- Remote attestation
  - Leverage trusted computing HW (e.g., TrustZone, TPM)
  - Platform has strong identity and secure boot capabilities
  - Assume that the OS is correct



secure channel (e.g., SSL)
n
Attestor
$Sign(m, k_{hw}), Cert(K_{hw})_{HwManuf}$
$m = \{h(OS), n, RMODE, LeaseInfo\}$
Strapp
App
Android
$h(OS), k_{hw}$
Trusted HW

Use Case 1: Auto Phone Mute in Movie Theaters

- eTicketing strapp that handles cinema tickets

- Upon ingress, a trust lease is issued to mute the device
- Stop condition: timeout = movie duration or exiting event
- Device is attested when validating the tickets

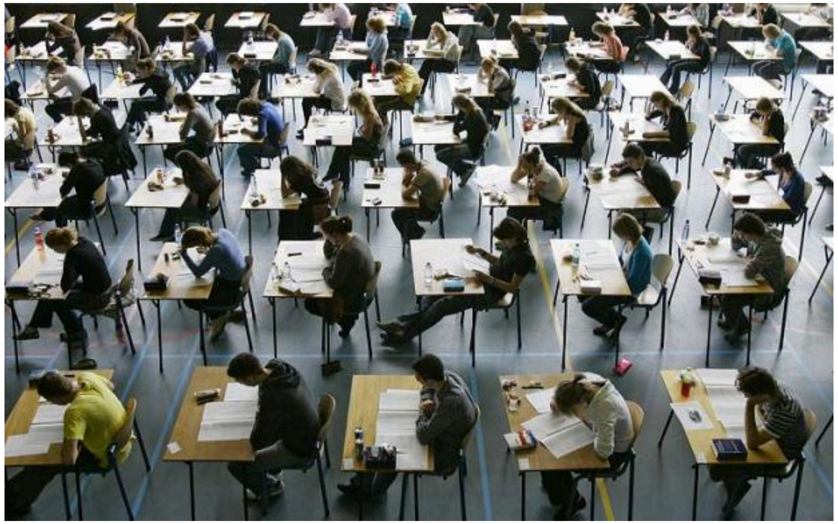
Use Case 2: Private Mode in Business Meetings

- eMeeting strapp to prevent info leaks (e.g., by malware)

- Trust lease to kill all but a few trusted apps (e.g., email, calendar)
- Trust lease finishes after timeout or coordination event
- Meeting leader attests everyone's devices before the meeting starts

Use Case 3: Exams on Students' Mobile Devices

- eExam strapp to let students fill out exams on their mobiles w/o cheating



- A trust lease blocks the device to run the eExam strapp only
- Trust lease active for the exam duration, or until exam submission
- The exam supervisor attests the device when entering and leaving

Conclusions & Current Status

- In certain scenarios, mobile devices must be constrained
- Our proposal: security architecture based on trust leases
- Trust leases enable dynamic restriction of devices’ functionality
- Currently extending Android and working on use cases

Thanks!
Questions?

http://www.gsd.inesc-id.pt/~nsantos/