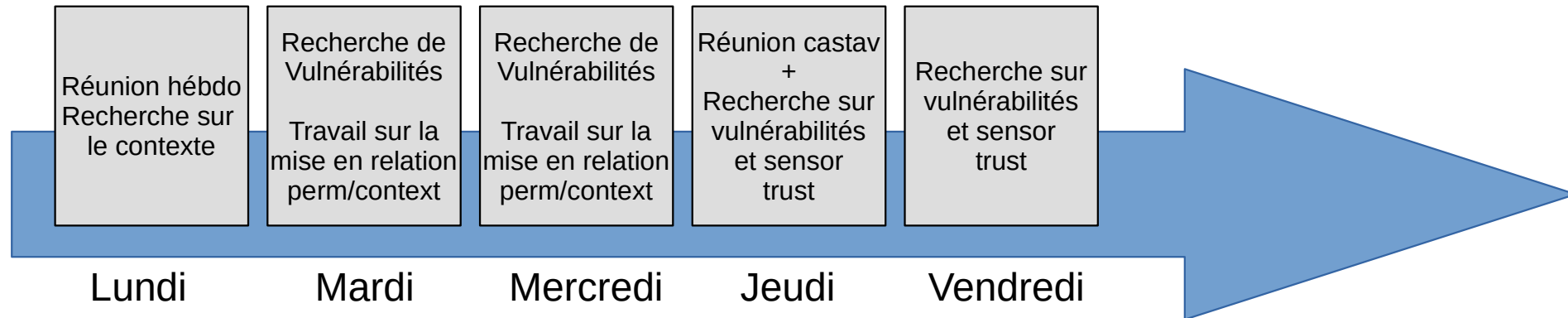


# Réunion hebdomadaire 1

20/09/2021

## Overview de la semaine



*Ivan BAHEUX*

*Semaine 37*

# Travail de la semaine dernière : s 37

Rappel présentation CASTAV (Il me faut un nom de projet)

Progress on the topic :

⇒ Study of subject terms :

- Context
- Permission system
- Model-based security testing (MBST)

⇒ Early work on context-dependent vulnerabilities and on the permission system of Android

# Travail de la semaine dernière : s 37

Rappel présentation CASTAV (Il me faut un nom de projet)

For the moment 4 possible research axes:

- Vulnerabilities related to context dependent code  
e.g.: If `no_wifi()` then [Vulnerability].
- Vulnerabilities related to sensor trust / permissions  
e.g.: if `scan_face_with_camera() == bank_user_face` then ...
- Vulnerabilities related to a delegation of permissions  
ex : Confused deputy attack / Indirect collusion attack
- A combination of the above

# Travail de la semaine dernière : s 37

## Travail sur la relation entre capteurs, permissions et vulnérabilités

### Pourquoi ?

- ADB et d'autres outils récents (SMASheD) permettent d'écrire dans les capteurs et ainsi « mentir » aux applications se servant du contexte
- Il s'agit de la piste de la diapo 3 qui semblait la plus complète

### Avancée

- Travail sur les outils d'attaque :
  - SMASheD
- Travail sur la littérature liée à mon sujet et aux capteurs :
  - *A Context-Aware Framework for Detecting Sensor-Based Threats on Smart Devices*
    - *Machine learning*
    - *Détection durant l'exec*

### Que reste-t-il ? / Questions

- Une piste intéressante ?
- Une idée pour la suite :
  - Static Information Flow control
    - Devrait détecter les data-leak, les confused deputy et les collusion attack
    - Possiblement déjà existant bien que rien directement en relation avec le contexte
    - En relation avec les permissions et leak de privilège
- Des idées / conseils ?

# Réunions à venir

Réunion KTH: mardi 20 septembre à 15h

# Travail à venir

Prévisionnel pour la suite :

Choix de la piste à suivre d'ici mardi 20 septembre ?

- En fonction de vos conseils et de mes recherches

Écriture de l'état de l'art (Background) du contexte

En fonction du choix :

- Écrire état de l'art sur les vulnérabilités
- Écrire état de l'art sur le security testing (plus court)