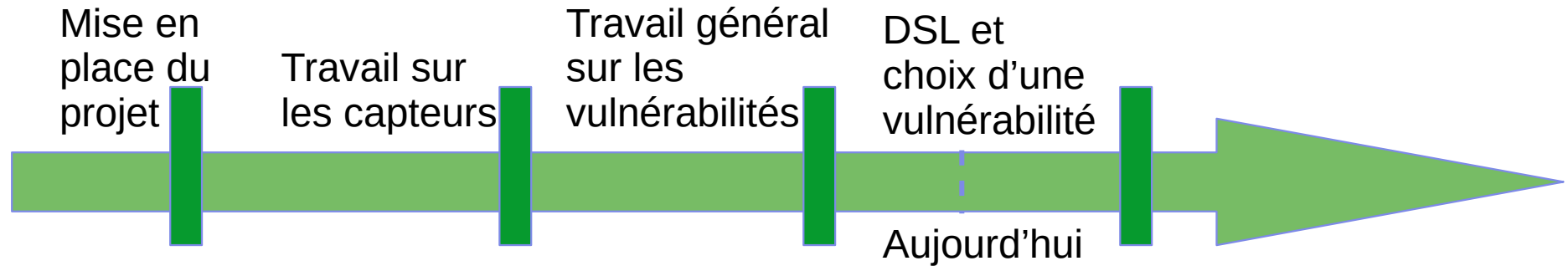


Context-aware security testing of Android applications

État du projet 2 :
Au 13/10/2022

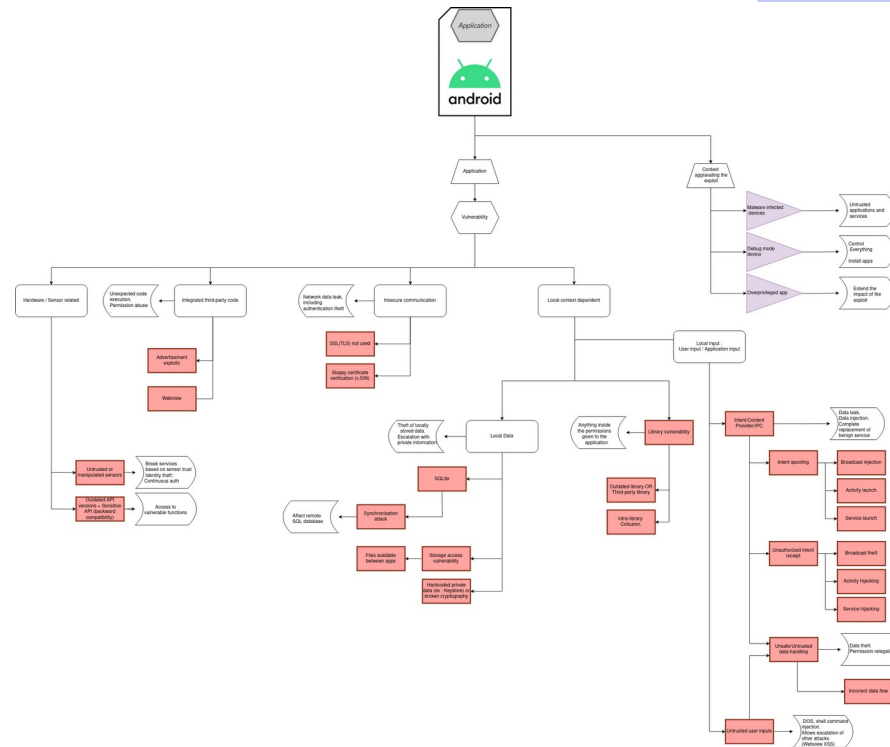


Ivan : Travail réalisé

- Travail de littérature sur :
 - L'architecture Android et le système de permissions
 - Le contexte (Définition et évolution dans le temps)
 - Les vulnérabilités Android (Etude sur les travaux recents)
 - Mise en relation avec des catégories plus globales (CWE)
- En ce moment :
 - Travail sur les DSL et les tests de sécurité.

Ivan : Vulnerability survey

Survey on vulnerabilities relating to Android applications



Vulnérabilités intéressantes

- Vulnérabilités en lien avec la backward compatibility des API Android :
 - Exemple :
 - Avant API level 28 (~1/4 des appareils)
 - Configuration par défaut accepte HTTP
 - Man In The Middle
- Interet :
 - Génération de tests par version prouvant la sécurité à toute version
 - Lié au contexte de l'appareil et semble implémentable avec le DSL de A.Adwan (après amélioration)