Resum

La disponibilitat de nous processadors amb major potencia de còmput per a aplicacions empotrades ha permès el desenvolupament de aplicacions que aborden problemes de major complexitat. Degut a açò, les aplicacions empotrades actualment tenen més funcions i prestacions, i com a conseqüència, una major complexitat. Per aquest motiu, existeix un interès creixent en per permetre la execució de múltiples aplicacions de forma segura i sense interferències en un mateix processador i memòria. En aquest marc sorgeixen les arquitectures de sistemes particionats basats en hipervisors com una solució apropiada per a la construcció de sistemes segurs
Un dels principals reptes en la construcció de sistemes particionats, es la verificació del correcte funcionament del hipervisor, donat que aquest es el component crític sobre el que descansa la seguretat del sistema particionat complet. Les tècniques tradicionals de V&V, com són el testing, inspecció i anàlisi, presenten limitacions que fan impracticable la seva aplicació per a la verificació exhaustiva del comportament del sistema, degut a que el espai de entrades a verificar creix de forma exponencial amb el nombre de entrades a verificar. Front a aquestes limitacions les tècniques de verificació basades en mètodes formals sorgeixen com una alternativa per a completar les tècniques de validació tradicional.

Aquesta dissertació es centra en la aplicació de mètodes formals per a validar la correcció del sistema particionat, en especial d del hipervisor XtratuM. La validació de la metodología es realitza aplicant les tècniques proposades a la validació del hipervisor. Per a aquest fi, es proposa un model formal del hipervisor basat en màquines de estats finits (FSM), aquest model formal permet la definició de les propietats que el disseny del hipervisor deu de complir per assegurar la seva correcció. Addicionalment, aquesta dissertació analitza com assegurar la correcció funcional de la implementació del hipervisor mitjançant tècniques de verificació deductiva de codi.

Per últim, s'estudien les vulnerabilitats de tipus *information leak* (CWE-200 [CWE08b]) degudes a la pèrdua de la confidencialitat de la informació gestionada per el sistema particionat. En aquest àmbit, es modelen les vulnerabilitats, s'apliquen tècniques de anàlisis de codi per a la detecció de les vulnerabilitats en base al model definit, per últim es valida la tècnica proposada mitjançant un cas pràctic sobre el nucli del sistema operatiu Linux que forma part de l'arquitectura particionada.