Citadel: A Trusted Reference Monitor for Linux using Intel SGX Enclaves

A.H. Bell-Thomas

Computer Laboratory, University of Cambridge

26th June, 2020

Background

Background

1. **Reference Monitor**

Background

1. **Reference Monitor**
   $\rightsquigarrow$ *Information Flow Control*

Background

1. **Reference Monitor**
   $\rightsquigarrow$ *Information Flow Control*

2. **Intel SGX**

Information Flow Control

- Access Control specifics *who* can access resources. IFC also mediates *how* they can be used once opened.
- Construct an abstract system of *entities*;
  $\rightsquigarrow$ processes, files, sockets, etc.
- Each *entity* carries a *security context*, defining its granular ownership or restriction information.
- Aim: achieve *non-interference* between all *security contexts*.

Information Flow Control

Very briefly;

- **Tagging**
  Entities must be uniquely and reliably identifiable to support decisions.

- **Tracking**
  Contexts are mutable to accommodate an evolving situation.

- **Policy Decisions**
  Is an operation acceptable given its consequences?
  e.g. $A \to B \iff A_s \preceq B_s \ \wedge \ A_i \succeq B_i$

Decentralised Information Flow Control

- Centrally administered systems are highly restrictive.
- Idea: let entities specify their own protection policy for assets they own. Enforcement becomes *discretionary*, allowing more flexibility and support for operations such as *declassification*.

Enforcement is implemented using a *reference monitor*.

Intel SGX

Motivation

Citadel

Results

Related Works