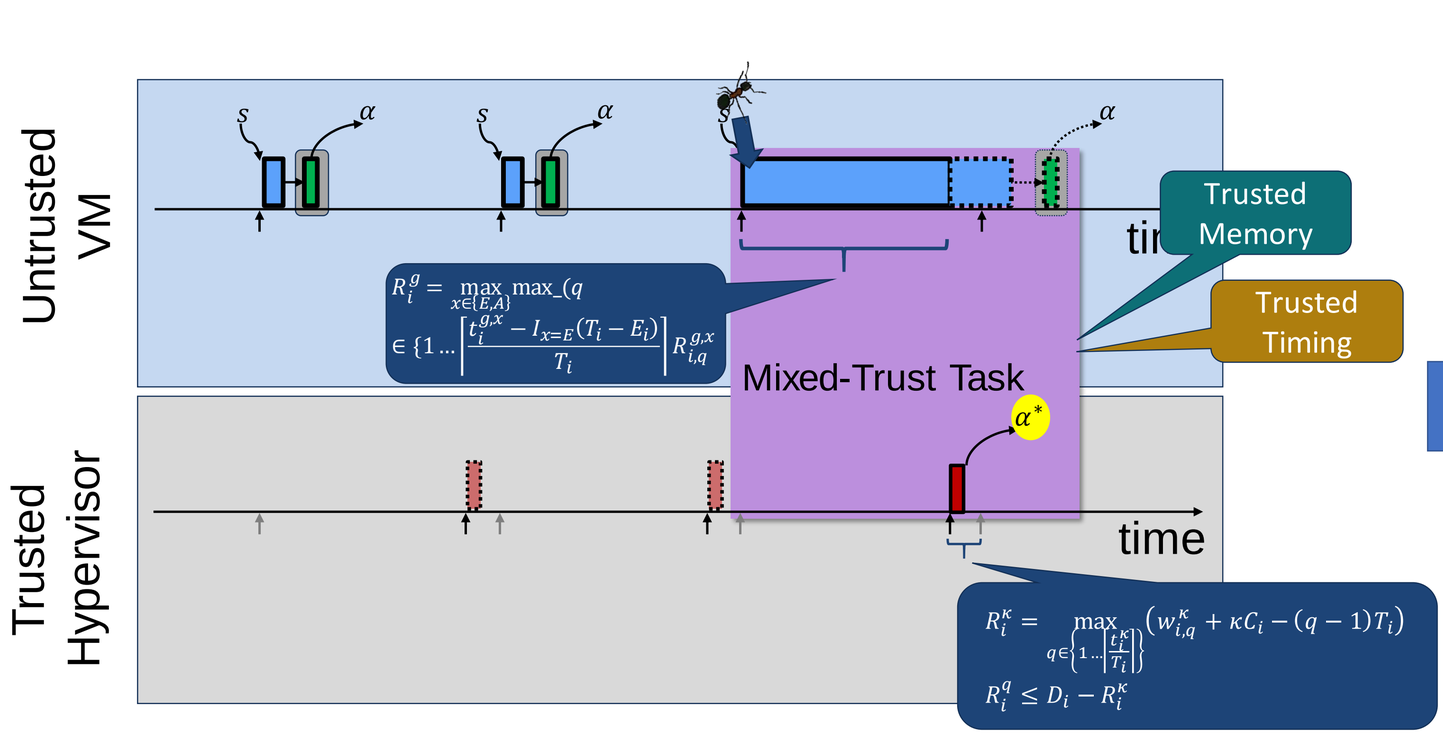
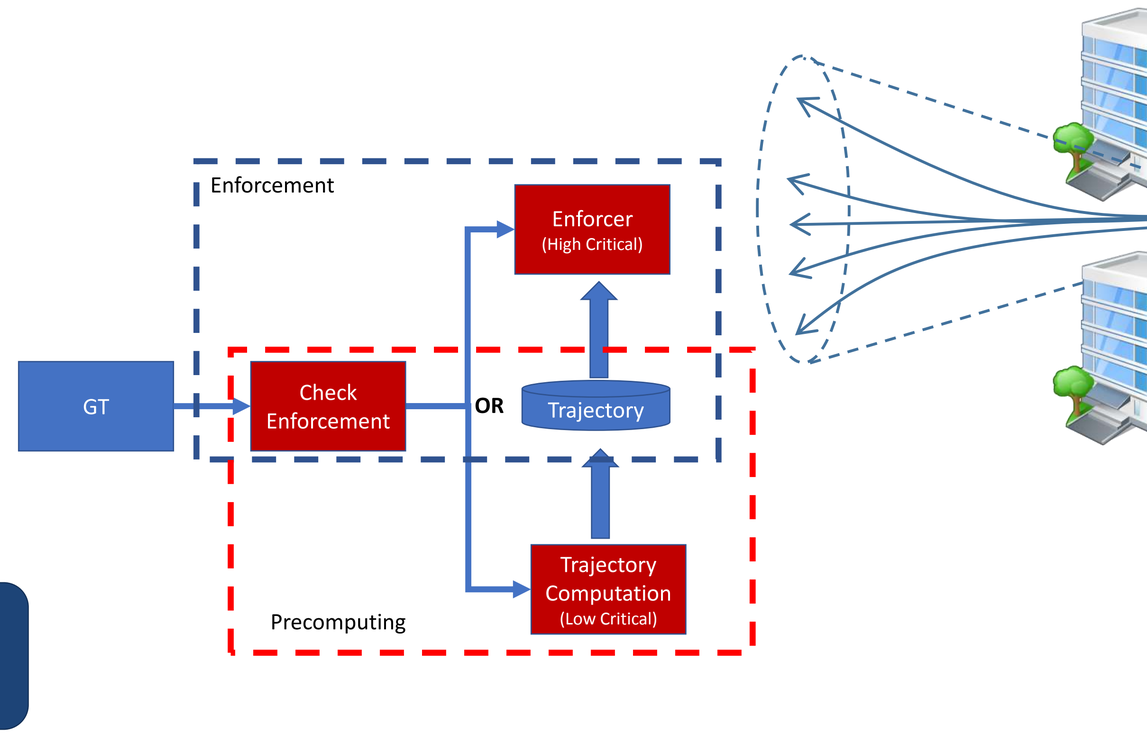
This material is based upon work funded and supported by the Department of Defense under
No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Eng
Institute, a federally funded research and development center.

DM20-1076





Mixed Trust Scheduling Combines (in mixed-trust task)
- Untrusted part (Guesttask - GT) in VM (preemptive FP)
- Trusted part (Hypertask - HT) in verified HV (non-preemptive FP)
- to monitor and enforce safety properties (w trusted timing)

Enforcement may need to look ahead (trajectori
Precomputing reuses time unused by HT

- To pre-plan enforcement (e.g., trajectories)

Based on multi-frame scheduling:

- Response time sketch: $R_i^p = \kappa C_i^p + \sum \left\lceil \frac{R_i^p}{T_j} \right\rceil \kappa C_j^p - \left\lfloor \frac{R_i^p}{I_j T_j} \right\rfloor \left(\kappa C_j^p - \kappa C_j^e\right)$
  - With: WCET predictive: κC_i^p, WCET enforcer κC_j^e, Ratio of predictive to enforcer I_j
- Non-preemptive
  - Enforcement
  - Prediction

$$R_i^{\kappa,e} = \max_{q\in\{1\dots\left\lceil\frac{t_i^\kappa}{T_i}\right\rceil\}} (w_{i,q}^\kappa + \kappa C_i^m - (q-1)T_i),$$

$$t_i^{g,x} = \left(\sum_{j\in L_i} \text{rbf}_j^E(t_i^{g,x}, 0)\right) + \text{rbf}_i^x(t_i^{g,x}, 1) + \sum_{j\in H_i} \max_{y\in\{E,A\}} \text{rbf}_j^y(t_i^{g,x}, 1),$$

$$w_{i,q}^{g,x} = \left(\sum_{j\in L_i} \text{rbf}_j^E(w_{i,q}^{g,x}, 0)\right) + qC_i + (q-1+\mathcal{B}_{(x=E)})\kappa C_i + \sum_{j\in H_i} \max_{y\in\{E,A\}} \text{rbf}_j^y(w_{i,q}^{g,x}, 1).$$

(6)

$$t_i^{\kappa,p} = \max_{j\in\kappa L_i} \kappa C_j^m + \left\lceil \frac{t_i^{\kappa,p}}{T_i} \right\rceil \kappa C_i^p + CP(i, t_i^{\kappa,p}) + \sum_{j\in\kappa H_i} (\left\lceil \frac{t_i^\kappa}{T_j} \right\rceil \kappa C_j^p + CP(j, t_i^{\kappa,p})),$$

$$w_{i,q}^{\kappa,p} = \max_{j\in\kappa L_i} \kappa C_j^m + (q-1)\kappa C_i^p + Q(i, q-1) + \sum_{j\in\kappa H_i} ((\left\lfloor \frac{w_{i,q}^\kappa}{T_j} \right\rfloor + 1)\kappa C_j^p + CP_w(j, w_{i,q}^{\kappa,p})),$$

$$CP(j, t_i^{\kappa,p}) = \begin{cases} \left\lceil \frac{t_i^{\kappa,p}}{T_j \cdot I_j} \right\rceil (\kappa C_j^e - \kappa C \\ - \left\lfloor \frac{t_i^{\kappa,p}}{T_j \cdot I_j} \right\rfloor (\kappa C_j^p - \end{cases}$$

$$Q(i,q) = \begin{cases} \left\lceil \frac{q}{I_i} \right\rceil (\kappa C_i^e - \kappa C_i^p) \\ - \left\lfloor \frac{q}{I_i} \right\rfloor (\kappa C_i^p - \kappa C_i^e) \end{cases}$$

$$CP_w(j, w_{i,q}^{\kappa,p}) = \begin{cases} (\left\lfloor \frac{w_{i,q}^{\kappa,p}}{T_j \cdot I_j} \right\rfloor + 1)(\kappa C_j^e - \kappa C \\ - \left\lfloor \frac{w_{i,q}^{\kappa,p}}{T_j \cdot I_j} \right\rfloor (\kappa C_j^p - \kappa C_j^e) \end{cases}$$