Attack Model in the Presence of Trusted Hardware

2007-03-21

Thomas Herlea
(presented by Jan Cappaert)

Katholieke Universiteit Leuven

for RE-TRUST Work Package 3 Step 4

Attack Model Methodology

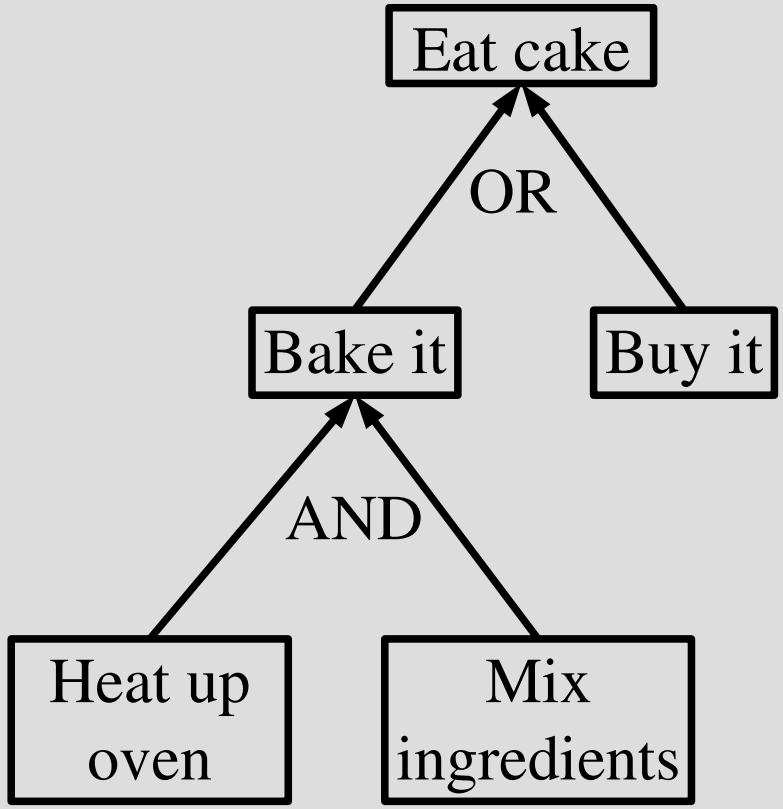
- Define assets
- Characterize attackers
  - Goals
  - Means
  - Limitations
- Describe attacks

See presentation from Trento, December 2007

Today's talk

Attack Trees

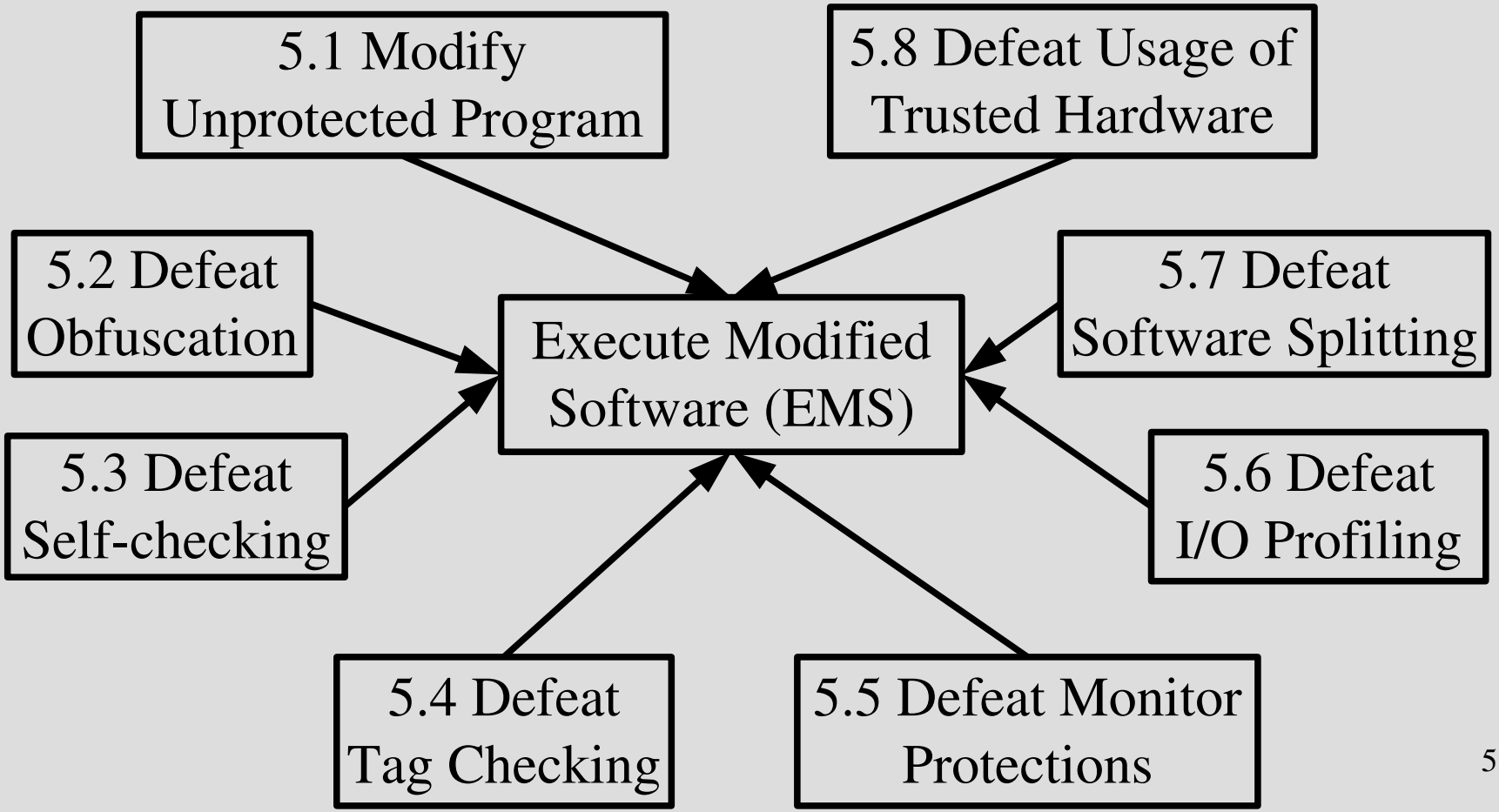
- Suggested by Bruce Schneier
- Applicable in the "Describe Attacks" step of the Attack Model



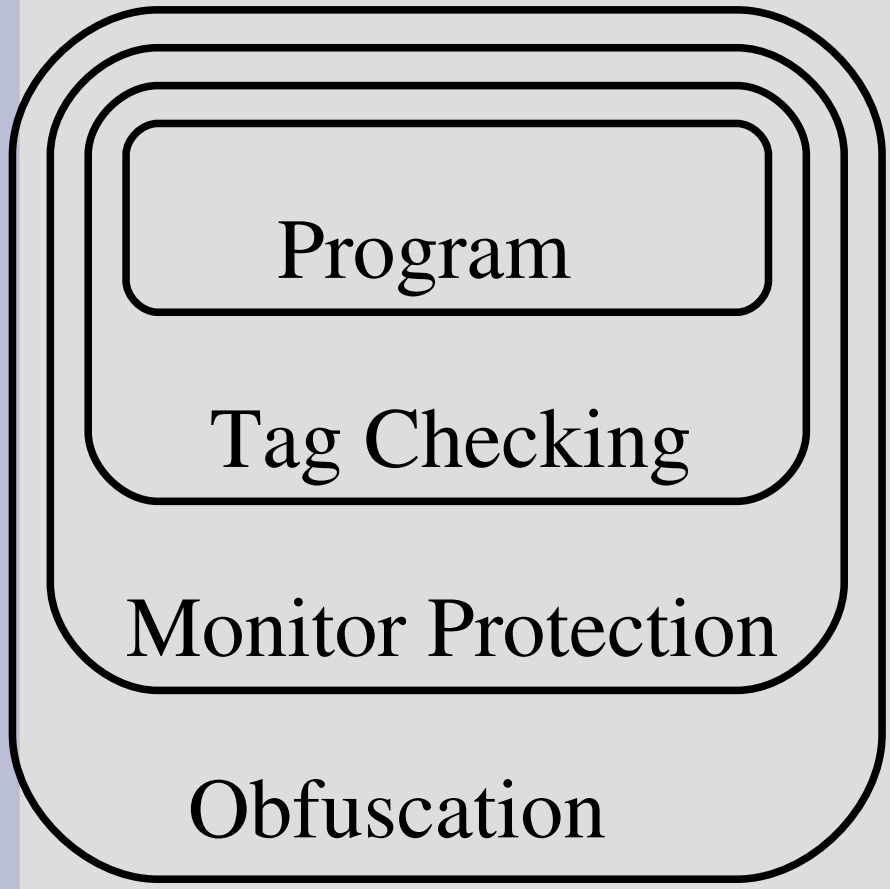
Disclaimers

- Attack Models are normally done for a concrete system
- We made assumptions about the defences
- Most ideas using trusted hardware (WP3) also work with just a trusted server (WP2)
- Instead of attack trees we needed directed acyclic graphs

Root of the Attack Tree

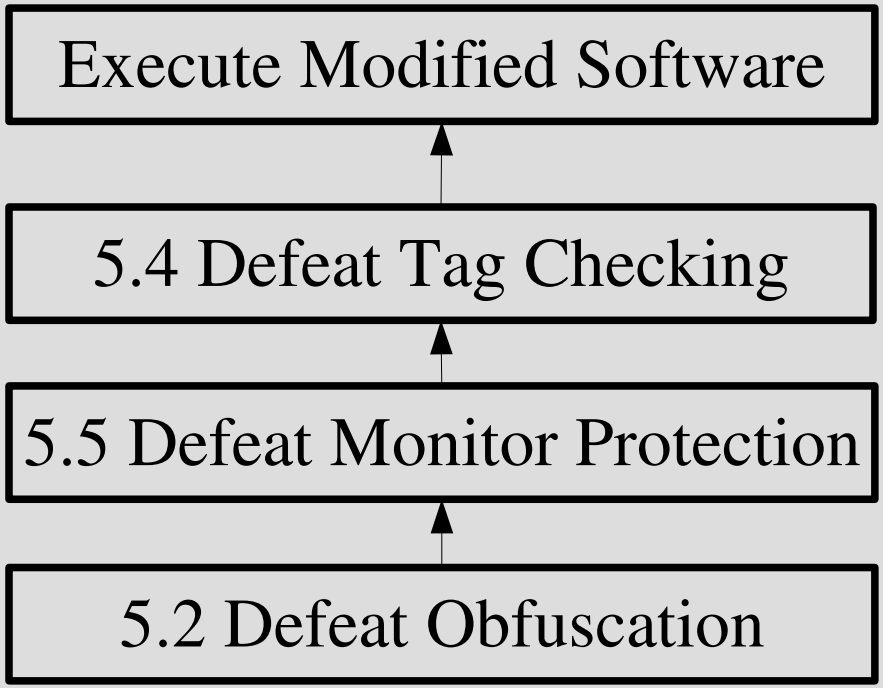


Example: Layered Defences

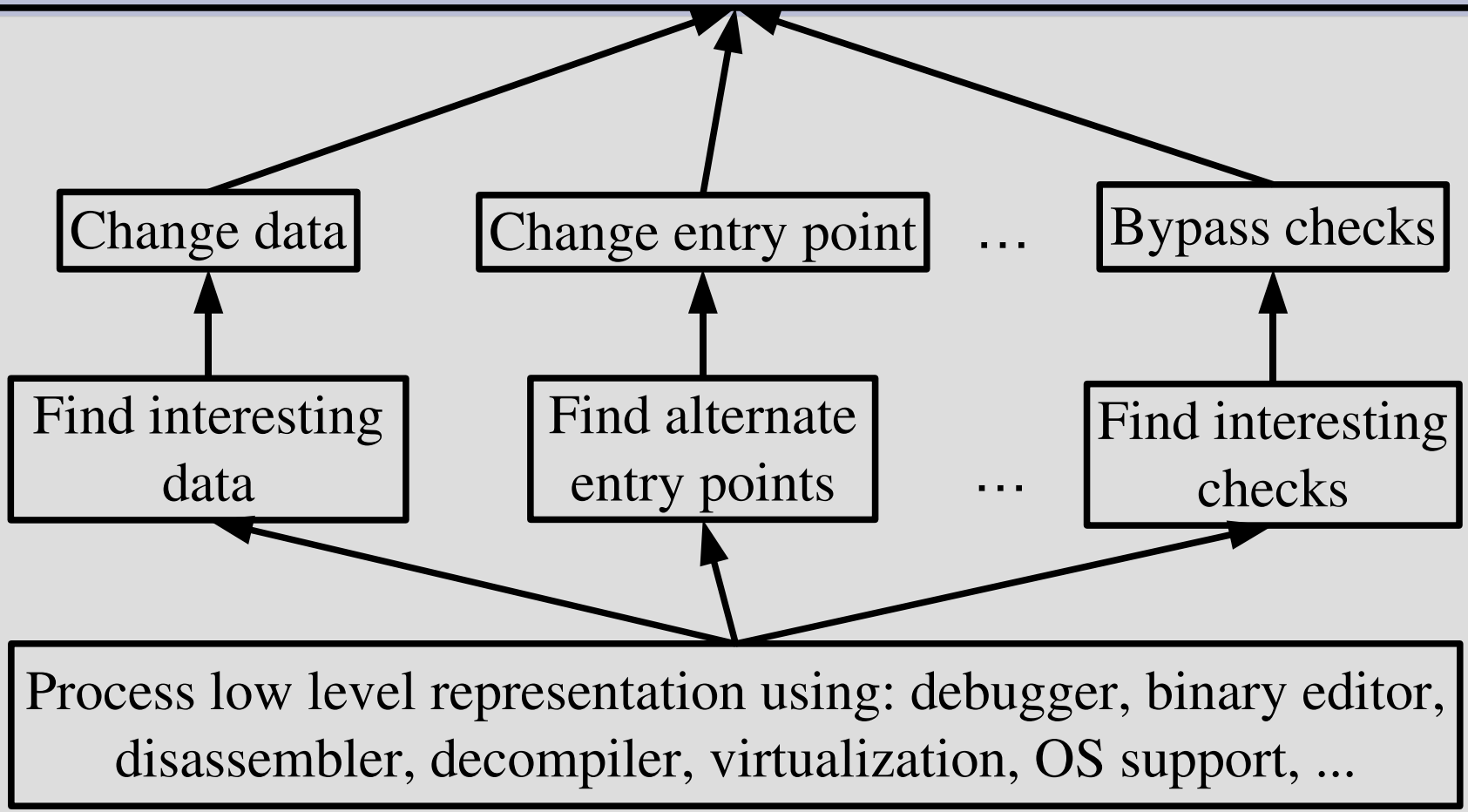


⇒

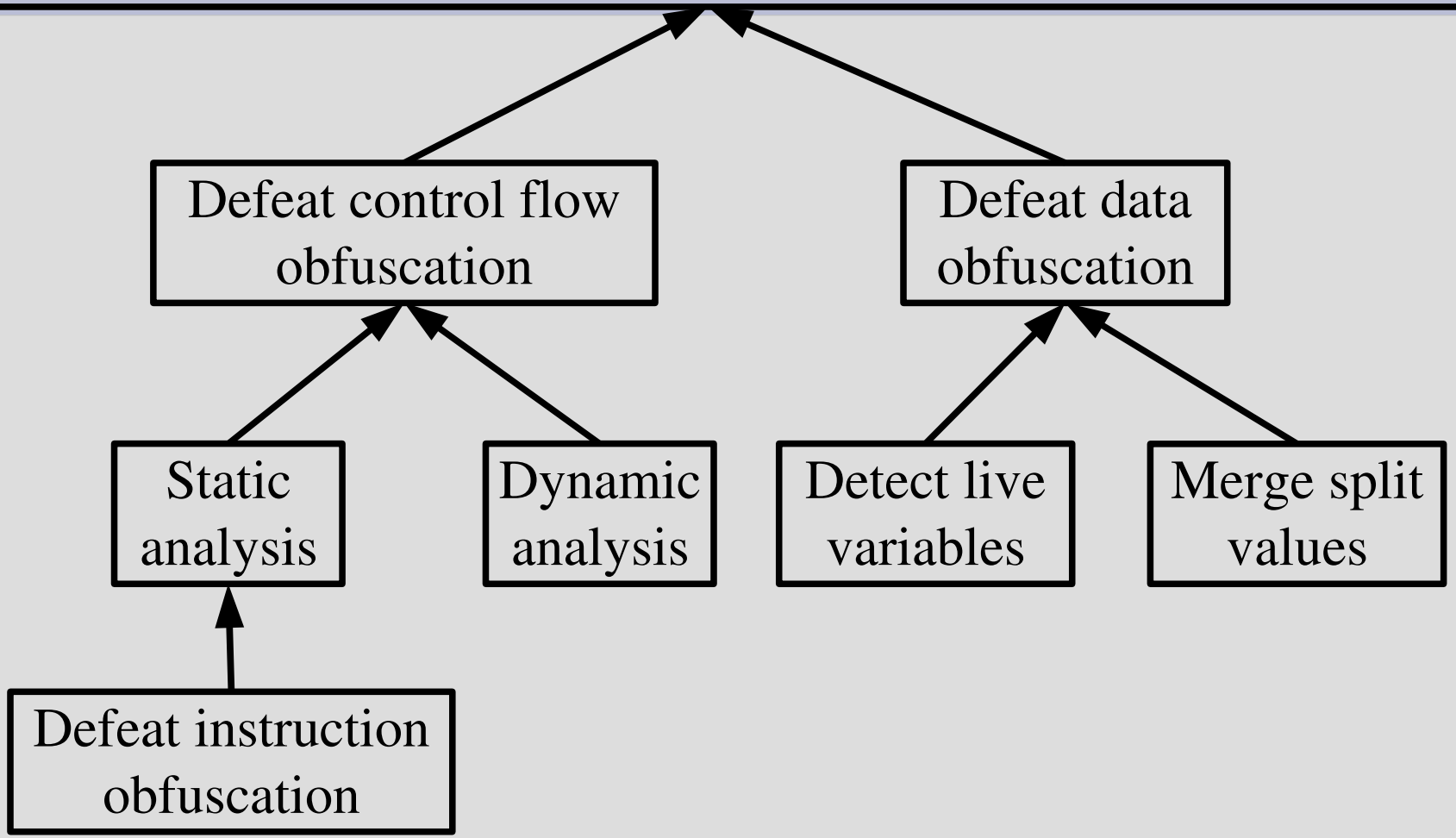
Concrete Attack Tree



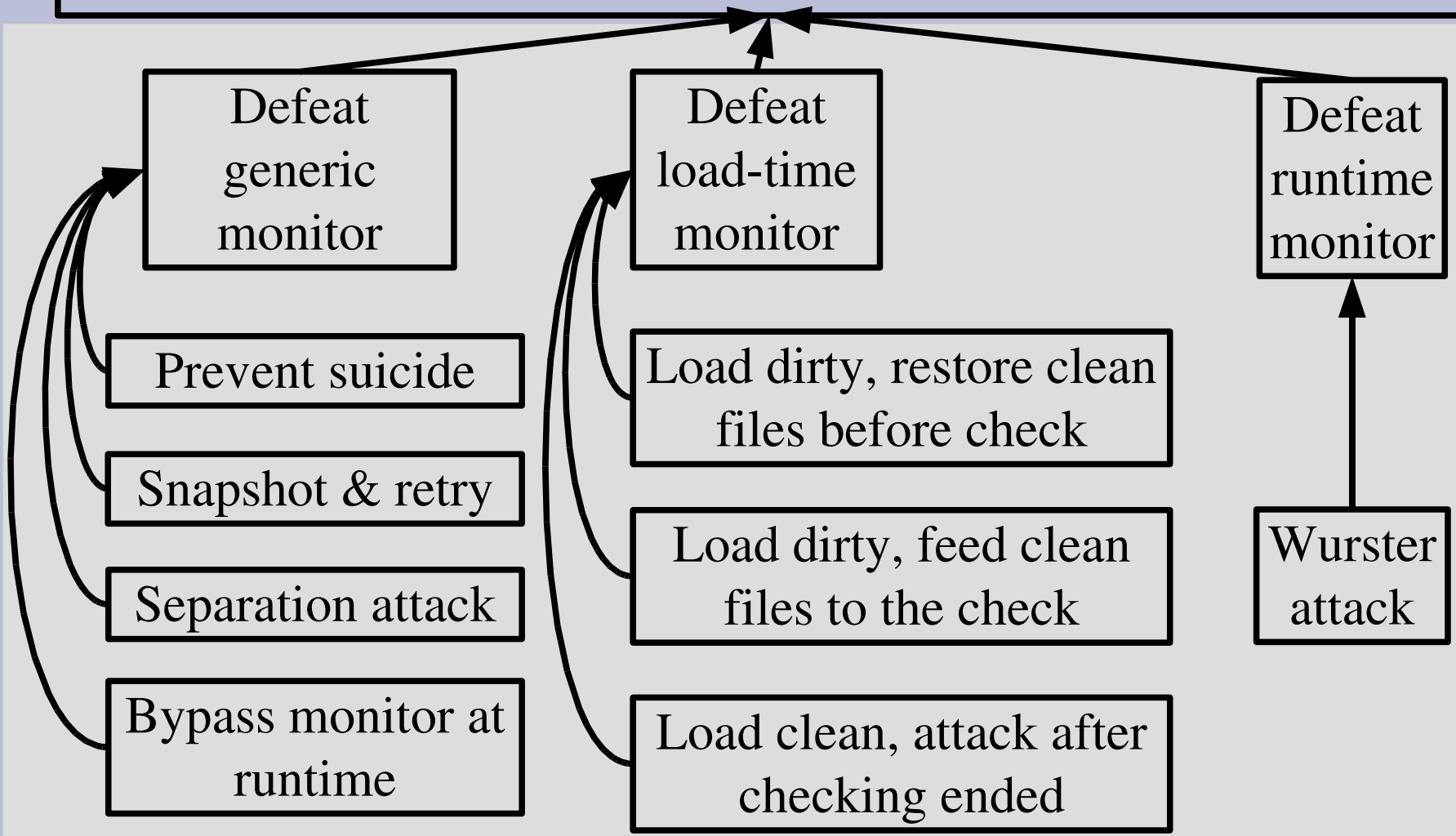
5.1 Modify Unprotected Program



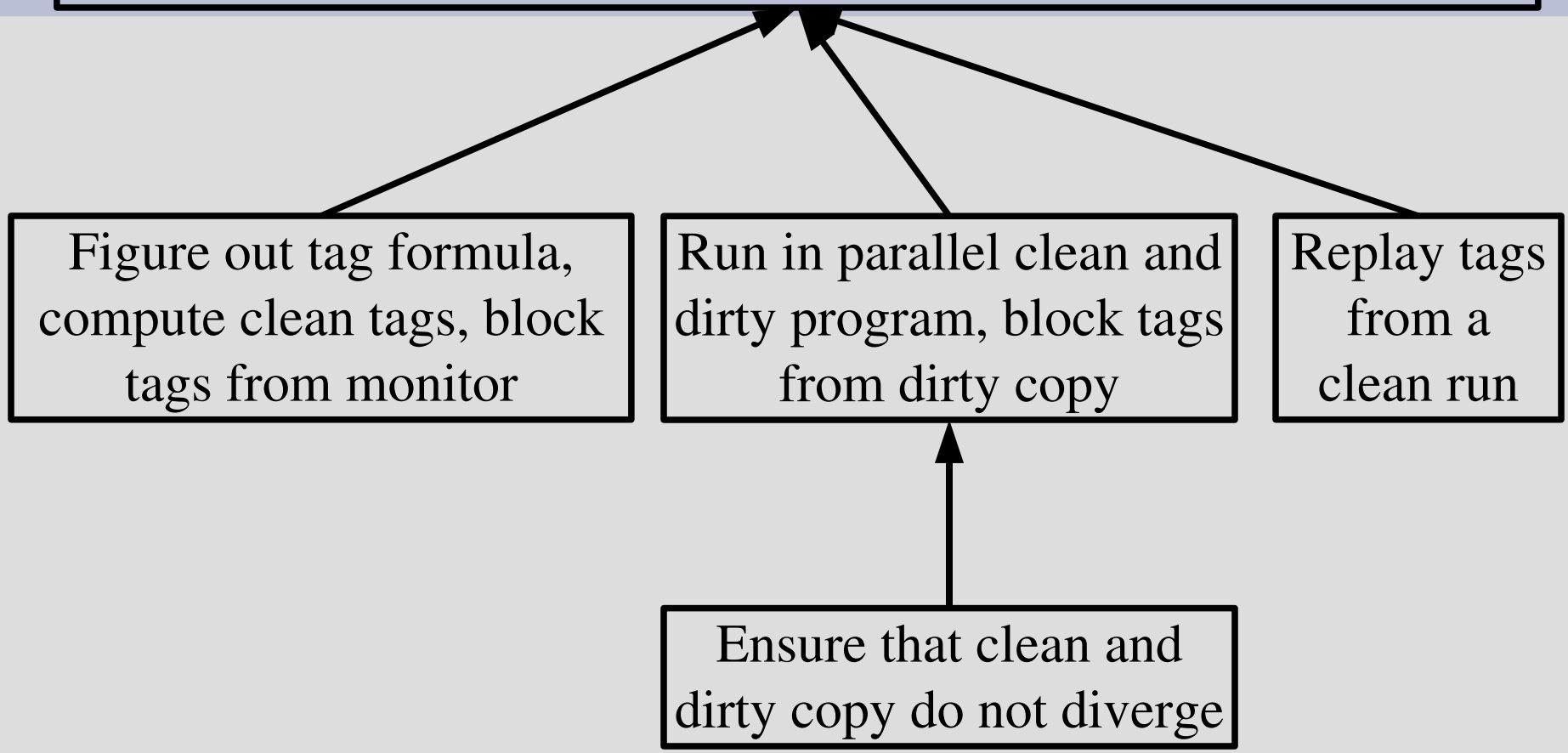
5.2 Defeat Obfuscation



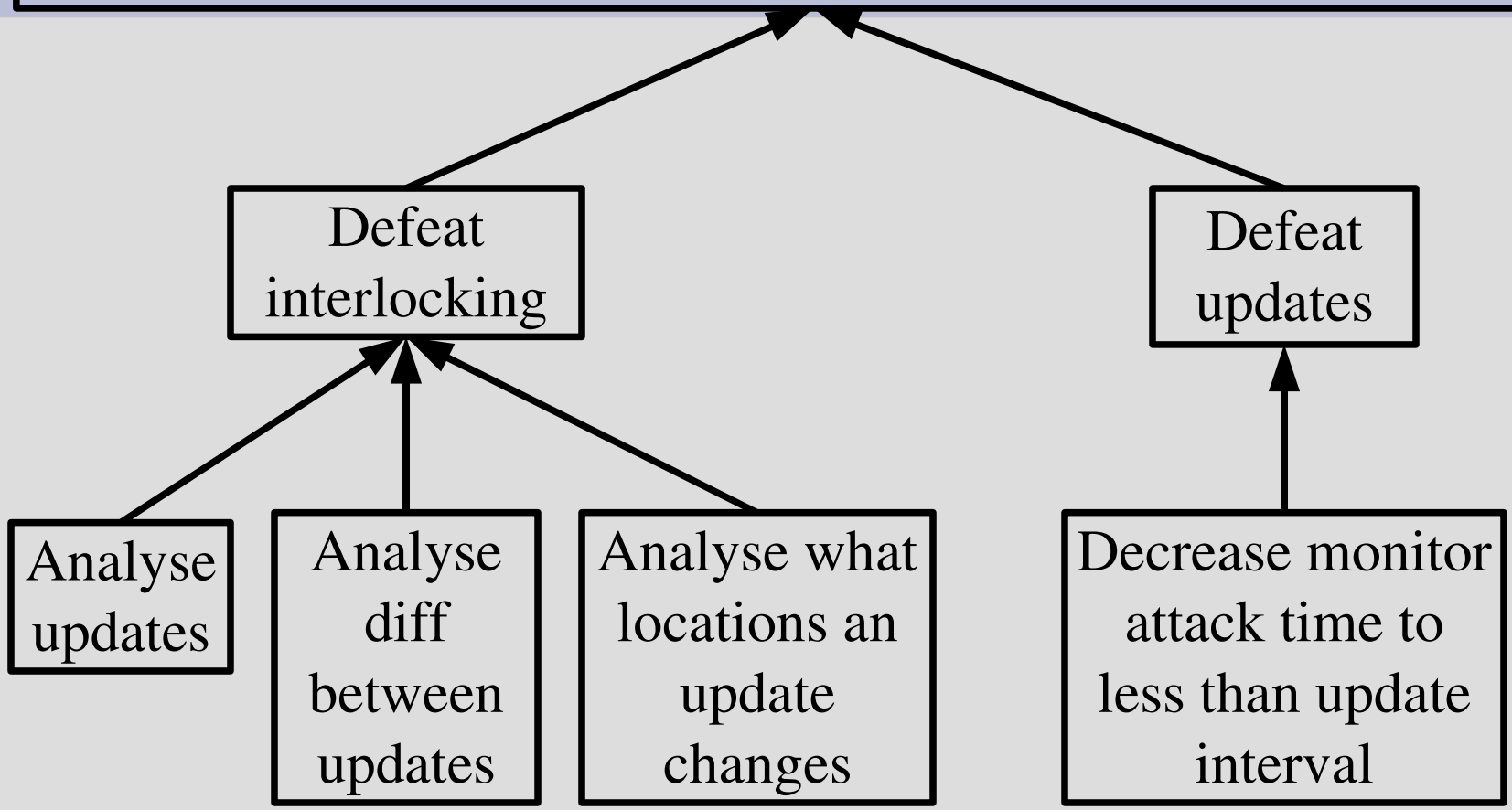
5.3 Defeat Self-checking



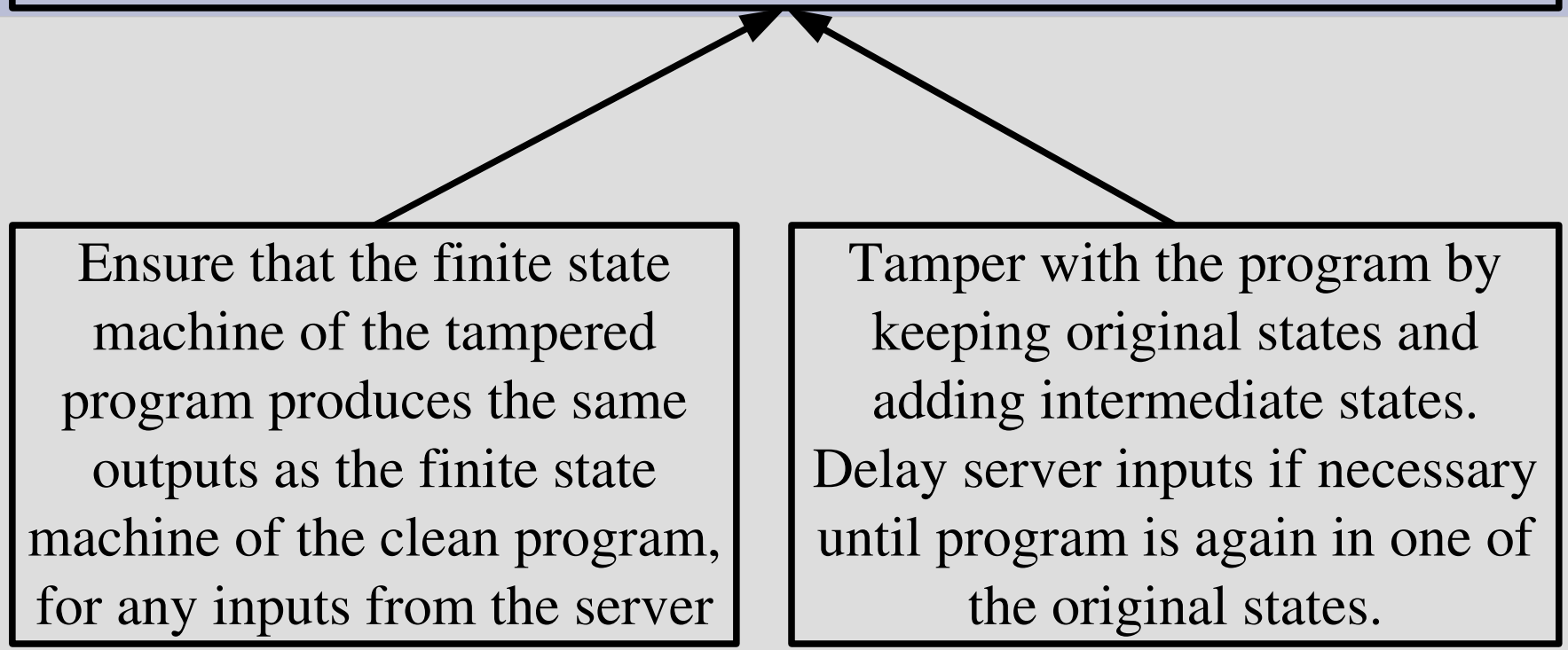
5.4 Defeat Tag Analysis



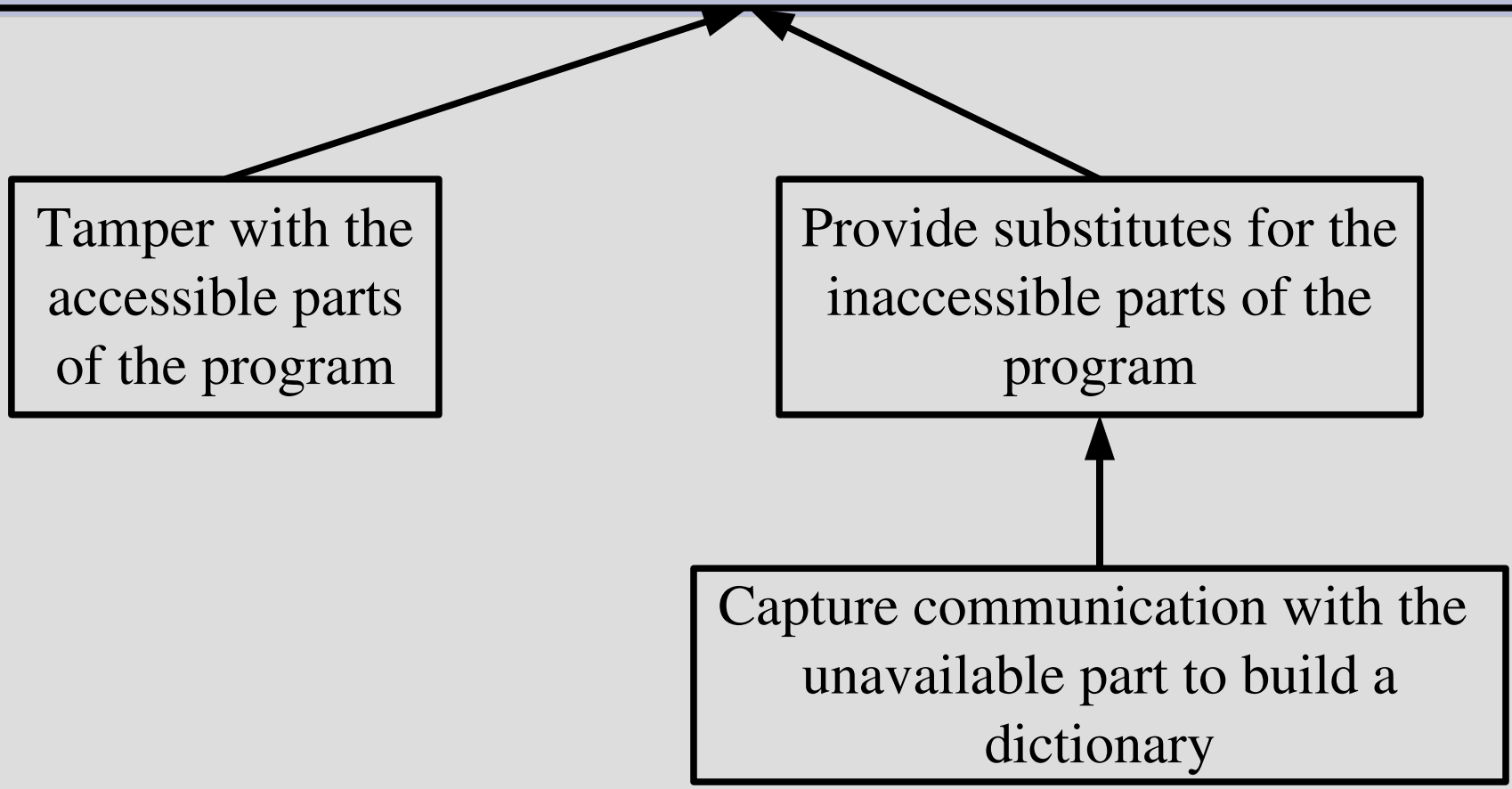
5.5 Defeat Monitor Protections



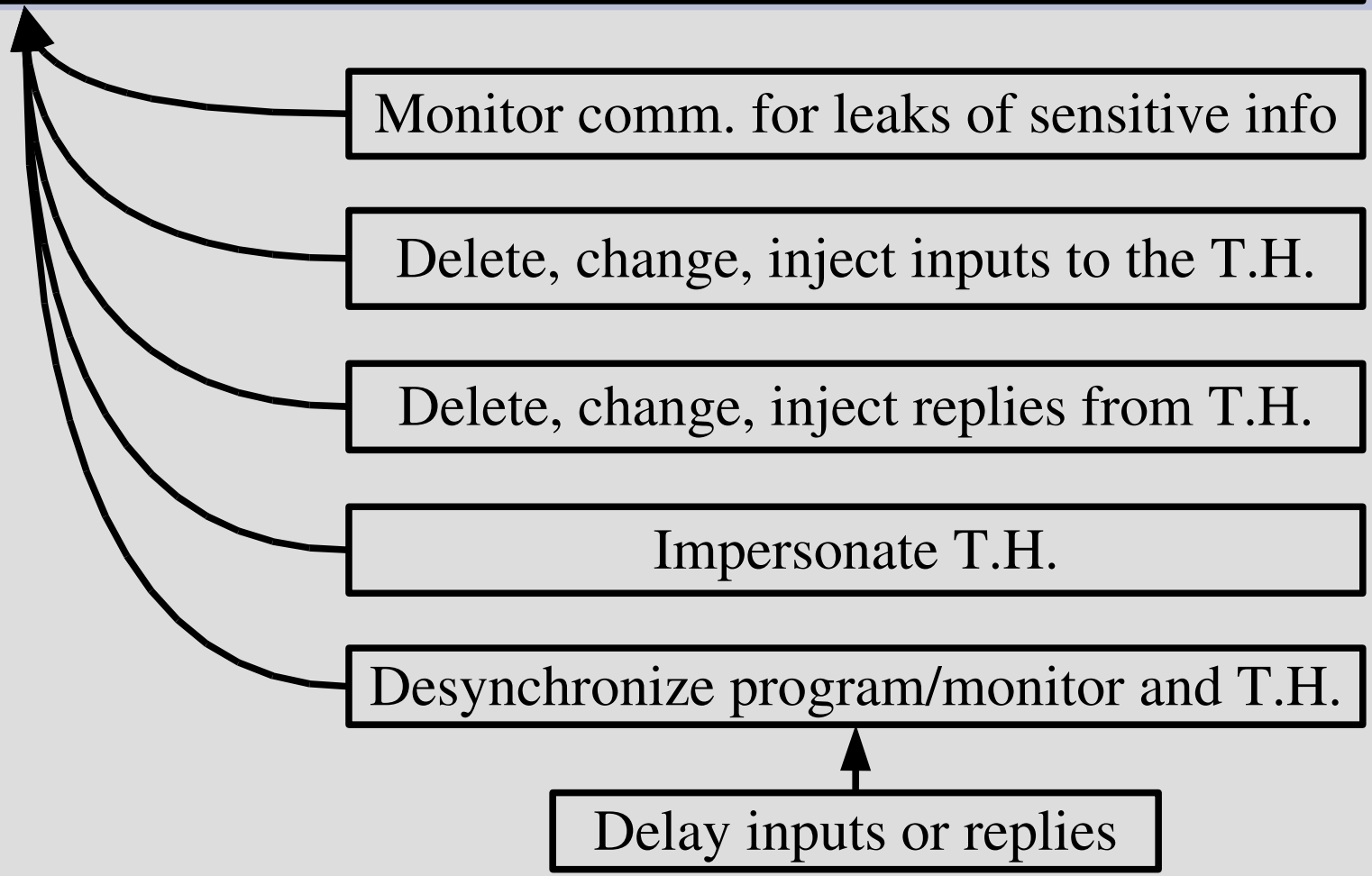
5.6 Defeat I/O Profiling



5.7 Defeat Software Splitting



5.8 Defeat Usage of Trusted Hardware



Closing remarks

- The attack model is:
  - relatively detailed about attacker means and limitations
  - less clear about the assets and about the attacker goals, they depend on the application
  - vague about the attacks, they depend on the design of the solution
- Send questions and constructive criticism to *Thomas.Herlea@esat.kuleuven.be*