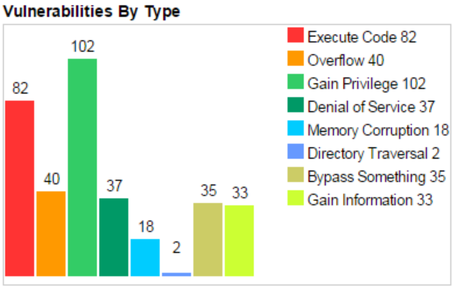
29b

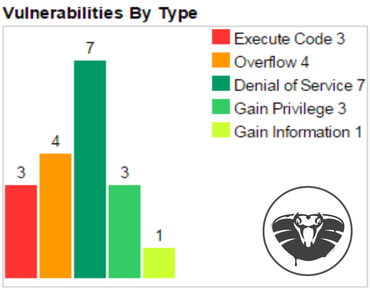
SECURE EMBEDDED SOFTWARE

MULTI-DOMAIN ATTACK

– How to protect your software/data when not all applications are trustworthy?
  – 3rd-party software modules
  – Internet-facing applications

– Existing solutions weaknesses:
  – Standard hypervisor too heavy to be fully verified
  – Verified hypervisor lacking operational features



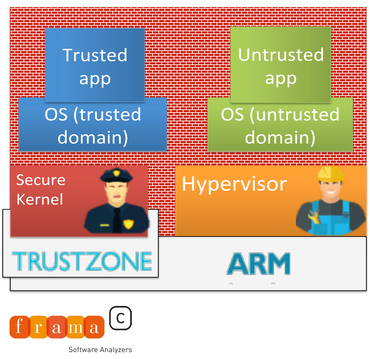


CEA SECURED HYPERVISOR

– Combines:
  – Full feature-set
  – Secure and verified kernel

– Off-the-shelf hypervisor:
  – Out of TCB
  – Cannot see hosts

– CEA's Secure Kernel:
  – Small TCB
  – Formally verifiable
  – Protected by ARM® TrustZone®



frama C
Software Analyzers

CEA TECH: YOUR PARTNER TO SECURE YOUR SOFTWARE

– Secure your software architecture against multi-domain attacks

– Integrate and deploy CEA's Secure Kernel

Contact: olivier.heron@cea.fr - www-list.cea.fr

INSTITUT CARNOT CEA LIST

université PARIS-SACLAY