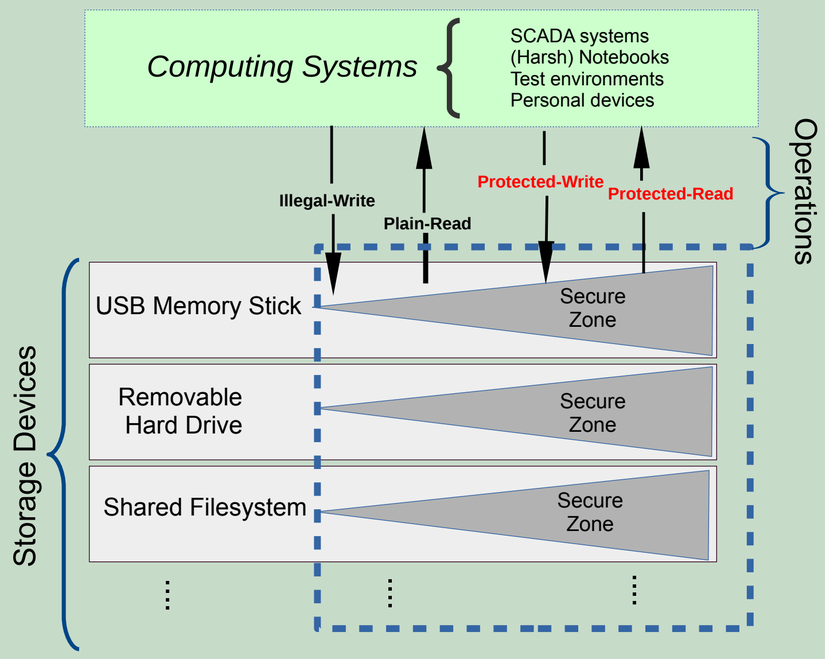
Preemptive - EC FP7 STREP- www.preemptive.eu
Preventive Methodology and Tools to Protect Utilities

Integrity of removable storage in ICSes

*A system that allows utility companies to **safely** use **untrusted** removable storage in both critical and non-critical systems*

F. Griscioli, M. Pizzonia - Roma Tre University

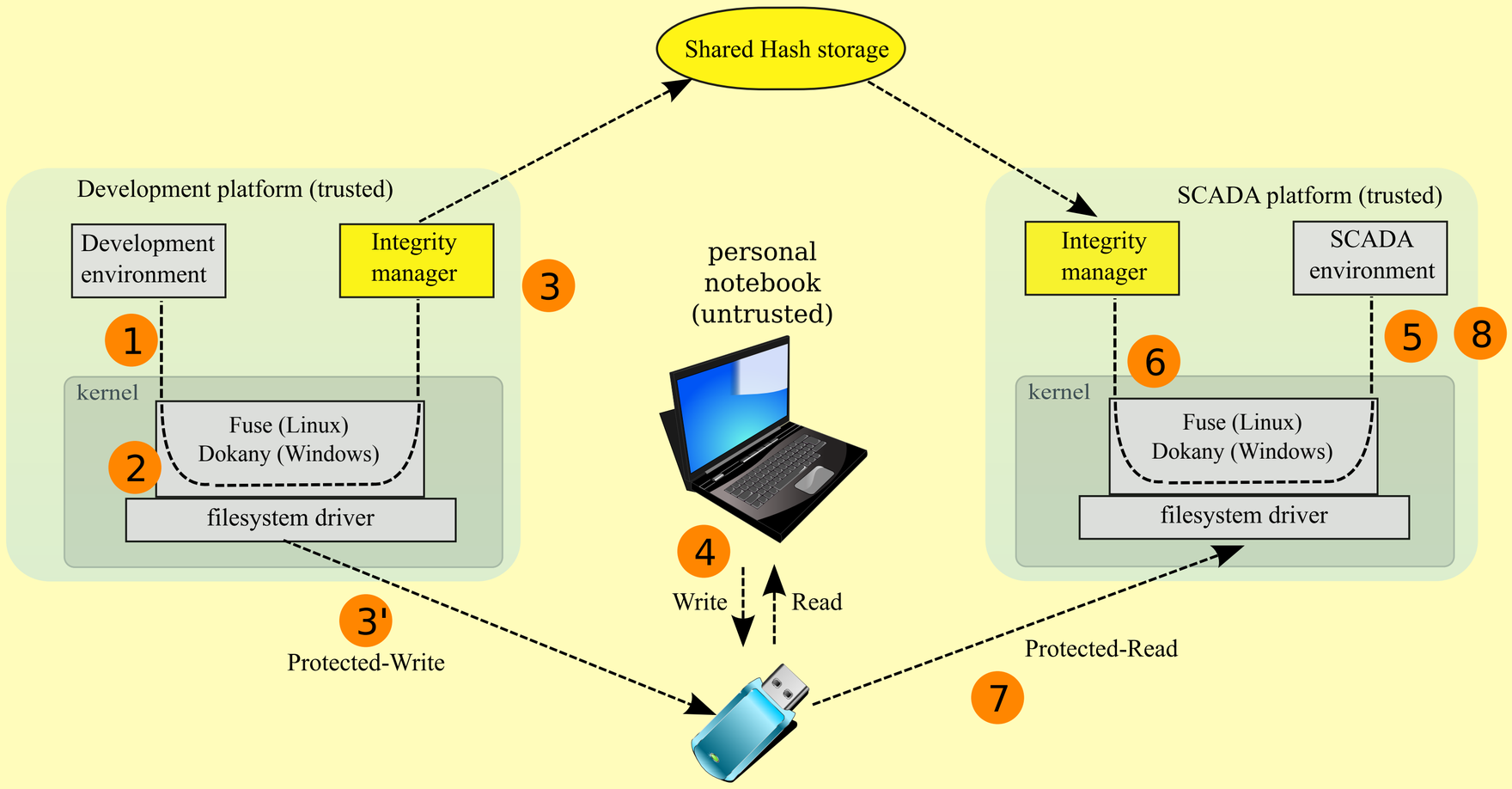
USB memory sticks are handy but it is easy to misuse them. Advanced Persistent Threats (like Stuxnet) can use memory sticks as a primary infection vector. We propose an architecture that enables to safely use memory sticks in both critical (e.g. SCADA) and regular systems (e.g. personal notebook) in a promiscuous manner. Our proposal adopts cryptographic techniques in order to protect also against zero-days threats.



Ingrendients

► **secure zone** in untrusted devices
► **integrity system (trusted)** in each critical system that reads or writes into the secure zone
► **hash** representing a snapshot of each secure zone, it changes each time content of the secure zone is changed

Integrity check of a memory stick in a promiscuous envirnoment



1. User asks to the operating system to write the secure zone on the memory stick.
2. The "write" system call is intercepted by FUSE/ Dokany module and handled by the Integrity manager.
3, 3'. The integrity manager updates both the secure zone and the shared hash of it.
4. Possibly the secure zone on the memory stick is read (legally) and written (illegally) in an untrusted environment.
5. The memory stick is used on another critical trusted system, where an application requests to read the secure zone.
6. The "read" system call is intercepted and handled by the Integrity manager which fetch the shared hash of the secure zone,
7. It also reads the data from the memory stick, and check the integrity of the data against the hash.
8. If data is genuine, they are retruned to application, otherwise an error is returned.