

# Using Tripwire to check cluster system integrity

Elio Pérez Calle  
Miguel Cárdenas Montes  
Francisco Javier Rodríguez Calonge

CIEMAT  
Madrid, Spain

Computing in High Energy Physics  
Interlaken, Switzerland, 2004

- **Increased security** needed for large computing clusters:
  - Perimeter Security.
  - Intrusion Detection Systems (IDSs).
- The target of an IDS is **early detection of an intrusion** to minimize damages.
- Tripwire is one of the most powerful IDSs.
- Tripwire is oriented to monitor the status of files and directories to detect any changes: **Integrity checking.**

# How it works

- A **snapshot** of the system is taken, including information for any file or directory that should be protected (operating system files, core scientific software. . .)
- This information is stored in a **crypted database** to avoid any unauthorized modification. This database is kept and it is used for reference.
- **System checks** are performed regularly. Present situation is compared with the reference one. A **report** is generated for each check. Reports may be stored or sent by email automatically.

- **Policy and configuration files** define Tripwire's behaviour.
  - Configuration file covers general options.
  - Policy file defines monitoring for each kind of file, depending of its characteristics and importance in system overall security.
- A **original crypted database**. The information is protected before being stored. That is a key feature of Tripwire that guarantees its own security and integrity.
- **Reports** generated by comparing the original database with the present status of the system. Reports include a general summary and a detailed list of any detected modifications.

# Tripwire at CIEMAT: Policy and Configuration

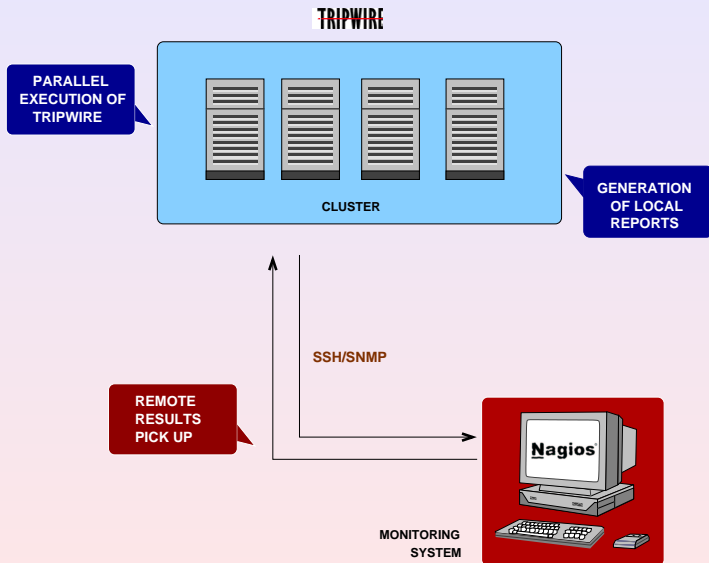
## MAIN FILESYSTEM MONITORED PROPERTIES

FILE ADDITION, DELETION AND MODIFICATION  
FILE PERMISSIONS, PROPERTIES AND OWNER  
FILE TYPE, SIZE AND BLOCKS ALLOCATED  
INODE NUMBER, NUMBER OF LINKS AND  
INODE GENERATION NUMBER  
ACCESS CONTROL LISTS (ACLs)  
TIMESTAMPS OF FILES AND INODES  
HASH CHECKING

## MONITORING MODELS DEFINED IN POLICY FILE

OPERATING SYSTEM CRITICAL FILES  
FILES WITH SUID AND SGID BIT ON  
OPERATING SYSTEM CORE BINARIES  
CONFIGURATION FILES OF IMPORTANT APPLICATIONS  
GROWING FILES (SUCH AS SYSTEM LOGS)  
INVARIANT DIRECTORIES

# Tripwire at CIEMAT: Implementation (I)



# Tripwire at CIEMAT: Implementation (II)

- **Large-scale** and **parallel** execution of Tripwire at any computer in a network.
- Monitoration is implemented in a **central computer**:
  - Throws parallel executions of Tripwire in the cluster by SSH.
  - Gets information from the MIB tree of the cluster by SNMP.
- Use of a **monitoring system** (Nagios) as a **visual interface** for intrusion detection. Features:
  - Offers information about remote executions.
  - Sends alerts by email if a problem is detected.

# Tripwire at CIEMAT: Implementation (III)

- Implementation **prototypes** on **LCG2 clusters** at CIEMAT (35 machines monitored) and other collaborating institutes: UB (6 machines) and UAM (37 machines).
- Implementation in other computing clusters related to local scientific projects at CIEMAT.
- Wide clusters **get global protection**:
  - Cluster system integrity checking.
  - Large-scale centralized execution.
  - Remote control of execution results.
  - Administration interface using Nagios.



- Combining **Tripwire** and **Nagios** provides:
  - A very secure and versatile IDS tool.
  - Complete monitoring of system integrity.
  - Adaptable to the needs of a large cluster.
  - User friendly visualization and configuration interface.
  - Remote control using alarms.
  - Free software (GPL).
- Main **references**
  - Tripwire project: <http://www.tripwire.org>
  - Nagios monitoring system: <http://www.nagios.org>