

## Monitoring accountability policies with AccMon framework

Walid Benghabrit, Hervé Grall, Jean-Claude Royer

► **To cite this version:**

Walid Benghabrit, Hervé Grall, Jean-Claude Royer. Monitoring accountability policies with AccMon framework. GDR-GPL, Jun 2016, Besançon, France. hal-01332040

**HAL Id: hal-01332040**

**<https://hal.inria.fr/hal-01332040>**

Submitted on 15 Jun 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.





**WALID BENGHABRIT**

**IDENTITY**

DIRECTOR: PR. JEAN-CLAUDE ROYER  
SUPERVISOR: A/PROF. HERVE GRALL

<first name>.<last name>@mines-nantes.fr

# Monitoring accountability policies with AccMon framework

**SPECIALITY** Computer Science  
**LABORATORY** Inria, LINA  
**TEAM** ASCOLA Research Group  
**LOCATION** Mines Nantes - France

**context~\$**

- Interconnected systems with many different technologies which implies many security breaches.
- Your personal information are already on the cloud!

**problematic~\$**

How to ensure that the privacy policy is respected?

Distribution makes systems harder to monitor

There is NO perfect security

**approach~\$**

- Accountability: Beyond security to preserve privacy
- Monitoring: Flexible and extensible framework
- Distributed temporal logic: Formal verification over distributed system



- monitoring frame**
- (1) We define what, when and how we log.
  - (2) We write the property to monitor in FODTL<sub>3</sub>\*.
  - (3) We watch the running system.
  - (4) We audit the system when violations occurs.
  - (5) We decide if the violation is legit or not and we trigger the remediation monitor if any.

**work (AccMon)~\$**

$\psi ::= \text{true} \mid \text{false} \mid \neg\psi \mid \psi \vee \psi \mid \psi \wedge \psi \mid \phi$  (propositional)  
 $\mid \exists x.\psi \mid \forall x.\psi$  (first order)  
 $\mid X\psi \mid \psi U \psi \mid \psi R \psi \mid G\psi \mid F\psi$  (temporal)  
 $\mid @ p \psi$  (distribution)  
 $\phi ::= P t *$  (predicates)

Monitoring technic: Progression (Formula rewriting)

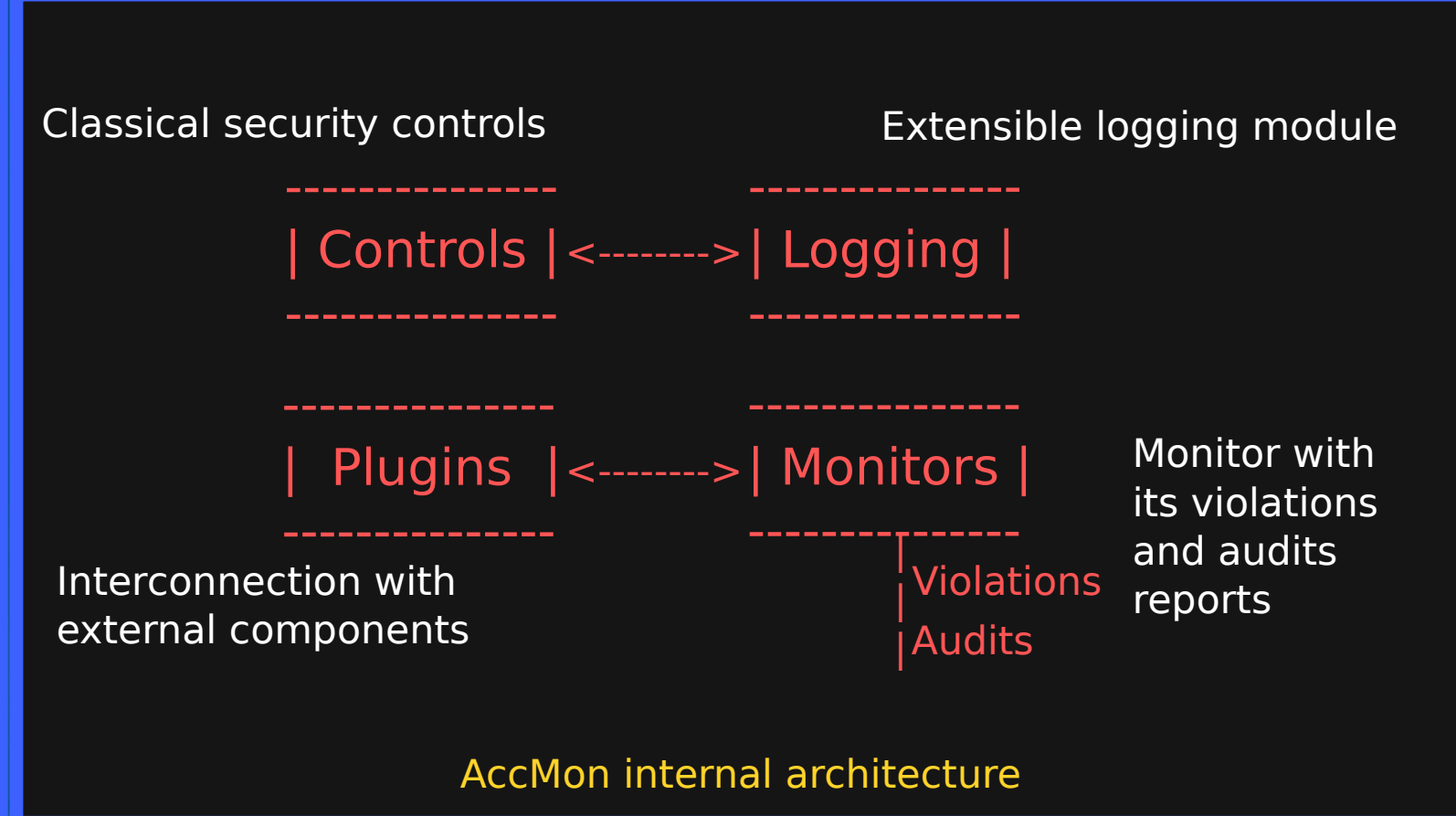
$\text{eval}(\psi) = \text{True} \mid \text{False} \mid \text{Unknown}$

\* Three-valued First Order Distributed Linear Temporal Logic

`root@root:~$ man AccMon`

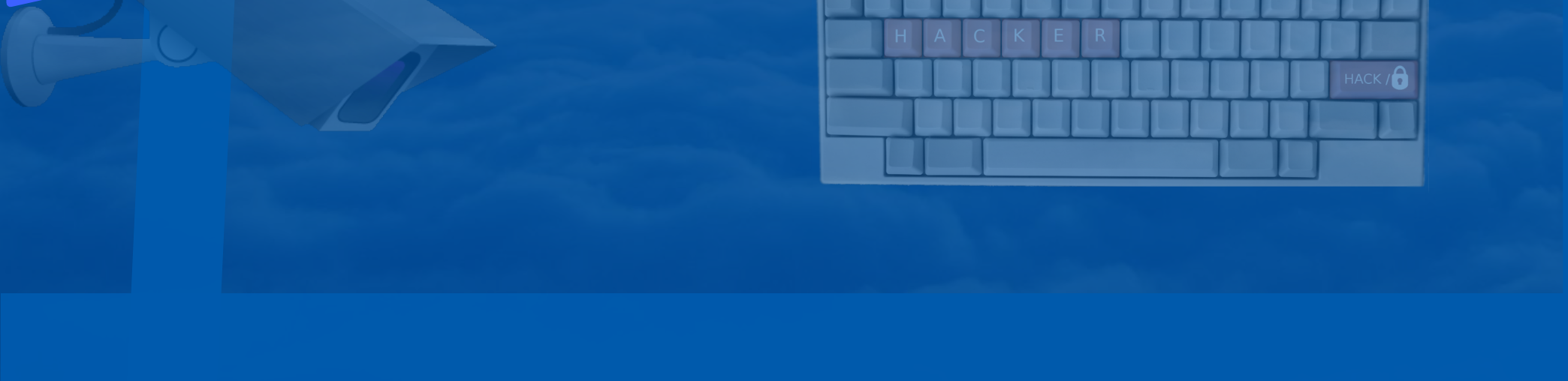
- Centralized / Distributed monitoring
- Posteriori / Realtime control
- Extensible framework

Manual page AccMon (END) (press h for help or q to quit)



**future~\$**

- Automated audit/remediation (Deep learning. Ethical problem? Computers tacking human decisions...)
- Usability (Improve logical formula writing to non specialists)
- Monitoring: protect privacy by violating your privacy? (Nothing is good or bad, it's all about how you use it...)



00100000 00001010 01101111 01110101 01101110 01100010 01101001 01101100 01101010 01111001 00001010 01110000 011011 01101100 01101001 01100011 01101001 011001 01110011 00100000 01110111 01101001 011101 01101000 00100000 00001010 01000001 011000 01100011 01001101 01101111 01101110 0010000 01100110

$\exists x$        $\forall x:\text{Human. watch}(x)$

Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

Edward Snowden

Take the control of your data and care about your privacy, it's already too late...

<https://github.com/hkff/AccMon>  
<https://github.com/hkff/fodtlmon>  
<https://github.com/hkff/AccLab>