Monitoring accountability policies with AccMon framework

Walid Benghabrit, Hervé Grall, Jean-Claude Royer

To cite this version:


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.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License
Monitoring accountability policies with AccMon framework

problematic

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

How to ensure that the privacy policy is respected?
Distribution makes systems harder to monitor
There is NO perfect security

context

accountability

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

monitoring frame

(1) We define what, when and how we log.
(2) We write the property to monitor in FODTL*. 
(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)

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

work(AccMon)

- Automated audit/remediation
- Usability
- Monitoring: protect privacy by violating your privacy?

future

- Monitoring technic: Progression (Formula rewriting)
- Three-valued First Order Distributed Linear Temporal Logic
- Automated audit/remediation
- Usability
- Monitoring: protect privacy by violating your privacy?

root@root:~$ man AccMon

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

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/AccLab
https://github.com/hkff/fodtlmon

classical security controls

Extensible logging module

Interconnection with external components

AccMon internal architecture

Monitor with its violations and audits reports