

Why to simulate access controls?



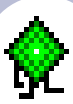
- 7 pages to discover a new concept in IT security: the simulation of access controls
- To test the concept, see the software:
<http://accessroad.sourceforge.net/home.html>

Version 1 - October 2009

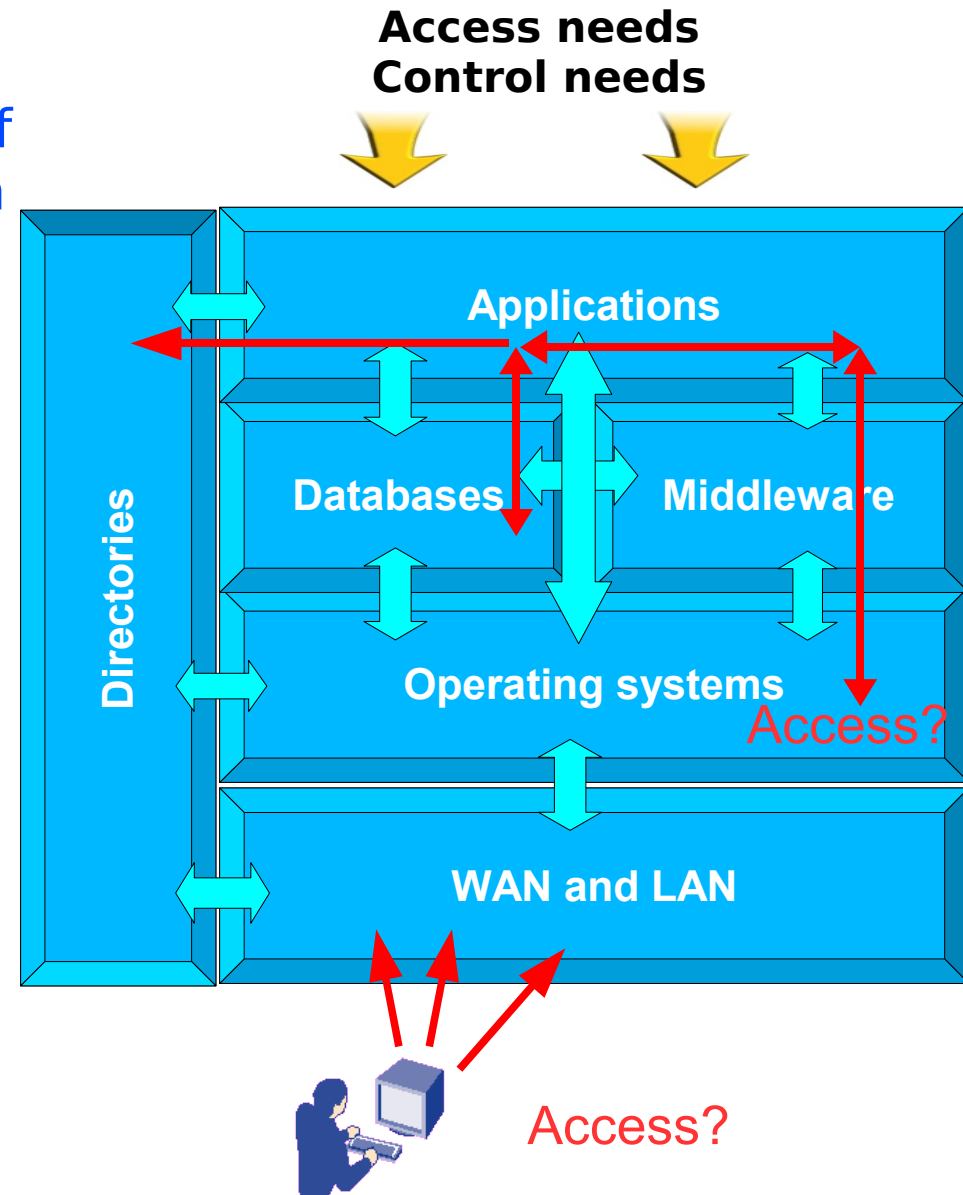
SARL ACCBEE - 35 bis Rue des Renouillères - 93200 Saint-Denis - France - EU

patrick
.thazard @ accessroad
.info

For a better handling of threats, we have to know: who/what has access to what ?



- An information system is composed of multiple layers of software running on many servers
- Access rights in these softwares are managed by numerous actors
 - responsible to the coordination (needs, security policy), or,
 - which design, manage or control the rights in the software
- **With the current means in your company, what efforts should be required to get a full reply to this question?**



Who/what has access to what ?

The current means to reply

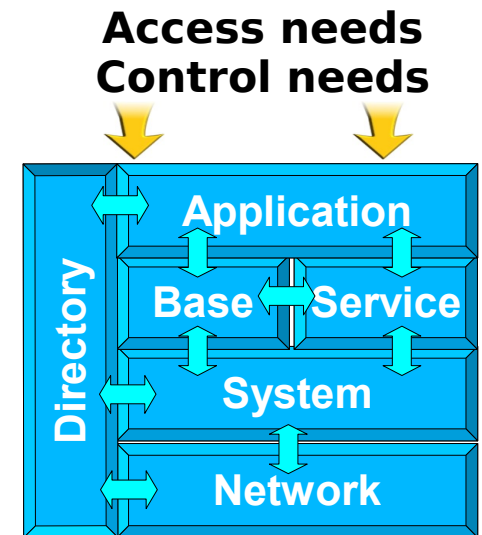


- The first need has been to operate the IT system, the user and rights administration. This was the priority during the previous ten years.
- The identity management tools allow to fully reply to “who has access to what”, but...
 - it is a static answer, without an easy study of all the options,
 - no reply to “what has access to what”, where the answer is fragmented, from varied tools
 - you have non-integrated technical replies, following the perimeter of each tool (network, directory, and so on)
- It is necessary to go further on the more sensible sub-systems

Access control simulation: what it is?



- Simulation studies **the authorized access paths**
 - in every simulated software
 - and from end to end: user ↔ data, program ↔ program, server ↔ server
- For controlling the quality of rights in the **more sensible sub-systems**
 - from the security policy
 - from the IT technical architectural framework
- For bridging the gaps between the conceptual level, the technical levels of access controls handling, and each parameter
- For building up a better communication between **all the points of view** in the company about access controls



For what: some uses of access control simulation



- Technical uses:
 - design access controls, with
 - the user or process context, the segregation of duties
 - analyze the global impact of any change in rights and components
 - control the application of the access control policy (example: from the SOX policy)
 - analyze the global impact of a no-fix security vulnerability
- Organizational uses:
 - share the same vision among the internal specialists about the access controls architecture
 - learn and recall the access control functions
 - build up a referential of patterns in access controls
 - share with partnerships a common security architecture for sensible exchange systems

The first priority: the design of sensible applications



- A sensible application may have inner access controls, or may use the services of a portail or a server.
- The design of access control needs the collaboration of varied people, from the IT team to the application administrators.
- A simulation tool may bring the following services:
 - define a common vocabulary of concepts to link the conceptual level of access control (user, role, right...) and the technical levels (depending on the implied software),
 - compare varied architectures of access controls,
 - reuse the application simulation at every step of the application life, to strengthen the access control quality and its understanding.

Access control simulation and beyond: the future is in the integration of general and very specialized tools in a global approach

