

» Avoiding the dangers of accumulated access rights «

A white paper by Duncan de Borde,
Siemens Insight Consulting



If you were to consider which people in your organisation had the most wide-ranging access rights to your IT systems, who do you think they would be? Would they be the CxOs or IT system administrators? In fact, in many organisations you will find the people with most access rights are those people who have been in the organisation the longest, and have undergone the most changes in job. These people can unwittingly have become some of the most powerful users in the organisation in terms of the range of information they have access to and the rights they have.

If insufficient controls are in place they may even have conflicting access rights, undermining the compliance and governance principles such as segregation of duties. Whilst you may trust these people, the potential for risk, or the damage an attacker could do if

they were to compromise that user's accounts, could be immense.

This paper describes how this problem can arise through traditional access right management and some measures, including the use of role-based access control, that can play a part in avoiding this situation.

Typical employee lifecycle

Joiner

When a person initially joins an organisation, they are often given a basic set of access rights that are necessary for them to do their job. This is not always a scientific process. Sometimes it may be a case of "Bob does the same job as Bill, give Bob the same access Bill has". This can give Bob all the access they need on day one, but often leads to excessive rights. Bill may have other rights that they have been inherited over the years, that they no longer need, and Bob will inherit these also. In other instances, a new starter may be given basic access and find, as they do the job, they need further access. This method avoids excessive privilege but is inefficient. A new starter may often find they don't have all the access they need to do their job, and cannot work effectively until further required access is granted, often after a significant delay.

Mover

After some time in an organisation, it is likely an employee will move onto a new role. This will most likely require new access rights to be given. Here similar considerations may apply as for a new starter, e.g. will they be given excessive rights by modelling on another user, or will they get their access inefficiently, bit by bit. Even if the need to remove access rights for the old job is considered at the time of moving, it is often the case that they need to keep their old access for a period, as they support both job roles for a handover period. If the access is not removed immediately at the time of moving, it is easy to neglect to remove this access at a later date.

As an employee makes a number of moves within an organisation, it is possible for their access rights to accumulate over each move, the end-result being an employee who has wide ranging access over a number of disparate systems, much of which is no longer required for them to do their job. The employee may not even be aware of all of the access they have.

Leaver

It has long been recognised that there is a potential security risk associated with leavers, if their access are not fully terminated when employment ceases. Not all organisations can still efficiently de-provision access for employees at the end of their employment. What is not always considered is that, in the case described above, an employee might have much wider ranging access than was realised. Thus their current access rights may be terminated, but they may have access rights in other systems that is not identified at the time of leaving and is not terminated.

Accumulation of access rights

The chart below illustrates an example of how an employees access rights can accumulate during the employee lifecycle.

As an employee starts work on each job, they obtain all the access they need to perform that job. On each job change, some of the access rights for the previous job are removed, but some remain. Access rights for prior jobs are likely to be maintained indefinitely. Each time a change of job occurs, the employee has accumulated further access. At the time of leaving, all access rights for the current job may be terminated, but whilst some access rights from previous jobs may also be terminated (e.g. by virtue of disabling known accounts), access rights on other systems may remain even when employment has terminated.

How role-based access control can help solve the problem

As with any problem, more than one solution may be appropriate depending on the particular requirements of the business. One method particularly suited to resolving these issues is to use role-based access control (RBAC), or role-based provisioning.

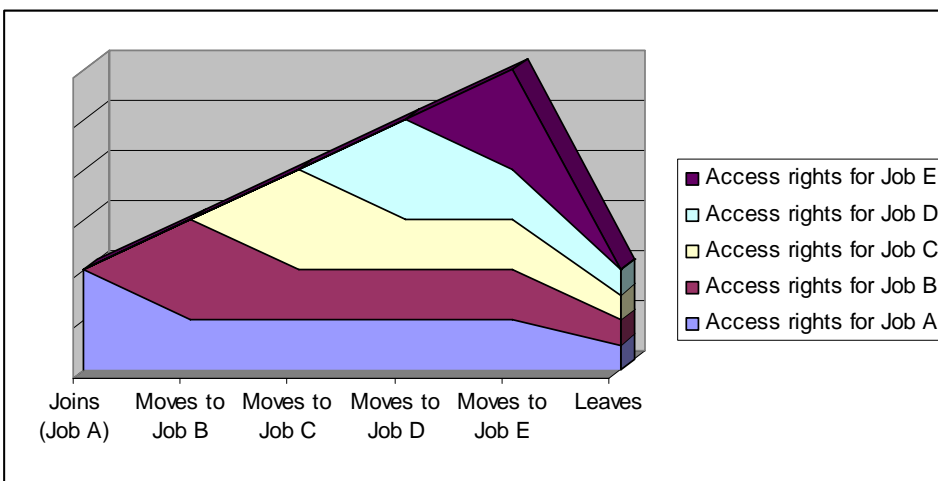
In RBAC, rather than defining individually what access each person requires, you define the access required to perform a particular role (or job function), and then allocate people to their required role(s). This has a number of advantages:

- Once the roles and their required access rights have been defined, it is much simpler to allocate a person to a limited number of roles, than to allocate a number of disparate access rights
- As all the access rights required for a role can be allocated to a person in one go when they start a new job, that person can be sure to have all the rights they need to do their job from day one
- It is much easier to audit what access users have, as there are a smaller number of role assignments, and these will typically be more meaningful at the business-level than individual access rights
- When an employee leaves a job, you can ensure by removing their role assignments that all their access required by the old job is removed.

The use of roles also permits greater discipline to be introduced into the allocation of access rights. Roles can be suitably designed (getting away from "give Bob the same access Bill has") to give the correct access required for the role, i.e. all the access required to do the job, but no excessive privileges that could pose any risk (the "minimum privilege" principle). These role definitions can also be maintained and reviewed on an ongoing basis to ensure they continue to fulfil the needs of the business. Any changes in role definitions would automatically be reflected in user access rights.

Managing role allocations

Role-based access control on its own is not a panacea for the above problems. Any role-based access control system needs to be supported by appropriate business procedures. If role allocations are handed out with no more control than individual access rights have in the past, they will not achieve significant benefit.



Avoiding the dangers of accumulated access rights

As roles can encompass more than an individual access right, they should only be allocated when the requirement for a person to have that role is confirmed. Two common approaches to role allocation are:

- Rule-based allocation, e.g. automated role allocation (and de-allocation) based on some property of the user, such as their location, department or job title, according to business policy
- Approval based allocation, where some approval mechanism e.g. via a line manager, is required before a role can be allocated. In this case one tool may encompass the approval process and role allocation, or roles can be allocated by administrators after a separate approval process.

Both approaches can help reduce the issue of accumulating access rights. Rule-based allocation as well as automatically giving roles, can also be used to automate the removal of roles when the business rule is no longer satisfied. On a job change, approval based allocation can be used, not just to request roles for the new job, but to request removal of old roles, possibly identifying an end-date for their removal, thus allowing the old roles to be maintained on a short term basis, e.g. for a temporary job handover.

Approval can also be extended to re-approval, i.e. to ensure that, where a role has been allocated to an employee, the need for that person to keep that role definition is re-confirmed on a regular basis (also called attestation).

To achieve the above some tool is required to implement the role-based access control. This will need to have a view of all of the systems to which people will need access and the access rights within them. It must also be able to provision these access rights dynamically as role assignments and role definitions change. This will often required the use of an Identity Management system with suitable role management functionality.

Summary

Employees having excessive access rights can pose a risk for any organisation. Often such excessive rights can be associated with people who have undergone a number of job changes. The use of role-based access control is one method that can greatly reduce this exposure to risk. In addressing this risk, some of the key-points identified below may need to be considered:

- Management of access rights based on roles rather than individual privileges can both reduce the risk and make the process more efficient
- Role definitions should be appropriately designed, reviewed and maintained
- The use of an identity management system is often required to allow roles to be centrally managed and applied across diverse systems
- Roles may be assigned through business rules or an approval process
- Procedures for job moves should also consider de-provisioning of old access rights, possibly after an identified future date
- Role assignments may have requirements for re-approval
- A role-aware identity management tool can provide the central point of control for role definition, provisioning of access rights, definition of policy, automation of processes and audit.



Authors biography

Duncan de Borde is a Consultant at Siemens Insight Consulting. Duncan has a first class honours Bachelors degree in Physics and Electronic Engineering as well as a Masters degree in Computing for Commerce and Industry.

Duncan has specialised in Identity and Access Management since 2000 and has been involved in a number of successful implementations, including a global identity management system for a major pharmaceutical company. Duncan also has wider experience within the information security sector having previously worked on Smart Card security and Public Key Infrastructure. He also has extensive development experience.

Duncan's particular skills are in the delivery of solutions that meet the requirements of businesses, recognising how technical and procedural solutions can be best applied to resolve business problems to manage risk or deliver value.

Insight Consulting is the specialist Security, Continuity and Compliance unit of Siemens Enterprise Communications Limited and offers a complete, end-to-end portfolio encompassing:

- Security
- Compliance
- Continuity
- Identity Management
- Managed Services
- Training

Siemens Insight Consulting subscribes to the CESH Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against ISO 27001 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight