Human Processes

Keith Harrison-Broninski
CTO Role Modellers (www.rolemodellers.com)

khb@rolemodellers.com

How Processes Can Secure The Other End

In my November 2012 Column, I discussed the current fast pace of innovation in Identity Management (IM), and argued that new IM technologies still provide little support for securing the primary occupation of most knowledge workers - collaboration with colleagues, especially those in other organizations. If an organization is going to grant access to business-critical resources, it needs to know *why* access is needed and *what will be done* with those resources.

In other words, you need to understand the work item that has caused the person to request access – and this means understanding the business process context in which access is being granted:

- The Activities the person is carrying out;
- The Roles they have been assigned, to which the Activities belong;
- The Plans (projects, programs, processes, initiatives, ventures, …) to which the Roles belong.

First I will summarize the main argument of my November column. Then I will discuss a related challenge. Increasingly, business systems are used to send messages, by email and other means, often containing sensitive content. The sender may be known, but what about the recipients? There are process management techniques that can streamline and improve collaborative work across multiple organizations in a way that automatically authenticates, authorizes and audits not only the sender but also the **recipients** of any message.

Role-Based Access Control

For purposes of authorization, the key element of identity is the Role. In a workplace context, someone generally requests access to a resource not because of who they are (Alice Smith) but rather because they have been asked to play a Role in some kind of work programme (Quality Assurance in Social Care Transformation Programme 2013) and hence to need to do a specific Activity (Review Workforce Training Needs). It is only on being assigned to the QA Role that Alice needs to review the documents – and if she is re-assigned, goes on leave, or is too busy, someone else will do it in her place.

Role-Based Access Control (RBAC) tells us how to think clearly about confidentiality. An enterprise infrastructure without an RBAC layer based is shown in **Figure 1**:

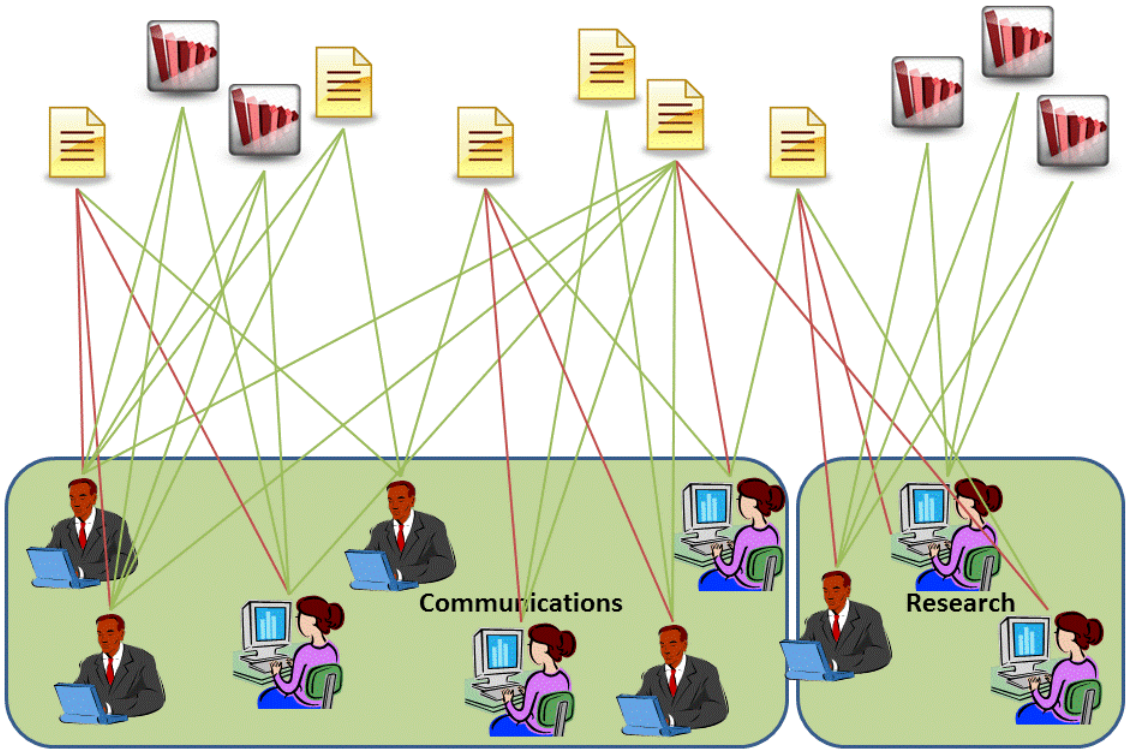

Figure 1: Identity "Management" without RBAC

This picture is not understandable. Without some means of seeing *why* people need access to resources, and *what they are doing* with those resources, the situation is next to impossible to manage or audit. By contrast, **Figure 2** shows how the picture simplifies if you introduce Roles as an intermediate layer to facilitate authorization and accounting:

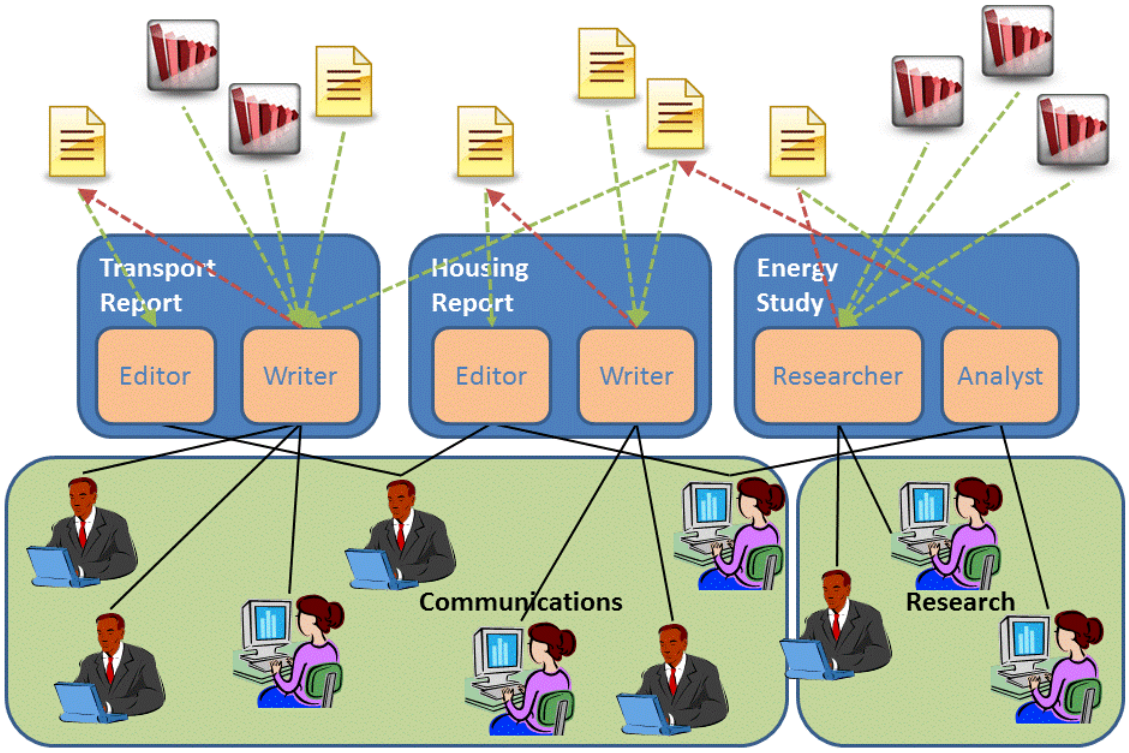

Figure 2: Identity Management with RBAC

The blue boxes in the above diagram are Plans (representing projects, programmes, processes, initiatives, ventures, …) in which people play Roles to deliver work streams as part of a **Virtual Team**. A Virtual Team is a group of people who work together only to carry out a specific Plan – they don't necessarily sit together and often work for different organizations. Once access control is guided by Role assignment in Virtual Team Plans, not only is it possible to understand what is going on, but to manage it. For instance, authorization can be shared and delegated through re-assignment of Roles as necessary. So not only does RBAC permit more powerful and practical securing of access to information, but also transfer of that access – which is a normal, fundamental part of the way that people work.

Securing Email and Instant Messaging

A further aspect of RBAC that is fundamental to the modern workplace is management of communications.

Most workplace messages are sent via email, with instant messaging increasingly an alternative option. Even if encryption is used for messaging, the volume of messages sent daily in most organizations makes it almost impossible to gain retrospective understanding of why people sent things to each other – a clear security risk, since it prevents meaningful audit.

However, once Roles are introduced to the security picture, it becomes possible to manage data sharing, even by email. This is because Roles exchange information via purposeful communication channels. If a Virtual Team Planning tool is used to manage workplace collaboration, messages are not emailed by Alice to Bob and Charlie, but sent by the QA **Role** that Alice plays to all colleagues in the relevant **Stage** (work stream) of a **Plan**.

Further, a Virtual Team Planning tool unifies email and instant messaging – the user gains the ease of use and immediacy of instant messaging, but under the hood, all messages are transferred by email, and can be read using any normal email client. This enables encryption, ensures that all messages are automatically recorded for auditing in a context that is simple to understand, and makes it possible for people to choose how to send/receive messages – they can use email as usual, or the Web-based planning tool, just as they prefer.

In effect, the use of RBAC via Virtual Team Plans enables organizations to "secure the other end" – to manage the flow of information, not just internally but to and from partner organizations with who staff are collaborating. RBAC, implemented in this way, means that security does not stop with the message sender – it also applies to message recipients, automatically.

Conclusion

Virtual Team Plans allow provision of access to people from multiple organizations to be managed without need for complex cross-boundary approval procedures. The organizational affiliation of each Role player becomes secondary to their assigned Role in a Plan of action that has already been agreed by all parties concerned. Organizations that implement IM in combination with Virtual Team Planning will be able to share business information with partners safely and manageably.

In particular, RBAC makes sharing of business information *conscious*, not accidental, and *tracked*, not invisible. The first step in managing business communications is to understand them, which means putting them in process context. For long-term, collaborative work that spans

multiple organizations, such processes can only be handled by treating them as Virtual Team Plans.

Author

Keith has been regarded as an IT and business thought leader since publication of his 2005 book "Human Interactions: The Heart And Soul Of Business Process Management". Building on 20 years of research and insights from varied disciplines, his theory provides a new way to describe and support collaborative human work. Keith speaks regularly in keynotes to business, IT and academic audiences at national conferences, most recently in Poland, India, the Netherlands, the UK, Finland and Portugal.

Keith Harrison-Broninski is CTO of Role Modellers, a Gartner BPM Cool Vendor 2012. The company's product, **HumanEdj**, is cloud software for Virtual Team Planning that provides unique support for large-scale, complex collaboration across multiple organizations.

More information about HumanEdj is available at www.rolemodellers.com and about Keith at http://keith.harrison-broninski.info.

We created a BPTrends Discussion Group on Linkedin to allow our members, readers and friends to freely exchange ideas on a wide variety of BPM related topics. We encourage you to initiate a new discussion on this publication, or on other BPM related topics of interest to you, or to contribute to existing discussions. Go to Linkedin and join the BPTrends Discussion Group.