Understanding Security Administrators

Granting Access in Academic, Start-up, and Enterprise Environments

Luke Kowalski
Corporate UX Architect, Oracle Corp.
500 Oracle Parkway, 2op1030
Redwood Shores, CA 94065
luke.kowalski@oracle.com

1. INTRODUCTION

Who administers security and grants access to applications? Are these individuals dedicated security administrators, or are they DBAs, functional admins, or general IT group professionals? How do the roles differ based on size and nature of the business? What are the differences and commonalities in academic, start-up, and enterprise environments? Are some security models better suited for a particular environment? **Is the consumerization of IT [1] affecting security?** Are concepts from social networks and mash-ups permeating the enterprise and already causing security headaches? Will we see increased deployment of reputation-based access models blended in with traditional role-based accesses control? These and other questions will be answered by a comprehensive study of administrators dealing with access control. Ethnography, interviews, and surveys will be used to shed more light on how security administrators work, the tools they use, and policies they live by.

2. SECURITY ADMINISTRATOR – CREATING A PERSONA

An earlier study of administrators [2] identified several types of administrators in an enterprise application deployment. While this study focused on medium to large size businesses (more than 100 employees) the results identified numerous specializations. System administrators focused on hardware, firewalls, and global help desk tasks. Database administrators had their hands full with database and security. Application or functional administrators maintained, configured, patched, and tuned the business flows of enterprise applications like human resources, procurement, or manufacturing. Managing security, at least outside of the government and military complex did not emerge as a dedicated role. Corporations do employ chief security officers, and vice presidents of global information security, but who really manages the operational side of security? If a new employee comes on board, or happens to be terminated a typical process involves a large number of people in human resources, real estate, IT account provisioning, and other areas. But who is really in charge, feeds information back to the policy side of the business, owns escalations, and who serves as the point person for access security? What limitations do the encounter and how could we help them?

The study hopes to identify the titles security administrators hold, unique roles, type of experience they posses, and focus on differences and commonalities between academic, start-up, and enterprise environments. A user persona will be developed for each, bringing forth a better understanding of security challenges, best practices, and skill sets required of administrators.

Figure 1. Typical HR application administrator work environment. Post-Its instead of retina scanners.

3. GRANTING ACCESS

Most of the research in security is focused on end users. Passwords, phishing, trust, and privacy are some of the most often covered topics. Focus in the press is also most often on: “How did the end user breach security?” Even IT departments look to and blame the end user when it comes to security breaches. But the reality is more complex. Bad design, uninformed policies, inflexible systems, and confusing security-related user interfaces are often the underlying reasons for security breaches. For example, Global IT departments often dictate guidelines for strong passwords. Some rules are so complicated and require password changes so often, thus causing the end users to record passwords in plain text on their mobile devices, or in plain sight on post-its. In other cases single sign-on systems are so prevalent that users assume that everything from a given vendor is SSO-integrated. This creates a situation where end users share that one SSO password with a non-SSO application, simply through the brand association.

Motivators that drive security in the consumer realm are slowly emerging as economic, partly based on the pioneering work of Ross Anderson [3]. But what happens in the enterprise? What confluence of policy, end user, operational tools, or other factors contributes to security violations? Amanda Andress begins to identify the best practice of integrating the people, process, and technology [4], but how does it all come together for the security administrator? How do they fit into the end user, administrator and policy triangle? Did the user not change the password

because the system administrator never hardened the applications, or the vendor shipped it misconfigured? Is a flawed corporate security policy tying the adminstrators' hands, and better dialogue is needed between operational and policy sides of the house? Are the designed-in or architectural limitations of the identity management software preventing good practice? Are customizations so complex that the forest is lost for the trees? **Using the user-centered inquiry process, what can we learn from the administrators granting access to applications, and how can this inform the rest of the security ecosystem?**

3.1 Role Based Acess Control and the New Way -Consumerization of Security?

Access control in enterprise applications is overly complex. Customers and consultants complain about this at Oracle and at other Silicon Valley companies. Extensive training, certifications and experience are necessary to understand the architectural models and the terminology. Grants, menus, permissions, roles, and other terms in fine-grained security are often used interchangeably in different identity management products and administrative tools. Large corporations with outposts across the globe need to support thousands of unique roles, with unique access controls for individual menu items and data objects in business flows. Standards, like the latest XML-based security effort are helping to streamline the concepts and the vocabulary, but the complexity is still daunting and expensive to implement.

Consumer portal security and access models can be simpler, but they, too are evolving, and affecting the enterprise. Concepts from that realm, like Web 2.0 mash-ups with content from disparate sources are creating new challenges around applications access and security in the enterprise. The old RBAC models, even when adopted do deal with web service interfaces are now getting stretched to deal with this dynamic content aggregation model. Social networks also play a role and are starting to appear in enterprise deployments. These communities often employ a reputation-based application access model. If a given user has enough positive feedbacks he or she will be given access to more of the system, often being allowed to perform administrative tasks. In one start-up example end users who contribute the most leads to jigsaw.com, a community designed to trade business cards, are given permission to de-duplicate and clean data records. Elsewhere user navigation patterns and traversal logs often trigger algorithms that create extra permissions for the user. Lastly community consensus in discussion boards promotes regular users to moderators, which allows them to edit threads, create new topics, and ban other users. How does the security administrator accommodate the hybrid of these security models, and how can the consumer concepts be bolstered with enterprise characteristics like auditing, policy, legal, intellectual property protection, and hierarchical organization structures?

In other words can some of these consumer practices and reputation-based security models be blended with the traditional enterprise access control methods? Some of this is already occurring. Bharosa software, when configured by security administrators in banks can grant or deny application access based on user access history, location of access, or other patterns it encapsulates in algorithms. Customer relationship management systems tap the power of the community to manage security. End users are allowed to flag problematic entries in the corporate database; similar to how someone using craigslist can flag a post they think is an overseas money transfer scam. Will the blending of enterprise and consumer access models happen in a complimentary way, or will it create tension between operational and policy stakeholders? What can security administrators tell us about this phenomenon?

4. FUTURE RESEARCH and METHODS

User centered design methods stipulate best practices in designing software. The first step involves trying to better understand the user. Creation of multiple personas for the security administrators in three different environments will hopefully facilitate this understanding. A combination of ethnography (site visits), interviews (phone and in person), and surveys will be used to achieve this goal. Site visits and interviews will involve at least 5 administrators from each setting, while the survey will target hundreds of participants. A user screener will be developed to better select the participants.

A Wants and Needs Session, as modeled by Catherine Courage and Kathy Baxter [5] will then identify ideal characteristics of a system to grant access in a complex enterprise setting. This method elicits a list of characteristics, objects, and tasks associated with a piece of software. These are recorded on index cards and later prioritized, and grouped into logical clusters (card sort). The last stage will involve the creation of an **online repository of design patterns dealing with security administration**.

Any findings will be published and further disseminated to inform the next generation of identity management or access control management software**. A better understanding of who administers access control will also create better connections between operational, policy, and technology components of the security ecosystem.**

5. REFERENCES

[1] Oltsik, John. 2008. What the heck in IT consumerization?. c/net News Blog. http://news.cnet.com/8301-10784_3-9952825-7.html?part=rss&subj=news&tag=2547-1_3-0-5.

[2] Kowalski, L. and Greenwood, K. 2007. 10 Heuristics for Designing Administrative User Interfaces – A Collaboration Between Ethnography, Design, and Engineering. In Proceedings of the HCI International Conference (Beijing, China, July 22 - 27, 2007). HCII 2007. Springer/ Heidelberg)http://www.springerlink.com/content/9wrx870188845lh5/

[3] Anderson, R. 2007 Searching for Evil. Google Tech Talk series. http://video.google.com/videoplay?docid=-1380463341028815296

[4] Andress, A. 2004. "Surviving Security, How to Integrate People, Process, and Technology", Second Edition. Auerbach Publications.

[5] Baxter, K. and Courage, C. 2005. "Understanding Your Users: A Practical Guide to User Requirements Methods, Tools, and Techniques". Morgan Kauffman. San Francisco