The Divine Right of Kings: Domain Administrators and your (In)secure Network.

The Divine Right of Kings is “a political doctrine claiming that the monarchy was a divinely ordained institution in which kings and queens were answerable only to God.”[1] By extension, this would mean that the actions of these kings and queens are not limited, nor even supposed to be questioned. Indeed, King James I went as far as to say that “kings are justly called gods”[2] and “judges over all their subjects and in all causes and yet accountable to none...”[3]

The reader may ask, “ What does this have to do with Domain Administrators and my network?” Ideas that were passé by the end of the 18th century could hardly be applicable to the fast paced world of Information Security right? Wrong.

In an article dated 21 March 2001, the statistic is presented that in a survey of 267 firms, 91 percent stated that due to insider network abuse, they suffered over $41 million in combined losses over the past year.[4]

Typically network security professionals are faced with a multitude of tasks in which they struggle to keep their network intact. Internet threats, whether cracker/hacker based, automated worms or viruses, etc. We all know of the headline grabbing threats to our networks. We deploy a vast array of tools to help us combat these assailants. ‘Insider network abuse’ in the statement above is the phrase to keep in mind however. What constitutes insider network abuse? Examples of insider network abuse are: information theft, sabotage, and property theft.

What do all of these abuses have in common? Access control. Whether that means physical access to hardware, or file permissions to sensitive data. Access control is the common thread. Security of data centers, laptop inventories, and general physical security is out of the scope of this paper and therefore will not be discussed. This paper will instead focus on access control of network resources, and how it relates to information theft and sabotage. I should clarify my usage of sabotage here. Sabotage is defined as “destruction of property or obstruction of normal operations…”[5]. I seek to focus on the latter half of the definition as it pertains to network security – the obstruction of normal operations – this includes willful or unintentional disruption of normal network operations.

How does a one limit the potential damage from information theft and/or sabotage? By following the ‘principle of least privilege’. This principle can be defined as: “access to information is given on a ‘need to know’ basis. By default a user has no access”.[6] If the user cannot get to it /alter it/ find it, they cannot harm it. The problem with this though is that, there *are* users that have absolute power and access (at least in theory)[7] to everything on your network:

[1] http://www.xrefer.com/entry.jsp?xrefid=502150&secid=.- paragraph A

[2] http://www.wwnorton.com/college/history/ralph/workbook/ralprs20.htm paragraph B

[3] *ibid* paragraph B

[4] http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58737,00.html paragraphs I and J.

[5] http://www.dictionary.com/cgi-bin/dict.pl?term=sabotage

[6] http://www.cccure.org/Documents/Domain_1.doc section *6.13.3.1 Least Privilege* (this document is an open source study guide for the CISSP).

[7] The writer is writing from the perspective of a predominately Microsoft Windows NT environment that contains

your Domain Administrators –the Kings of your network. Some questions arise with regards to this type of access from a network security perspective: Who are these Kings? What do they do? And do they truly need to be King?

Typically your Domain Administrators are your server operators, system support personal and your system architects. Each one of these job functions requires broad access to network resources. Your server operators traverse vast regions of your network making sure everything is up and running, your system support personnel perform a wide range of tasks that need expansive permissions and your architects need to be able to add to and configure your domain to ensure optimal operations. These among a plethora of other tasks are why personnel with these job functions are usually assigned to the Domain Administrator group.

But is this truly necessary? Do these people actually administer your Domain? Are they allowed to set policies in place governing user and system rights? Let's take your server administrators for example. They need to be able to control and administrate all the servers on your network right? Correct. Rather than give them the blanket Domain Administrators privilege, why not create a "server operators" group and add that group to the appropriate machines/files etc. that these server administrators would need access to with the appropriate access level (i.e. local administrator etc). It can be refined even further based on the size of your network, or what have you. Maybe isolate distribution servers or domain controllers, etc. for a further breakdown of permissions. Remember, the goal is to give them access to only that which they need –the principle of least privilege.

What of your system support personnel? They must add and remove machines from your domain, perform a hundred tasks a day troubleshooting the pains of daily operation of your network. Surely they need to be Domain Administrators? Again, the answer is not so. Create a group called "domain machine adders" and add your system support personnel to this group and give the group the permissions to do just as it describes.

To relate and create groups for all of the possible needs of network privilege is again, beyond the scope of this paper, however, the author hopes that the above two suggestions will lead the reader to imagine similar solutions that could be implemented in their own network. It will take time and a great deal of work on your part to set things up in such a way that your organization operates properly and yet securely.[8]

But what of others in your company that are Kings as well, are they 'Kings by right'? Does a desktop support technician get to be King based on his certification as an MCSE? Does a Vice President retain his Domain Administrator 'title', even though he has transitioned into

500+ servers and 6000+ workstations supported by 51 Domain Administrators (not including service/process accounts with this access level). The writer is also making the assumption that the reader has the perspective that there is a preponderance of Domain Administrators in their own network and is seeking a solution to this security risk.

[8] There are vendor products that can assist in the delegated authority role. However at the risk of becoming an advocate of one or another, the author will refrain from recommendations at this point. In Appendix A at the end of this paper there will be a couple of links to vendor products that may assist you in your goal of tightening up network security permissions.

development projects and no longer plays a supporting role in your network?

If the reader will allow this brief aside to comment on MCSE certification, the author would like to reference a recent news article concerning MCSE certification. This article dated 13 August 2001, comments upon the lack of security training to be found in the standard Microsoft certification curriculum.[9] Both Stephen Northcutt[10] and Alan Paller[11] have pointed out repeatedly that MCSE training includes little to no security training. To paraphrase: The SE in MCSE does not stand for Security Engineer.

To return to the aforementioned desktop technician, according to the principle of least privilege, (s)he is to be given privilege according to his/her job functions, not based on apparent qualifications or certifications. The same criterion applies for the Vice President also mentioned above. If the powers required for his/her station requires domain administrative privilege, then by all means, however, if this person is no longer performing a role that requires this level of access, then it is imperative that this access be removed.

If the reader will indulge the author once more, he would like to relate an anecdote from his personal experience that may further illustrate the necessity to apply the principle of least privilege towards their network:

> *My network has a 24-hour monitoring center to assure network uptime. I was awakened at 2am by a series of pages: (we have network monitoring tools in place that page a number of individuals in case of domain policy changes). A night operator was attempting to assist the security guards at the front desk of the building. A desktop support technician, with the idea of being a nice fellow, created a user account for the guards; ironically named "security". The policy for account creation is regulated and administered via our helpdesk, who create all the accounts on the domain. Except of course this one, which was created outside of the established procedure. The security guards had incorrectly entered their password and locked out their account. They, knowing that the night operator was on duty, called him to have their account unlocked. The night operator, again, in the interest of being a nice fellow, decided to give the security guards a couple of extra tries to get their password correct. He proceeded to open User Manager for Domains, and set the password policy to 7 tries before lockout, instead of 3. As you can imagine, the network-monitoring tool paged me and I was able to reverse the policy change back to how it was supposed to be.*

The key to this story is that there was no intentional sabotage of the network. However, both the night operator and the desktop technician were both Domain Administrators, attempting to be 'nice guys'. But I'm sure the reader can see the problem here. If the desktop support technician was unable to create accounts on the domain, there would not have been an original issue. If the night operator was not a domain administrator, he would not have been able to change the user account policy on the domain. In both cases, had the principle of least privilege been applied to the author's network at the time, both incidents could have been avoided.

What then is the network security administrator to do? A suggestion of using the principle of least privilege in setting network security permissions is yes, indeed a good one. But how does one go about designing delegated security roles and permissions? And what am I to do about

[9] http://www.computerworld.com/cwi/stories/0,1199,NAV47-81_STO63028,00.html

[10] SANS Institute distribution email Friday 3 August 2001. Subject: Securing Microsoft's IIS Web Server. See Appendix B.

[11] *Ob cit*. quoted in article above.

having too many Domain Administrators? Fear not my dear reader, I do not seek to lead you all this way, and then abandon you to revealed issues, raised questions and yet, no answers.

However, only you can decide what is best for you network from a security perspective. You know it better than any other, and since I will make the assumption that you've attended the SANS courses as otherwise you would not be reading this, I feel safe in the previous two assumptions as well. You then have the knowledge at hand to start devising ways of limiting the power of the various administrators of your network.

Unfortunately, or perhaps fortunately, there is no Network Security for Dummies[12] book that you could recommend for your entire IT staff to peruse, to help bring everyone on board with your crusade at securing your network resources. It would be tremendously effective if all of your IT staff attended a SANS conference and became as 'security aware' as yourself, but that of course may not be realistic in terms of scheduling or budgeting. So barring these two possibilities as solutions, you are left with a great deal of work on your own.

I would recommend interviewing your support staff and finding out about the jobs that they do, what they need access to and why. Standardize as much as possible and make note of exceptional duties that are performed by members of one group or another. Isolate these actions for later. You can always add permissions as needed in an exceptional case for an individual. This interview process accomplishes two tasks: Accountability and Justification. You will better learn who is doing what and when to your network, and also, are they the ones that should/shouldn't be performing this task. Gaining a better knowledge of what is going on in your network better adapts you to reacting to issues and to ascertain other risks that you may have not come across before.

One caveat though, especially in regards to your Domain Administrators. I am afraid that some Machiavellian maneuverings are in order here. As stated above, Domain Administrators are the Kings of your network, and as King James I said above "accountable to none"[13] is their creed. So how does one convince one who "will not be content that my power be disputed" and/or be warned to "not meddle with… my craft…to meddle with that were to lesson me… I must not be taught my office"[14]. How was one so powerful as a king made to submit to the will of Parliament? Without going into depth regarding the reigns of Charles I (James I's successor), The English Civil War, and James II, it took Parliament until the reign of James II (1688, 63 years after the death of James I)[15] to be able to finally convince the monarchy to have a limitation of its own power. I say this to you my dear reader to warn you that it will take a great deal of time and effort on your part to be able to pare down your Domain Administrators. How will you, the Parliament of your network, then succeed in your endeavor to apply the principle of least privilege before you retire?

[12] http://catalog.dummies.com/booksanddownloads.html. However, interestingly enough, there is a Windows 2000 Server Security book: http://catalog.dummies.com/product.asp?isbn=0764504703.
[13] http://www.wwnorton.com/college/history/ralph/workbook/ralprs20.htm paragraph B
[14] *Ibid*. paragraph C and D respectively.
[15] http://www.xrefer.com/entry.jsp?xrefid=504628 and http://www.xrefer.com/entry.jsp?xrefid=502150&secid=.- for the death of James I.

Your solution lies with the Glorious Revolution of 1688. Where the reign of James II ended with the arrival of William of Orange and Mary to take the throne. A king was used to remove a king with the help of Parliament to support the regime. In the case of your network, you must choose your Domain Administrators to help you gauge the others in your interview process, removing those unnecessary according to your criterion for network security.

A by-product of this process of course is that you yourself are assured of lasting power in your network. You become the 'king-maker' if you will, and then can control who is elevated to the lofty heights of Domain Administrator. Being 'king-maker' is a good position to have if you intend to keep the principle of least privilege in place. As an added security measure, have the Domain Administrator group audited, or even use network-monitoring tools to alert you if someone has been added to this group so that you can prevent or approve this action. I did say it was Machiavellian[16]…

In conclusion, I, your humble narrator, hope that this strange sojourn into history has helped you, my fellow network security professional, to see the importance of applying the principal of least privilege to your network resources. I also hope that it has opened your eyes to the possibility of a network without an excessive amount of Domain Administrators. It will be a long road to travel to obtain the level of security that you desire and need for your network, and this is but one step of many that are required to achieve this level. But I urge you to have faith in the face of adversity and to consider this when trying to implement your ideas. You may encounter those that with to remain with the status quo. Those that would argue that the system of permissions works well enough now, and so why should it be changed? Think then on this:

The concept of the Divine Right of Kings as representative of the power and infallibility of the King and monarchical rule has been totally debunked. Yet, for hundreds, indeed thousands of years, no one questioned it and it persisted. Great strides were made for society as a whole under this system. No one could question that. However, a new way of thinking (the French Revolution)[17] brought about change, irrevocable change. And this 'new' way of thinking about government is now accepted as the normal and proper way to run a society. Dictatorships, Communist Cabals and Monarchies, are now thought of as backwards and totalitarian governmental systems. My point here is that over time, and with persistence, and yes, even some conflict, what was then new, has now become accepted as the norm. It is our goal as Security Professionals to change our own little worlds and domains into something new. A network where it is not just business as usual, but business done safely and securely.

[16] A good resource about Nicolo Machiavelli his theories and practices can be found at http://www.sas.upenn.edu/~pgrose/mach/. I would recommend *The Prince* by Nicolo Machiavelli to read his actual political stratagems. *The Prince* is available at any bookstore or the full text is available online at http://www.ilt.columbia.edu/projects/digitexts/machiavelli/the_prince/title.html

[17] A good source about the French Revolution is again http://www.xrefer.com/search.jsp as a starting point for quick reference and link guides. Bon chance!

Bibliography:

All relevant documents cited within footnotes. The following is a list of the general resources utilized for research.

For Dummies book series:
http://catalog.dummies.com/booksanddownloads.html.

Historical Reference Search Engine:
http://www.xrefer.com/search.jsp

Insider Abuse Article:
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58737,00.html

King James I, *Works (on the Divine Right of Kings)*
http://www.wwnorton.com/college/history/ralph/workbook/ralprs20.htm

Machiavelli resources:
http://www.sas.upenn.edu/~pgrose/mach/.
http://www.ilt.columbia.edu/projects/digitexts/machiavelli/the_prince/title.html

MCSE article:
http://www.computerworld.com/cwi/stories/0,1199,NAV47-81_STO63028,00.html

Online Dictionary:
http://www.dictionary.com

Open Source CISSP guide and resources (homepage):
http://www.cccure.org/
(Relevant document)
http://www.cccure.org/Documents/Domain_1.doc

Appendix A:
Vendor list to assist with delegated authority roles in implementing the principle of least privilege:

http://www.netiq.com/solutions/security/default.asp

http://www.tivoli.com/products/solutions/security/news.html

http://www.bindview.com/products/solutions/security.cfm

Appendix B:

From: The SANS Institute [sans@sans.org]
Sent: Friday, August 03, 2001 10:15 PM
To:
Subject: Securing Microsoft's IIS Web Server

Hello, I am Stephen Northcutt, from the SANS Institute. The recent code red worm has been an interesting and instructive experience for all of us. We are very fortunate that this worm was essentially benign; it did not delete files and only consumed bandwidth and took down routers. Things could have been a whole lot worse! As you know, the root cause of the problem is poorly configured Microsoft IIS web servers. If we don't learn to deploy IIS properly, then any vulnerability in IIS can be used to start another worm and we will have to go through the whole mess again. In this world of copycat attacks, is a significant and immediate possibility. Please ask your MCSEs and others managing Windows systems to get your IIS systems configured safely. Microsoft certification does *not* cover this material or much security at all. We each need to do our part to get this mess cleaned up.

SANS Instructors, Jason Fossen and Eric Cole are available during the next few weeks to teach a special one-day course on Securing IIS. The description of this course can be found at:
http://www.sans.org/sec_IIS.htm

We have found space in several cities in the coming weeks. The draft schedule is included at the bottom of this note.

We will run this class only in those cities in which there is sufficient interest. If you are interested in attending, or sending your people drop us a note at IIS@sans.org by Wednesday, August 8. Tell us your name and your organization's name, the city (and date) you would attend, and the number of people from your organization who will definitely come, the number who will probably come, and the number who may possibly come.

If you are running Unix and you know someone running Windows IIS, please forward this note to them. If we have enough interest, we will run the courses. We haven't determined pricing yet, but it would be inappropriate to try to capitalize off of this attack. When we know the cities in which people are interested in attending the course, we

will calculate the hotel, travel and printing and other costs and
compute an average and send the price (probably under $250) to everyone
who asks us to hold space for them.

Regards,

Stephen Northcutt
The SANS Institute

Ottawa - August 13
Crowne Plaza

New York City - August 20
Sheraton New York

Atlanta - August 22
Sheraton Colony Square

Raleigh - August 25
Sheraton Imperial

Boston - September 11
Boston Park Plaza

Chicago - September 13
Westin Michigan Avenue

Los Angeles - September 15
Westin Hotel

San Jose - September 17
Sheraton San Jose

Washington DC - September 22
Renaissance Hotel