



Goldie Locks and the Three Least Privilege Desktops



Table of Contents

About the Author.....	3
Obtaining Least Privilege for Desktops.....	3
Goldie Locks and The Three Least Privileged Desktops.....	3
Goldie’s Work Responsibilities.....	3
Goldie’s Application Needs.....	4
Goldie Finds the Computer Lab.....	4
The Rest of the Story.....	8
For More Information.....	8
About Beyond Trust.....	9



About the Author

Derek Melber, MCSE MVP, is an independent consultant, speaker, author and trainer. Derek's latest book, *The Group Policy Resource Kit* by Microsoft Press, is his latest best-selling book covering all of the new Group Policy features and settings in Windows Server 2008 and Windows 7. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, security, and desktop management. Derek also provides sales consulting, to help sales and marketing sell technology. Derek speaks and trains all over the world. You can contact him at derekm@braincore.net.

Obtaining Least Privilege for Desktops

Like most corporate computer networks, there are a wide range of environments in which users work. Our story deals primarily with the desktop environment. While this particular example focuses on end-users, similar stories exist for other user groups like IT staff, developers, mobile users, and other unique workers in the corporation.

As the standard end-user makes up more than 75% of all users in the organization, we've decided to start our story here. This story focuses on one employee, Goldie Locks, and the three desktops that she discovers -and tries to work with.

Goldie Locks and The Three Least Privileged Desktops



Goldie is a new, upbeat employee who is familiar with Windows desktops. Her experience is based on having used computers in college and her current hobbies at home. From this exposure, she knows how to use her computer rather well.

Goldie Locks is most familiar with Windows XP Professional, having only dabbled with Vista once. She has two degrees: marketing and multimedia communications. Goldie has a general understanding of program development from a Visual Basic course she usually skipped in college, but one would never consider her proficient. Goldie also understands enough about networking to have created a wireless WEP network, which uses the built-in security of the router connected to her cable modem. She regularly attends IT seminars and tries to absorb as much information as possible

from the few technology magazines that she subscribes to via her iPad.

Last month, Goldie was hired by a medium-sized Information Technology company. She is responsible for much of the company's external marketing efforts. She oversees both print and Internet marketing, as well as the monthly webinars that the company provides to promote their products. Goldie requires slightly more than a standard desktop, due to the applications required to perform all of her job duties.

GOLDIE'S WORK RESPONSIBILITIES

Goldie spends a significant amount of time on the Internet in order to develop, test, verify, and research the products and messaging she produces. On any given day, Goldie may need to:

- Install a printer
- Install a new application
- Run an application designed for developers, so she can update the website or preview a layout
- Perform research online, maybe even downloading an Internet Explorer add-on
- Run web-based applications for the webinars, which typically require an ActiveX plug-in
- Install an ActiveX plug-in to access a site that might have a video, application or widget she needs



GOLDIE'S APPLICATION NEEDS

The applications that Goldie runs are essential for her job. The most important is her front-end application to the database of users. Goldie is learning that she can create her own custom queries, which make her job more efficient and her marketing more targeted.

This application requires that the user running it be a local administrator. The application makes changes to files within the System32 folder, which are specific for each user, but are still stored in the System32 folder by design. Optional solutions have been considered, but to date no solutions exist allowing standard users to run this application.

Goldie also runs several web development applications, which she uses to update, test, and evaluate the company website. Goldie either works on the live content that she directly controls or gets a copy of the current content and runs a local web server so she can see the results of her changes immediately.

Goldie's computer runs a WWW publishing service in order for the applications to function properly, and the majority of the development applications require her to be a local administrator in order to develop content.

Goldie must have the ability to install a local printer on her computer. She must review each design physically before sending the files out for production. Goldie has several printers connected to her computer, as she knows she will have to swap printers based on her printing needs.

Goldie uses several web-based marketing tools which require the use of ActiveX controls. There are two issues that have the IT staff concerned. First, all ActiveX controls require the user be a local administrator to install the control. Second, ActiveX controls can harbor and distribute worms, viruses, etc. which the company wants to avoid.

Goldie absolutely needs the autonomy to install any ActiveX control that is needed for these sites and she understands that security is important to the company. She has agreed to notify the IT staff when installing any ActiveX control, so they are aware of what is running on her computer in the event of a virus.

GOLDIE FINDS THE COMPUTER LAB

One afternoon, while walking through the halls of the office, Goldie stumbled upon the computer lab. Through the office door she saw three computers sitting on a table. Each computer was labeled: "No Privileges", "Over Privileged" and "Ideally Privileged".

The computers were new and the seats looked so comfortable that Goldie couldn't resist. Looking both ways down the hall, she slipped into the lab to have a look.

Goldie Finds Computer #1



First, Goldie sits down at the computer labeled "No Privileges." At first, she is excited to work on a computer exempt from viruses, malware, and other malicious applications.

Goldie finds that all of her applications are installed, just like on the computer at her desk. Her marketing application is installed and appears to be configured properly. She finds her web-based development tools are installed, as well as the WWW publishing service.

Goldie notices that no printers are installed, which she wants to fix since she's so proficient at that task. The computer is connected to the Internet, so Goldie also wants to test her web-based tools that run ActiveX controls.

Goldie Tries an Application on Computer #1

Goldie decides to start with the marketing application that is so critical to her job. The application takes her to a client-side login, but when she enters her username and password, she gets an error message which states "You must be a local Administrator to run this application. Contact an Administrator." Goldie sits back in her chair and thinks about how the computer labeled "No Privileges" can't run her application, even when the application is installed. She is a bit disappointed, but considers the other tasks that she must run for her job.

Goldie Tries to Install a Local Printer on Computer #1

Goldie then tries to install a local printer. But when Goldie then clicks the option to install the printer another message box appears. It also states that to install a local printer she must be a local Administrator.

Again, on the "No Privileges" computer, Goldie is unable to perform a routine task that she needs for her job. Goldie realizes that the "No Privileges" computer might not be all that functional, even though it appears to be secure!

Goldie Tries to Install an ActiveX Control on Computer #1

Finally, Goldie heads to the Internet. Goldie types in the URL to one of her favorite research sites and is immediately shown an error message. The message says that she can't access the site because an ActiveX control needs to install, but can't. Of course she knows immediately what the issue is... she is not a local Administrator.

Goldie is completely distraught at the "No Privileges" computer. She has tried nearly all of the typical tasks that she needs for her job and not one of them worked. Goldie leans back in her chair and decides... "The No Privileges computer is too restrictive!"

Goldie Finds Computer #2

Goldie slides over to the next computer, which is clearly labeled "Over Privileged." She is a bit apprehensive, knowing that default settings are often too loose to properly secure a computer for a corporate, or even home, environment.

However, she is determined to test this computer in the same way she tested the previous computer.



Goldie Tries an Application on Computer #2

Goldie finds her marketing application and launches it. She inputs her username and password, and clicks the OK button.

From the Start menu, Goldie launches the marketing application which loads immediately. Goldie has no problem seeing or making changes to her documents. The application works like a charm.

Goldie then finds another application -one she has never seen. She clicks on the application, which loads instantly. The application begins to display lists of information, which Goldie can clearly see are network traffic packets. Goldie clicks on one of the packets, which shows information about users that are logging on -including the domain name, username, and password hashes." Goldie immediately closes the application and looks around. She knows that many corporations have Intrusion Detection Systems (IDS) to monitor and flag this type of application. Since no one from the security department knocks on the door, she moves on to her next task.

Goldie Tries to Install a Local Printer on Computer #2

Goldie launches the printer install wizard and within moments has it successfully installed. She selects the "Test Print

Page” option and sees that there are no error messages. It is clear that on this “Over Privileged” computer Goldie will be able to install her local printers with ease.

While in the Control Panel, Goldie can see the Users and Groups option. She decides to try and create a new user. She is able to create a new user, and gives that user a password. Not only is she able to create a new user, but she is able to add this user to the local Administrators group, giving her unlimited access.

Goldie closes the users and groups window. She knows that granting local Administrative privileges on the desktop is just like giving up full control of that desktop to the local user.

Goldie Tries to Install an ActiveX Control on Computer #2

Finally, Goldie heads to the Internet to see if she can access her favorite research site. She inputs the URL and finds the computer installing the ActiveX control, followed by the site coming up. She runs a few queries, and finds that the site is fully functional on this “Over Privileged” computer.

Goldie clicks the Favorites tab and discovers a site she has never seen before which is intriguing. She clicks on link and within a few seconds, the computer becomes non-responsive. She waits to see if the site is just installing an ActiveX control or plug-in, but the mouse still is very slow to respond. Goldie closes out of IE to see if it would help, but finds that the computer is nearly locked solid.

She restarts the computer and inputs her credentials. While everything looks normal, the mouse is still non-responsive... Goldie hit a site which installed a virus or worm!

Realizing that she just infected the “Over Privileged” computer, she turns the computer off by the power source. She succeeded at each of her tasks, but she could also do ANYTHING she wanted on the “Over Privileged” computer.

Goldie pushes back from the desk and decides, “The Over Privileged computer is too insecure!”

Goldie Finds Computer #3

Goldie moves over to the next computer, which is labeled “Ideally Privileged.” She is apprehensive as the first two computers were certainly not ideal. She is hopeful that this computer is the right fit.

Goldie Tries an Application on Computer #3

Goldie launches her marketing program, logs in, and can do everything that she needs. Success!

She tries to run the network traffic program she saw on the “Over Privileged” computer. An error message appears saying the application requires local Administrator privileges.

Goldie sits back bewildered. How can she run her marketing application, which requires local Administrative privileges, but not the network traffic analyzer, which also requires local Administrative privileges?

Goldie Tries to Install a Local Printer on Computer #3

Still puzzled, Goldie decides to try installing a printer. She quickly moves through the menus and finds that on the “Ideally Privileged” computer, the printer installs easily.

She then tests to see if she can create a new user and include them into the local Administrator group. To her surprise, she could neither add a new user nor add to the local Administrator group. Both actions required local Administrator



privileges.

Goldie began to think that this computer might really be “Ideally Privileged”.

Goldie Tries to Install an ActiveX Control on Computer #3

Finally, Goldie goes to the Internet to test her favorite research site. The ActiveX control installs easily and she is able to use the site fully. Goldie then decides to test and see what happens when she visits the “malicious” link from the “Over Privileged” computer. She clicks on the link and the site loads, but her mouse still moves quickly and smoothly. She searches through the site but has no change in performance.

Goldie leans back in her chair smiling and realizes the impact this computer could have on her productivity. This “Ideally Privileged” computer is exactly that, IDEALLY PRIVILEGED! She can run all her applications and perform her other daily functions without infecting or altering any essential aspect of her computer.

She then realized, “This computer is secured just right!”

IT Staff Finds Goldie in Computer Lab

Just then, the computer room lab door opens and in walks Steve, a member of the IT staff. Steve asks Goldie what she is doing in the lab and she explains that she was walking by and decided to come in to see what was going on.

She tells Steve of her experience with each computer which intrigues him. Steve asks Goldie for more information on her experiments.



Goldie Describes Computer #1

Goldie explains to Steve how the “No Privileges” computer was just too secure and not functional. The applications she needed on a daily basis would not run, she could not install local printers, and her essential research websites would not function because the “No Privileges” computer wouldn’t allow her to install the ActiveX controls which were required.

Goldie Describes Computer #2

Then Goldie tells Steve about her experience with the “Over Privileged” computer. Yes, she could run her applications, install her printers and use the Internet for research, but the computer became highly unstable and was easily infected by viruses or worms.

Steve laughed and made a note to himself to rebuild the system.

Goldie Describes Computer #3

Goldie’s eyes lit up as she began to describe the “Ideally Privileged” computer. She explained how she could run her programs, install printers and install ActiveX controls for her web-based research needs. Then she explained her confidence and joy at discovering that she could not harm her computer, even when she purposely tried the same actions that had made such a mess of the “Overly Privileged” computer.

Goldie then expressed her puzzlement as to how this was possible. “How can I run the applications and features I need, which require local administrative privileges, but can’t run the applications or features I don’t need, which also require administrative privileges? I would love to have this computer on my desk! It’s ideal! But how is it possible?”

Steve got a big smile on his face and explained with great confidence how BeyondTrust® PowerBroker® for Windows made it all possible. It is PowerBroker® for Windows that makes the “Ideally Privileged” computer JUST RIGHT!

THE REST OF THE STORY

The IT staff took the advice and experience of Goldie. They knew they could configure all of the existing desktops and create "Ideally Privileged" computers for everyone. They knew that each desktop had the user account tucked into the local Administrators group. They also knew that the user of the computer most likely knew the local Administrator account password, since they could easily change that password to something they knew.

It was at this point that the IT staff used the newly released Group Policy Preferences (GPP) from Microsoft[®]. GPP gave them the ability to quickly and easily remove every user from the local Administrators group. In the same policy refresh, GPP also allowed the IT staff to change the local Administrator password. The only thing left was to implement least privilege so that all applications could be installed and run, OS features could be, and ActiveX controls on essential websites could be installed.

The IT staff deployed BeyondTrust[®] PowerBroker[®] for Windows using Group Policy on each computer. Then the IT staff used the auto-rule generator from BeyondTrust[®] to produce all of the rules that were needed. Within no time at all, all of the desktops within the company were running the Ideally Secured computer with PowerBroker[®] for Windows providing the solution to all of their needs for running as least privilege users. The entire deployment of desktops were configured just right!



For More Information

If you find your desktops either over-privileged or under-privileged, you should take Goldie's advice! BeyondTrust[®] PowerBroker[®] for Windows can get your machines configured just right in no time at all.

[Click here for a free 30-day trial of PowerBroker[®] for Windows](#)

About Beyond Trust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in San Diego, California. For more information, visit beyondtrust.com.

CONTACT INFO

NORTH AMERICAN SALES

1.800.234.9072
sales@beyondtrust.com

EMEA SALES

Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS

550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US

Twitter: [@beyondtrust](https://twitter.com/beyondtrust)
Facebook.com/beyondtrust
[Linkedin.com/company/beyondtrust](https://www.linkedin.com/company/beyondtrust)
www.beyondtrust.com