iSeries Security in a Networked World

By John Earl

John Earl

Beginning with the day that you attached the first PC to your AS/400, your AS/400 has been exposed to the risks of networked computing. Many of us could afford to ignore those issues because we were working in insulated environments where our internal networks were generally protected from the outside world. But with recent networking advances, the growth of the Internet, and the acceptance of TCP/IP as a communications protocol on the AS/400, the insular status of our AS/400's has evaporated and many of us find ourselves at the mercy of those who know how to prowl the network.

Today, your network might include AS/400, PCs, mainframes and various flavors of UNIX, Linux, etc. In this networked environment, tools like FTP, Client Access Express Data Transfer, Remote SQL, DDM and others allow easy access to AS/400 data and services. These alternative access methods bypass the traditional Menu-Based security implemented in many AS/400 installations. In today's networked environment, even the attachment of one PC to your AS/400 introduces new security challenges that must be thoughtfully considered, and dealt with.

Who Are You Connected To?

It used to be easy to figure out whose system(s) you were connected to (and who was connected to you your system) simply because you could count the number of networked computers on one hand, and count the number of systems with outside connections on the other. But now almost everyone has a PC, there are numerous servers in your organization, and you connect your systems to an uncounted number of people who are outside of your organization. Monitoring which network connections are active could easily be a full time job, not to mention trying to keep track of what data is moving over those network connections. And even if you are comfortable with the security of your own network, every one of those connections represents the risk of an un secure network compromising the security of your network.

> "Not connecting your servers on the internet can be more risky than connecting them."

And yet, you can't realistically just shut off access to and from the outside world. If your business is going to do business in the 21st century, you've got to take advantage of the opportunities that B2B computing offers. Put simply, shuttering your servers from the outside world is as risky as putting them on the network without properly securing them. Businesses are demanding interconnectivity, and you'd be foolish to resist. As an IS professional, you can demand to conduct electronic business in a secure fashion, and use the tools and procedures are available to assist you.

You don't have the option any more (if you ever really did) of simply refusing to connect your servers to outside computers.

Hackers and the AS/400

Five years ago the AS/400 was a virtually unknown commodity in hacking circles. But several factors have conspired to change that. Beginning with V3R1, OS/400 supported a TCP/IP stack that not only performed reasonably, but IBM included that TCP/IP stack with the cost of the operating system.

At the same time that TCP/IP became more a more prevalent protocol, and increasing number of older AS/400's started to appear on the used system market.

The increased availability of cheap, used, AS/400's meant that more and more people could afford to put a bootlegged box in their basement and experiment with what was once a very closed and secretive operating system. In V4R1 IBM launched it's big push to the web, making AS/400's even more accessible, and more inviting as targets.

The confluence of these events has caused the AS/400 to be noticed by the hacking community. While their initial attempts at gaining knowledge of OS/400 weaknesses had been hampered by lack of availability, that lack of availability to the OS is becoming less of a problem. Added to that, there are a couple of individuals that frequent these hacking newsgroups who appear to have some basic understanding of OS/400 security – and it's weaknesses.

Closer to Home – an ODBC Wake-up Call

Still, OS/400 security architecture is very robust, having received the U.S. Department of Defense "C2" security rating for "Trusted Systems" when properly configured.

The security exposures introduced by network data access tools like FTP and ODBC do not indicate a failing on the part of AS/400 security. Rather, the data access level you provide to a user via AS/400 security for "Green Screen" access using menus and screens may not be the same level of access you want to allow using network tools like ODBC.

For instance, the same OS/400 authority that allows a user to view the contents of the Payroll file is the authority needed to download the file to a PC and post it on the Internet

Let's consider an example of a payroll supervisor 'Bob'. Bob has been granted *CHANGE authority to the payroll master file so that he may make changes to pay rates and add new employees in his department.

It is expected that Bob will do this work through the "green screen" menu-based programs. However, Bob is also well versed with programs like MS/Excel™ and MS/Access™. Using these PC based programs and an ODBC interface, Bob's ***CHANGE authority** is sufficient to Add, Change and Delete records from the payroll master. In fact, he could also delete all the records from the file. A simple typing mistake on Bob's part can compromise the entire payroll file.

Another concern is that Bob has read authority to the entire file. While using the green screen, Bob is limited to only viewing records for the employees that work in his department.

> "OS/400 is still one of the most securable operating environments available."

But with ODBC and his *CHANGE authority, Bob has the ability to view all of the records in the entire file... including his peers and the senior management. Now you find that Bob is suddenly sullen and upset with his compensation plan.

DDM and Remote Commands

DDM has been around and active on OS/400 since release 1. It's a wonderful tool that provides intersystem connectivity at a file level, and even at a record level. DDM also support Remote Command, which provides the ability to run a command on some target machine while you are currently signed on to another source machine.

DDM comes shipped with every AS/400 and iSeries machine, and defaults to active. This means that when someone sends a remote command from some other computer to your AS/400, your AS/400 is pre-set to receive and run that command. And worst of all, this DDM remote command capability does not honor the Limited Capability (LMTCPB (*YES)) parameter set in the User Profile. A major component of many security designs has been to limit the users' access to a command line. But if DDM allows these remote commands, then a major component of the security design doesn't work as designed.

Tying It All Up

The long and short of it all is that OS/400 is still one of the most securable operating environments available. (Note that I wrote "securable", not necessarily "secure.") When configured correctly, OS/400 can prevent undesirable access better than most OS's, and as well as the best of them.

But that leaves you, the system administrator, with the task of tying it all up. You've got to evaluate your OS/400 security as if it were the hub system in a vast planetary network (which it either is, or will be), and secure your system as if you have no idea who might come knocking next (which you don't).

Networked computing is a powerful industry force that, among other things, obliterated the value of our old security schemes virtually overnight. It's time to step up to new models and new ways of thinking about security in our complex and often heterogeneous networks. It's time for new models and new designs. And why wouldn't it be? Networking has changed the way that we compute. It must also change the way we secure. T🖫G

John Earl is the Chief Technology Officer of The PowerTech Group, a Seattle, WA Security Services firm. He is also the lead architect of the PowerLock Network Security for AS/400 product, an instructor for The 400 School, the Security Editor for Midrange Computing Magazine, a frequent speaker at AS/400 industry conferences and user groups, and a two time winner of COMMON's Speaker Excellence award. You can reach John Earl with your AS/400 security questions via e-mail at johnearl@400security.com.

Photos by Michael Earl

Dad, (John Earl) and Riley