Reader John Bumgarner told me about some nifty work he’s been doing to lock down canonical accounts – those standard accounts that have the same password across all systems at the time they’re installed. Typically they are used for system administration by software and hardware vendors but are left in their initial state because system owners don’t realize that the accounts are there and vulnerable. These canonical accounts must have their passwords changed at once to prevent abuse, but many systems have their doors propped wide open by unchanged standard passwords. Another approach, on those systems that use resource accounting and controls, is to assign a zero value to some critical feature (such as maximum allowed CPU seconds or maximum allowed session minutes) for a canonical account; such a value precludes new logins to that account until system managers reset the parameter.

With my usual disclaimer (I have no financial relationship whatever with Mr Bumgarner, his product or his company), here’s an edited version of what Mr Bumgarner wrote about his software project:

* * *

Canonical accounts not owned by end-users are among the easiest avenues for breaching system or network security. These trophy accounts often protect the crown jewels of an enterprise, but they are often configured to allow easy access to anyone.

On one security project I found an account that controlled hundreds of servers. Once the password for that account was broken, an attacker could pillage the network. The customer had no mechanism for rotating the account’s password or auditing the account.

Out of that encounter I got an idea for a new security application, PassGuard (not to be confused with the PassGuard Framework that handles encryption of passwords), that would reduce administrator workload and improve security by generating complicated passwords and changing them automatically at set intervals. These automatically-changed passwords, coupled with an audit trail, should interfere with brute-force attacks on the canonical accounts.

A typical complex password would look like this:
%Z7F(TMp,Abp8_Gu'$#pVJA21<zmT7}'}HA]"$N]GEgM=I08JJn!XjBq7&m\}wq(I"?G<@H\ot1}ho\kQgmbu(Q(!V&=7?PK6$#th<8]zpFR_]ZP{3+yN4A,,z2Ue. A supercomputer running 43 trillion calculations per second would take about 5 x 10^32 years to stumble upon this password using brute-force testing.

When a person does need to access the system using one of the accounts protected by the complex password, he or she removes the account from the management mode and sets a new, human-usable password. The account can later be added back to the management queue with a few mouse clicks. One can even schedule the account to be automatically added back to the
queue, thus reducing administrator overhead. The same scheduling feature is useful for granting and terminating access to specific accounts by temporary employees.

The product also has several built-in audits which allow administrators to query the network for common security vulnerabilities such as unused accounts, and to perform corrective actions such as removing or locking an account. All the audits allow the administrator to generate a report which can be used by auditors or by management.

These pre-defined audits have even been used to identify hackers who were using privileged accounts in the customer network after hours. Audits can also be scheduled to run unattended with the results e-mailed to the administrator.

PassGuard currently controls only Windows-based operating systems, but versions for others, such as Solaris, HP-UX and Novell, are being developed. A version is also on the drawing board that will support other platforms such as networking devices.

For more information about this project, see <http://www.cyberwatchinc.com/products.htm>.

***

For further information

Contact John Bumgarner, M.A., CISSP, GCIH, IAM, SSCP at Cyber Watch, Inc.
P.O. Box 690087
Charlotte, NC 28227-7001
Voice 704.573.4608
Fax: 704-573-6654
mailto:john.bumgarner@cyberwatchinc.com

Passguard Framework <http://passguard.sourceforge.net/>

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.