

Re: Account lockouts

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/0442.html>

From: Vin McLellan (vin_at_theworld.com)

Date: 01/11/05

Date: 10 Jan 2005 17:12:06 -0800

Steve Riley wrote:

> *Why don't you just disable account lockout? This feature is in the
> product only to satisfy old-style auditing requirements and the
> military. Really, though, it's more of a pain than anything else.*

Umm. So you live in a world where audit and other "compliance" pressures are diminished? You see installations which use reusable static passwords and that *don't* face Board of Director concerns about how to harden them and make them more resistant to guessing and replay attacks? I'm surprised. I see all the trends heading in the opposite direction.

Are the Microsoft, SANS, or NIST security templates any more liberal in their recommendations on account lockout policy than the NSA security template? Not much, as I recall.

You don't think it is a bit rash to recommend that Admins discard a security mechanism that has traditionally been seen as defense-in-depth for reusable passwords and the AAA infrastructures that rely upon them?

For those who work in public US companies, I suspect it will be a rare IT audit that does not press for more granular authorization, more extensive audit logs, and (where mere passwords are acceptable) all the obvious restrictions on password construction and use.

In that context, account lockout policy — duration, threshold, lockout counter reset — is often seen as a useful mechanism to insure a fail-safe (i.e., fail *closed*) policy for the access control systems under attack.

> *Account lockout supposedly protects you from password guessing or
> cracking attacks.*

Sounds right to me.

If we can estimate the cost of attack in terms of the amount of work, access, indifference to detection, special knowledge, and time to

detection and corrective action (WAIST), account lockout policies potentially limit both the attacker's freedom of access and time to detection.

Unfortunately, there is the typical tradeoff for higher security in potential hassle for the users, and certain hassle for the Admins. So what? Security costs something. Account lockout should never be applied haphazardly — since it obviously can cause legitimate user problems if the threshold is set too low — but there are options in the lockout scheme (threshold, duration, reset cycle) that also give the Admin tools to adapt his account policies to his local security requirements and his user base.

There are, you may recall, formulas that we can use to calculate the probability of success of password guessing attacks. While these are often reassuring, they can also be misleading. Precomputational guessing attacks like RainbowCrack for NTLM and AsLeap for Cisco LEAP have cut the amount of actual time necessary to calculate a password from its ciphertext to a tiny fraction of what earlier dictionary or brute-force attacks required. The Admin's arsenal of longer more complex passwords, etc., can make even this sort of attack more expensive — but storage and processing capacity continue to plummet in cost, and malware worms have added rapid deployment to the password-guessing threat.

Even for token-based authentication systems like RSA's SecurID, account lockout controls are seen as a critical defense against attacks on the weaker (static, reusable) element in the two-factor passcode. They are seen as especially valuable if the token has been stolen and a thief is guessing PINs, so that lockout threshold is usually set low.

> *In reality [account lockout policies] *create* opportunities for
> denial-of-service attacks, and this could be what you're
> experiencing. Users accidentally DoS themselves out of accounts
> all the time; attackers can easily DoS entire domains since user
> IDs are rarely secrets.*

Surprise. DoS risks are the stuff of Network Life, for good or ill. So long as network resources are finite, and networked systems interdependent, DoS attacks will exist and will have to be managed. They are probably unavoidable in a TCP/IP environment, and mitigated best if we can better hide more of the potential targets: networks, systems, apps, accounts.

Us users doubtless do shoot ourselves in the foot with irritating regularity, and account lockout policies inevitably do create opportunities for hostile DoS attacks, but the legitimate security function of those policies — as a fail-safe option for an account under attack — has historically been seen as more important than those risks, none of which are new.

- > *If you enforce strong passwords with group policy or a passfilt.dll, then*
- > *you don't need account lockout at all.*

Ah yes, the prayer for "strong" passwords. I'm no fan of reusable passwords — given a Draconian password policy or even a handful of password-protected accounts, "strong" passwords are almost always written down in the real world — but I had expected that most advocates of passwords would cling to account lockout as one more defensive barrier they could display to stave off pushy auditors.

- > *Someone did a study once that showed the average cost for doing a*
- > *password reset or account unlock is US \$70. There are better things*
- > *to do with that money and time!*

I don't know about \$70, but a similar number wouldn't surprise me when an Admin takes the time to find out why the account locked up. Auto reset is cheap, however. Where managers adapt and tune the lockout mechanism to their users and their environment, I expect the number and frequency of those help desk calls won't be a big deal, except when there is a real attack.

Among the new realities for IT in 2005, however, is the undeniable fact that enterprise managers face a battery of new external regulatory pressures to tighten up their IT system controls across the board. Authentication, authorization, and audit logs are particular concerns. Password-based user authentication is today often seen as suspect — too easily compromised or mismanaged to be the basis of either access controls or internal accountability, perhaps the most essential business process.

No one who counts — investors, directors, customers and partners, regulators, legislators — really gives a hoot about IT's work load, or IT's budget battles in the C ring, or whether the IT staff is too overworked to investigate account lockouts or manage account resets.

These "outsiders" brashly demand more trustworthy financial data, more secure data storage, tighter controls on access, more granular authorization, and much richer audit logs — and they no longer trust either corporate executives or "professional" IT security folk to voluntarily provide them with the level of assurance they require. Hence we have GLB, HIPAA, Sarbanes-Oxley, Basel II, and the EU and Japanese Data Protection Directives — all of which put new sharp teeth in those old-fashioned audit mechanisms.

Last year, as you may have heard, Bill Gates declared that passwords are "dead." RSA — for which I've been a consultant for many years — finally got to offer the SecurID as a native authentication option for MS Windows. This skepticism about IT controls inevitably spread into consumer circles with the phishing and "identity theft" epidemic. Last month, for instance, the FDIC "recommended" that US banks should

microsoft.public.security: Re: Account lockouts

upgrade from passwords to two-factor authentication devices for online banking.

I think it might be wise to consider the trends before you discard any security controls, even one as potentially irksome as account lockout. Suerte,

.
_Vin