

Re: Biometrics

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2008-07/msg00169.html>

- *From:* "Steve Riley [MSFT]" <steve.riley@xxxxxxxxxxxxxx>
 - *Date:* Sun, 20 Jul 2008 23:06:38 -0700
-

Thanks for reading.

1. More detail, please. Which ones do you have in mind that we haven't implemented?
2. There is no "internal safety" in the 9x code. If you connect a 9x computer to the Internet, it will get attacked. There are plenty of ways to boot a computer with an alternate operating system if you need to perform some kind of maintenance. (Note that as more and more people move to volume and drive encryption, there will be additional steps, especially around key archiving and recovery passwords.)
3. This is a typical recommendation for root certificate servers — they are the sources of authority for identity and they don't need to be online, so keeping them disconnected and physically secure is sage advice. (And note that you can't really ever "prove" that someone isn't a spy — you can't prove a negative.)
4. Most organizations achieve huge support cost savings by standardizing on hardware. Per-machine custom twiddles add unnecessary complexity, which increases the likelihood making configuration mistakes, which attackers will then exploit. (The TPM chip, a hardware device that can store encryption keys among other things, provides a useful machine identity.)
5. Can't argue with that.
6. You're talking about honeypots and honeynets. They're interesting for learning about attacker behavior and motivations, but they aren't security devices.
7. I'm not sure why you insist that the current version of Windows is the same as NT. Over time we have rewritten much of the code. One example is the IP stack in Vista/2008 — it's all new.

—
Steve Riley
steve.riley@xxxxxxxxxxxxxx
<http://blogs.technet.com/steriley>
<http://www.protectyourwindowsnetwork.com>

"Dan" <Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:A415E3B7-1750-44E6-8BDE-707D90A5EDB0@xxxxxxxxxxxxxxxxxxxxxx>

I looked over your blog and like your points Steve. You certainly have a great grasp of the security aspect of protecting computers. Now here is my

Re: Biometrics

view:

1. Please implement all of your security protocols
2. Use Windows 98 Second Edition Machines as a safety internal protocol as Chris Quirke, MVP suggests how the internal safety of 9x is awesome and makes remote hacking difficult thus when someone does manage to hack a network they cannot overcome the internal safety of the 9x operating system that has the maintenance operating system of DOS that Chris Quirke, MVP maintains is sorely lacking in Vista.
Consider the possibility of having one 98 Second Edition machine as a Gateway to the Network.
3. Maintain certain machines as off-line only in locked and secure rooms with minimal access and information only given on an as needed basis as is done in the military and at defense companies like Raytheon after full background checks and after enough time has passed that you can prove the person is not a spy.
4. Implement the proper configuration and customize hardware options of all machines so if a certain machine that is released in the market has been compromised the security and safety of your network is not at risk.
5. Inform US-Cert (Department of Homeland Security in the States) of any attempted and seriously probing of your network.
6. Ideally have special catching machines to attract high level hackers to them for highly valued information via the proper protocol of bait and catch.
7. Have Fun and See How Many Hackers you can Catch and Remember this is Truly all a Game of being able to one up the hackers ---- ideally Microsoft will soon have a 3rd source code that can finally put 9x and NT to rest and have the best of safety and security within one source code but I wonder if this is even possible but certainly Microsoft does need a new source code.

Thanks Again for all of your Advice and Your Great Blog and Feel Free to Let Me Know My Shortcomings in the Debate ---- I really appreciate your Feedback