

# Re: Biometrics

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2008-07/msg00167.html>

---

- *From:* Dan <[Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 20 Jul 2008 21:46:06 -0700
- 

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 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 informaion 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

Re: Biometrics

"Steve Riley [MSFT]" wrote:

Biometrics can never replace passwords, because they aren't secrets.

It's me, and here's my proof: why identity and authentication must remain distinct

[http://technet.microsoft.com/en-us/library/cc512578\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/library/cc512578(TechNet.10).aspx)

--

Steve Riley

steve.riley@xxxxxxxxxxxxxx

<http://blogs.technet.com/steriley>

<http://www.protectyourwindowsnetwork.com>

"Dan" <Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:774EE7CB-CA2B-4E7B-82CD-20D2B56C04B4@xxxxxxxxxxxxxxxxxxxx>

Bingo! You solved the issue and yes it is one of those cheap fingerprint scanners where you just swipe your finger so it must have already had the image of my fingerprint on the scanner. It sounds like someone would need to clean the fingerprint scanner each time and it does indeed seem very easy to fool. So much for the security of Biometrics at least cheap Biometric devices

"Juergen Nieveler" wrote:

Dan <Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

How secure and safe is biometric technology? The reason I bring this up is because I was able to log in using my finger with a band-aid attached and this definitely makes me question the security and safety of biometric technology at least as far as laptops go. I imagine there probably is lots of articles on this already but I wanted the opinions of this newsgroup. Thanks in advance for the replies.

## Re: Biometrics

If this was one of those fingerprint readers where you simply put your finger on (as opposed to those where you rub your finger along the contact plate in a swipe motion), chances are that the camera inside picked up the latent fingerprint that was still on the glass – this is a common vulnerability of those cheap camera-based readers. All they do is notice "Oh, something is pushing on the glass, and I recognise the pattern" – if the person who last used it had greasy fingers, the fingerprint would still be on the glass, so putting something on the glass that doesn't have OTHER fingerprints will force the camera to use the weak fingerprint image still visible to it...

The swipe-type readers are safer in that there can't be an image left on the reader... but many of them still can be fooled by a fake fingerprint made by taking the fingerprint off something somebody touched (lots of how-to's available for that...).

Juergen Nieveler

--

A feature is a bug with seniority.