

# Re: Biometrics

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2008-07/msg00196.html>

---

- *From:* "Steve Riley [MSFT]" <[steve.riley@xxxxxxxxxxxxxx](mailto:steve.riley@xxxxxxxxxxxxxx)>
  - *Date:* Tue, 22 Jul 2008 14:08:51 -0700
- 

You are asserting that one single vulnerability allows "military and top secrets to be leaked" and thus requires the use of some other operating system. You simply cannot make this assertion, for two reasons.

1. NO ONE KNOWS whether your suggested operating system has the same vulnerability.
2. ALL software has vulnerabilities, many of which allow attackers to take control of a system. Establishing good security practices (patch when we release, install only the services you need, apply the principle of least privilege to data, and so on) is MORE important than the particular piece of technology you've chosen to deploy. And the older the software is, the more difficult it is to manage and the more likely it is to get attacked — because older software was not written to be centrally-managed (no group policy and no machine identity in 9x, for instance) and was not written with resiliency in mind.

And this talk of "internal safety" regarding 9x is really nonsensical. Vista and even XP+SP3 are FAR more difficult to attack than 9x was. We at Microsoft have the benefit of about 10 years of historical data from Watson reports (online crash analysis, Windows error reporting). We can divine a lot of information about attacks from this data. Whereas in the past most attacks were targeted at the operating system, this is no longer true. The majority of crashes we see now come from third-party software installed on the box. And in this case, crashes are good: various features in the operating system (DEP, ASLR, SRP, and more) have detected that something malicious is happening, and stop it before the attack succeeds. You could never do that with an OS as simple as 9x.

—  
Steve Riley  
[steve.riley@xxxxxxxxxxxxxx](mailto:steve.riley@xxxxxxxxxxxxxx)  
<http://blogs.technet.com/steriley>  
<http://www.protectyourwindowsnetwork.com>

"Dan" <[Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Dan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
<news:1D0AF19C-B164-450F-92D3-96F6E1E9FDA6@xxxxxxxxxxxxxx>

I see your point Steve but US-Cert maintains that all NT source code is vulnerable thus my point being valid about having 98 Second Edition machines within a network for internal safety reasons and potentially to act as gateways. How can we allow our military and top secrets to be leaked. Please see the United States Computer Readiness Team at the Department of Homeland Security and so you can see how I am getting at the true value of a

Re: Biometrics

source code that is flexible enough to offer external security, internal safety, and more. Thus we have a source code matrix as presented below. I am not skilled enough to write the code for this yet but I bet Microsoft and others are.

-----  
NT= New Technology ---- outer defense network

9x = Internal Safety ---- based upon DOS as maintenance operating system --- lacking in XP and Vista ---- no true maintenance operating system according to Chris Quirke, MVP ---- Vista is indeed great on security issues but still lacks in compatibility as the FAA has mentioned only using Windows 2000 (which I like as well ---- totally old-school reminds me of Windows 98 Second Edition) as well XP machines (which are good but too vulnerable in this day and age due to the large surface area created by too many services and not having strong enough default settings within Internet Explorer --- another reason to separate the browser from Windows like the Justice Department mentioned rightly in the 1998 case although Apple should be investigated now for the practice of tying Quick time with iTunes and I feel this practice of tying software must be banned for safety and security reasons in the future.)

Unix/Linux/Mozilla/etc. ---- third party programs and open source technologies mingling as one with closed proprietary software which is protected by IP. Thank you for continuing this discussion.

-----from us  
cert-----

Vulnerability Note VU#800113  
Multiple DNS implementations vulnerable to cache poisoning  
Overview  
Deficiencies in the DNS protocol and common DNS implementations facilitate DNS cache poisoning attacks.

<http://www.kb.cert.org/vuls/id/800113>

<http://www.kb.cert.org/vuls/id/MIMG-7DPJ7W> (Microsoft NT but not 9x vulnerable)

<http://www.kb.cert.org/vuls/id/MIMG-7ECLCY> (Ubuntu vulnerable)

<http://www.kb.cert.org/vuls/id/MIMG-7ECL5Z> (Apple unknown whether vulnerable)

I am sure you know see that 3 dans ---- 2 on that website and myself another Dan have helped bring this issue to light about how critical it is ---- kind of boggles the mind doesn't it ---- good reason to bring 98 Second Edition and/or another variant 9x/NT/Unix source code ---- on-line ---- Microsoft is

## Re: Biometrics

the only one that has the resources to do this and the whole world now needs your help — Thank You for seeing the Light of our current situation within the Defense Network.

---

"Steve Riley [MSFT]" wrote:

A standalone telephone certainly is secure, and keeps its users safe. For such a phone will never receive or transmit unwanted conversations, and the users of such phones will never be bothered with advertisements, thoughts that challenge their perceptions, or interesting and surprising opportunities.

A standalone computer certainly is secure, and keeps its users safe. For such a computer will never receive or transmit unwanted software, and the users of such computers will never be bothered with advertisements, thoughts that challenge their perceptions, or interesting and surprising opportunities.

No risk = no reward.

The value of a networked system increases as the square of the number of elements in that system. A single system has a value of  $1^2=1$ ; a two-element network has a value of  $2^2=4$ ; a three element network has a value of  $3^2=9$ ; and so on. (Bob Metcalfe, "It's all in your head," Forbes Magazine, 7 May 2007: <http://www.forbes.com/forbes/2007/0507/052.html>.)

Chris's distinction between the Internet and "a network" (presumably private, for Chris doesn't specify) isn't useful today. The network effect is clearly evident on the Internet; I'd argue that in a private network, the network effect is diminished. Why else would we all be rushing headlong into

the eventual recognition that private corpnet truly belong on the Internet, and that continuing to make the distinction means a loss of real business value? (Scott Charney, "Creating a more trusted Internet,"

[http://download.microsoft.com/download/2/f/7/2f752ae4-7e1d-4dbd-b75a-aa2dcb0eff5b/End to End](http://download.microsoft.com/download/2/f/7/2f752ae4-7e1d-4dbd-b75a-aa2dcb0eff5b/End_to_End)

Steve Riley, "Directly connect your corpnet with IPsec and IPv6,"

<http://blogs.technet.com/steriley/archive/2008/06/25/directly-connect-to-your-corpnet-with-ipsec-a>

I quote our own materials here as evidence of the demand from forward-thinking customers that the industry envision new practices and develop new technologies that allow for the full realization of the network effect. Chris's argument that per-user security "creates artificial scopes" doesn't reflect reality. On the contrary, stronger per-user (and per-machine) identity and authentication are critical for allowing the network effect to flourish. Indeed, the lack of strong identity and

## Re: Biometrics

authentication has been a hindrance, and that's why you see technologies like smart cards and TPM chips becoming more common. When we reach the point

where all communications are in the context of validated identities, carried in transactions with integrity and confidentiality protection, between endpoints that mutually authenticate their identities and their configurations, then who cares whether the underlying network is trusted or not?

--

Steve Riley

steve.riley@xxxxxxxxxxxxxx

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

<http://www.protectyourwindowsnetwork.com>