

## **Mad as Hell: I - Switching to Mac**

**Winn Schwartau ([Winn@TheSecurityAwarenessCompany.Com](mailto:Winn@TheSecurityAwarenessCompany.Com))**

This is my first rant written on a Mac. Ever.

Maybe I should have done it a long time ago, but I never said I was smart; just obstinate.

Here's the deal. "I'm Mad! And I'm not going to take it anymore." Of course I am talking about the WinTel world. Before anyone in Redmond or Inteland freak out... well maybe you should. I have had it.

Brief history. I grew up an analog geek. Tubes – valves. Built an analog computer in 1961. Programming in 1966 and on. First home machine in 1974: SWTC with binary switch encoding on the front panel. (Booooooring...) PET in 1977. Trash, too. Compaq, 1981 was it? DOS 1.0 and Lotus 1,2,3 1.0 and I still have the disks. CPM and pip.

Things used to work.

And this is exactly why I am coming to subscribe to the view that indeed, the WinTel hegemony is a threat to the national economic security of any organization or nation-state that relies up it.

In the coming weeks I am going to keep a diary of an experiment that I began in my company at 6PM GMT-5, April 29, 2005.

An experiment predicated upon an hypothesis that the WinTel platform represents the greatest violation of the basic tenets of information security and has become, indeed, a national economic security risk. I do not say this lightly, and I have never been a Microsoft Basher, either. I do not and will not dis any one company without a fair bit of explanation, justification and supportive evidence or experience.

So bear with me as I attempt to document the results of my experiment and I will attempt be fair to myself, my company, our clients and the computing public at large.

I am coming to the belief that there is a much easier, more secure way to use computers. Since I have spent several years focusing my security work on Ma, Pa & The Corporate Clueless, I have also come to the conclusion that if I and my kind (reasonably fluent) are having such problems, what about the other 98% of humanity who merely want a computer for e-mail and multi-media (Porn).

Read the rest of the Mad as Hell series and visit our homepage at the [Security Awareness Blog](#).

**Mad As Hell: II -- How I (And 98% of Ma&Pa) Work**

Even though I am a security guy, my day-to-day work is pretty much like everyone else's. I live on laptops and use my desktops at home and the office for geeking and experimenting. My pair of day-to-day laptops (Mac and Vaio XP Pro) are religiously backed up and so are my business machines. I don't need them to do a whole lot – except reliably work, and that is why I am so damned aggravated with WinTel. (My Dell/Linux is for fun when I have the time, and to determine when it would be safe for OO.o to go Prime Time IMHO.)

Here is why I am annoyed:

1. I want my computer to function every time I turn it on.

WinTel platforms don't work anymore – at least not reliably. More than anything else, I need my box to work. I don't need it to crash while giving a PowerPoint presentation to the Canadian Parliament or the ABA. I don't need Word to crash after writing the last irretrievably 12 brilliant paragraphs. I don't need IE to crash because the memory handling in Windows is so poor.[1] And so it goes with a global litany of crashes that require reboot or memory cleansing every day.

*[1] Do this. Open IE. Look at Processes in Task Manager and see how much RAM is being used. Now open a whole bunch of IE windows and watch the memory get eaten up. Now, close all of the IE windows and see how much RAM you are now using.*

2. I want my computer to not corrupt data when it does crash.

That has happened to every one of us. Nuf said.

3. I use a handful of applications: Microsoft Office

Whether I like Office or not is immaterial. (I do like it, though, or I am terribly used to it.) The fact is that the world uses Word, Excel and PowerPoint.

Open Office and Star Office are getting ready for Prime Time, almost. But there are incompatibilities that would drive the average computer user bonkers. Maybe in a year or so... but not yet. That's why I have a separate SUSE laptop to play around with.

4. I live on the Net. I do not want my browser to eat up all of my memory.

At the end of the day, most e-mail programs have pretty good features. I have always chosen one that is not the subject of endless assault by the 'hackers'. The world, of course, should never use IE or Outlook: they are the prime targets of entirely too many attacks and vulnerable to too many 'oopses' that are really unnecessary. I have chosen [Firefox](#). That's my current religion, and I reserve the right to change my mind whenever I damned well please!

5. My MP3 and video clips and movies should operate every time I click on them,

regardless of format. Hello? What is the problem here?

6. I use FTP pretty regularly.

7. In the WinTel world I have a terrific assortment of 3rd party tools to try to keep my PC alive. That's just crazy. My wife has, out of necessity, turned into an uber-geek-spouse. All she wants to do is write, e-mail, surf & shop, and do graphics. She spends between 4-8 hours per week performing security relevant tasks to keep her machine alive, and it still crashes all of the time. (Didn't the Intel dude just say the same thing?)

8. If I never install another operating system again... jeeez! It's happened to you. CRASH! Reboot is arguably poor. F2 says the BIOS is OK. F8 Safe Boot is indecipherable to all but the technically hearty. Dell New Delhi says "reinstall the O/S". Have you ever done that? Of course you have. But your machine is never the same. It's like laser surgery; you see better sometimes, but not always... and at night all bets are off. The WinTel O/S installation on your PC did not come from the disks they give you to reinstall Windows. It comes from the manufacturer's master build and they ain't the same! Sorry guys, but it's true. A new O/S install is just a quaint way of saying, "Shut up, Customer. It's as close as we can get without having to spend a lot of money to make it right."

That's enuf. For now. But there is more. Later.

## **"Mad as Hell" III - Month 1 Review**

It's May 31 and I've had my Mac for one month. This is my report.

I HAVE:

1. Upgraded OS X from 10.3 to 10.4. I slept thru it.
  - a. Done no OS X configuration other than screen saver and wallpaper. Moved the 'Dock' or task bar.
  - b. No security add ons.
  - c. Upgraded to 10.4.1. Seamless. Painless. But, yes, it does require a reboot.
2. Installed a "legal copy" of MS Office for Mac.
  - a. Macros in Office apps. From everything I have seen and heard from my new 108,745 close personal friends, OS X viri in the wild are simply not a concern. But MS Word macro viri are real, although there is some debate about how much damage they can do in the OS X environment. The MS app default is to advise me on opening docs with macros. I guess I have opened and received more than a thousand docs this month. No alerts. I double checked my settings and gave myself an infected Word doc just to check it was working. All is good.

3. Even though I don't need to, my stomach wouldn't rest until I added anti-virus for Mac. [www.ClamXAV.Com](http://www.ClamXAV.Com). Paranoid habit.
4. I prefer Firefox to Mac's Safari, but that's religion. Camino is the Mozilla.Org OS X specific browser. IMHO, it's not ready for Prime Time. My Intranet displays like crap. Cool features I will watch.
5. I use the native Mail client.
6. That's it.
7. Application-wise I have:
  - a. Edited client movies.
  - b. Made our company switch to free online audio conferencing. (One button. No install. No new software.)
  - c. Switched our company to free video teleconferencing. (One button. No install. No new software.)
  - d. Published PDF. It's integrated.
  - e. Edited and worked on photos. It's integrated.
  - f. Screen shot clips and cropping, etc. It's integrated.
  - g. Imported 40GB of real Office XP data files.
  - h. Moved Favorites and Address Books (yada yada) in minutes.

## I HAVE NOT

Gotten over my security paranoia.

I openly admit I am still nervous. Being a paranoid security type, I tend to STOP and think through many actions I might take or Clicks to Click. I still am, and I notice it on the Mac. "Should I do this?" Oh, that's OK. "What about the security on this?" No worries.

It's a very strange feeling: growing confidence in the security of your platform (equals less fear, less tension, less Xanax). For those of you who think that none of this has to do with security, Part IV will educate you.

T'any rate: I HAVE NOT

1. Added any security applications like pop-up blocker, spyware blockers, anti-spam blockers.
  - a. Saves RAM.
  - b. Less possibility for conflict with apps and OS.
  - c. Less processes.
  - d. Better performance. (None of that slowing down crap, which is a violation of C-I-Availability.)
  - e. Cleaner desktop.

2. Added any other applications, but my measurable productivity is higher.
  - a. Same syntax and spell checker across ALL apps, not just Office.  
(Availability is the security view of Productivity.)
- i. 1 Hr. downtime for a broken computer is the same loss to a business as is 1 Hr less productivity due to lack of homogeneity in the computing environment.
- ii. FACT (or, my opinion...The MS Office for Mac is FAR superior to Office XP+++.  
Things work so much more intuitively once your fingers learn what codes you need.
3. Had any OS X crashes.
  - a. None.
  - b. Nada.
  - c. Rien!
  - d. The bloody thing works as advertised and I am tough on these things.
4. Had an app drive my Mac crazy. You gotta love protected RAM. My browser snafu'd, I Force Quit (roughly equal to CTRL-ALT-DEL End Process) and it's all good again.
5. Had to install printer drivers or tell it where on the network our printers are.  
Smart bugger.
6. Had to perform any whiney networking tricks to make things work as they should. For Ma&Pa this is priceless. (Someone... do a priceless ad for us, please?)
7. Had to spend any additional money on software, utilities, security, upgrades, management or anything else.

#### WHAT I DON'T LIKE

1. That cheap power cord into the side of my laptop. Apple added a little service loop strap which sucks. This puppy is gonna break. I've broken 'em all. Gotta get a backup.
2. Where the hell is the native FTP?
3. Still haven't conquered the mind set of why things become drives or not-drives, and how they appear from time to time of their own volition.
4. The screen on my 17" laptop is not NEARLY as good as my Sony Vaio. There is debate on this, as to the reasons for the 'softer' look on the Mac. My eyes are older than yours, and I really like the 1920X1200 incredibly hi-res on my Vaio. I use the Vaio for some apps... but that will all come out in future Mad As Hell pieces.

5. OH: The keyboard lights up at night. Just too cool and solves a major problem for me and my wife when I 'pute in bed.
6. I DO NOT LIKE having to spend 10 minutes to learn how to do something that is completely intuitive and ingrained in WinTel. But, that is the price. I'll get over it.

GRADE: 'A-': For managing to create a much safer and more secure computing environment that is more productive than any WinTel solution I have seen since DOS 5.0. (DOSTEL).

Think: In the WinTel world, could you do this? Or maybe you should ask, "Do I really want all of that paranoia to go away? Do I really want to spend more time enjoying whatever the hell I do on my 'puter, or maybe I should continue wasting hours every week on security crap that shouldn't be a problem in the first place?"

Hey. It's just a question?

Part IV: Some security basics for Ma&Pa who really need it, and for those of you who need a refresher.

Winn Schwartau

[www.TheSecurityAwarenessCompany.Com](http://www.TheSecurityAwarenessCompany.Com)

<http://SecurityAwareness.Blogspot.Com>

[www.TrustedLearning.Com](http://www.TrustedLearning.Com)

[www.Infowar.Com](http://www.Infowar.Com)

## **Mad As Hell: Part IV - Security Basics for Ma&Pa**

### **Security Basics for Ma&Pa**

Oddly enough: I am on my way from Whistler to New York. Been reading a book, "Hybrids", by Robert Sawyer. (I swear this is purely coincidental.) Page 299, and I quote: "every time her Windows-based PC displayed that blue screen of death, she felt like throwing her support in with Linux crowd. And now it had happened again, for the second time today. Mary did the three-fingered salute but after sitting through its interminable wait for the system to reboot, she found that it stubbornly refused to reacquire its network connection."

The Basics are the Basics

I've been in infosec since 1984, before the Feds tried to tell us what to do with the Orange Book and C2 and all that nonsense which had so little applicability in the real commercial world. And in those 21 years, I believe that the fundamental properties of infosec have not really changed one iota. Not one bit.

As our company is all about security awareness, it is only appropriate that we do cover the basics. No matter WinTel, Mac, PDA, File Folders, the principles upon which

all security should be designed and architected have not changed. The original thinkers were very smart.

In the classic model of infosec there are three components upon which all other aspects are built, much like protons, electrons and neutrons are often viewed as the building blocks of atoms. The classic security triad is based upon these tenets, also known as CIA:

1. Confidentiality: Simply put, keeping secrets a secret. The spy movies call it “Eyes Only” and in a sense that is true. Only those people who are supposed to see the information should have access to it. So, keep it written on paper locked away safely from prying eyes, encrypt it or use access control mechanisms.
2. Integrity: Insures that information is not modified or altered intentionally or by accident whether data or program. Banks really care about this.
3. Availability: All systems and information resources must be ‘up and running’ as per the needs of the organization. Denial of Service attacks confidentiality.

However, in physics we discovered a more basic unit, the quark, and in Infosec, Donn Parker (retired SRI security guru) suggested that we add a few more bits of granularity to make a security model more comprehensive.

1. Control/Possession: Do you remain in control of your resources? A software program can be duplicated without the manufacturer’s permission; they are not in control. You know your password, but who and what else has possession of it? How does that affect security?
2. Authenticity: How can you be sure that the person you are talking to is who he claims to be? Repudiation concepts fall into this category as well.
3. Utility: Say you have an employee who has encrypted data but you do not have the key to make the contents intelligible. The argument is that the data is available but you do not have the use or utility of it.

I agree that these are strong and valuable additions to the Infosec field, but I also believe that they are sub-categories of the first three, which are more ‘quark-like’ in their fundamental-ness.

Confidentiality > Control Possession

Integrity > Authenticity

Availability > Utility

Regardless if you use a hexad or triad as your corporate model, use one of them. These are the basics... no matter what the byte-heads might think. (No offense to byte-heads, of course!)

Winn Schwartau

## **Mad As Hell: V - Is The CIA PC?**

### **Is The CIA PC?**

Now that we all understand and agree on the basics, let's relate that to my concerns about security on PCs, Mac or WinTel.

Yes, I can secure a WinTel box. Well, secure as far is reasonable and practical. Nothing is perfect. One reader said all I needed was a firewall. That's crazy. Sure, my network router has a firewall, and sure my XP box and Mac have firewalls. But please do not make the same mistake at home or in SOHO that Corporate America made in the 1990s.

The non-techy Boss: "Hey, get us a firewall and we'll be secure. Then have Marge in accounting set it up. I hear she knows how to use Word really well."

A firewall, if properly installed, will make you and your network invisible to the bad guys and this is a good thing. But that is a far cry from the kind of security that you need today on any PC.

My concerns that really drove me over the edge did not focus on the issues of Confidentiality. To the best of my knowledge, no one has ever broken into any of my desktops or laptops. Good password practices accomplish a lot. I remember getting one harmless virus in 1995, because I screwed up and forgot to auto update my sig files.

My real issue is with availability. I want my machine to work all of the time. Much of the discussion on this blog has been about traditional security thinking; hacking, viruses, malware, etc., and while tremendously important as part of any Security Awareness effort (lest we get sloppy), I am really not concerned about them for me – albeit still ever a pain in the tuccous to buy and maintain.

To me, this discussion is more about availability as a prime security consideration.

If my screen goes blue ([www.bsod.org](http://www.bsod.org)) I can't use my computer, access my data or my resources. I am out of business until I can reconstitute the system. If my PowerPoint crashes in the middle of a rocking presentation, my audience will be annoyed... but not as annoyed as me. If my O/S bsod's on me, I have to spend time to figure it out and hopefully rectify the guilty party. But that is not a sure thing. (What about Ma&Pa? How many of us had to calm them in some soothing way)

Look at availability (security) from this standpoint:

1. How many times does your OS crash in one month? If never, cool. You're doing something really right.
2. If your WinTel crashes, how much time do you need to spend to repair the crash and rebuild the applications, etc.?
3. When your application crashes (or the OS), how much data have you lost that must be regenerated?
4. How much time does it take to pout things back the way they were?

I know that the answers to this will be all over the place: Bell Curves Rule. You and your PC experience WILL fit somewhere on that curve from "Never a Problem" to "Mad As Hell" and every flavor in between.

Not having access to your machine or your data is a critical security problem for critical infrastructures and is measured in real dollars. DDOS attacks have cost billions. If a bank's systems go down, they know how many dollars per minute they are losing. Availability. If eBay or any Net-based commerce site goes down, it costs the owners lost revenues and profits. So they invest in backup, fault tolerance and redundancy.

A virus infection in a company can bring it to its knees: no availability of the desktops and the network services.

From the PC perspective, it's the same thing.

Ma&Pa will likely not lose millions or even thousands of dollars if their PC fails. But they will lose time. As you will continue to see in this series, the most measurable metric we have in security is Time, and we have developed ways to quantify the Good, Bad and Ugly of computing environments using Time as the prime metric.

Hobbyists, who like to open the case and get under the hood of the OS, decompile apps and tweak the hardware, perhaps don't care about how much time they spend at it. For them, it's fun. I do care.

It ain't fun no more.

Many of my friends and neighbors don't want to waste time on endless repairs. Every business I know cares about availability and recognizes the potential for real losses if the 'A' in CIA collapses.

So, now that we understand that the majority of my issues with WinTel is about Availability and to some degree Integrity when systems go down, I am going to look a bit more at complexification as a key security component.

Winn Schwartau

**Mad As Hell: Part VI - Thinking MacTel**

Thinking MacTel. On an airplane, over Montana perhaps?

I read it too, and I knew about it as a rumor months ago. Hell, this is the Internet!

**REPEAT:**

**1. I do not hate Windows.**

**2. I do not hate Intel.**

**3. No one else for that matter.**

I just said that I felt that Mac was more security attuned than WinTel for all sorts of reasons that we are talking about here. One of the main reasons is that the Mac integration of OS, HW and BIOS provides additional security over the open architecture approach of many different vendors attempting to build to a set of standards.

After years of engineering, I subscribe to the philosophy: Simplicity yields security. I also know that some folks have trouble wrapping their brain around this for their particular needs, and I nod agreement in their general direction. (For the gent who said he has been running NT4 for several years: 1) He admitted rebooting regularly to keep things clean. 2) He also subscribes to my theory of simplicity. See upcoming Mad as Hell rant about this exact issue!)

Nonetheless, I am focusing on the needs of Ma&Pa and those corporate enterprise users who demand reliability, a reasonably headache free experience and perhaps a substantial savings in cost of ownership.

Consider VCRs: Back in the 80s, a battle raged between the technically superior Betamax and the winning yet inferior VHS.

Imagine that instead of purchasing a fully integrated VCR with hardware and software all provided, pre-built by GE, Panasonic, Sanyo... no matter... imagine if you had to pick hardware and the appropriate software from some sales guys at Best Buy. Now, take all of the pieces you just bought home with you and make your new VCR work.

CD/DVD players today. Same thing. Comparatively low-tech to PCs, but the same premise nonetheless.

Palms, PDA and smart phones are purchased fully integrated yet have limited capability (vis a vis PC). However, there is a lot of punch for the fruit juice in there. I always liked Windows CE because it gave me reliable, interoperable functionality with the WinTel world. PDAs? Sure, you can add more, but if you just want it to work for what you bought it for, you can.

Now for MacTel.

Some readers have sent me notes: “You are such a schmuck... see what happened?” Others have said that Apple is opening itself to much of the same criticism I level at the WinTel world. “So there, Mr. Smarty pants! What do you think of that?” Others, more courteous (I don’t play flame games) have asked, “Does this affect your opinion? Did you waste money?”

What I think is this: I don’t know for sure, but I have some ideas and a pretty strong prediction. I switched to Mac and advocate it for many uses for reasons explained. But real questions raise their head:

\* Running OS X on Intel? The underlying OS has run on x86 for decades. There are no inherent problems there. No magic. I also have to believe OS X has long been ported to x86.

\* Will Apple design it right? I hope so. Jobs and Co. have been working on this for years. They have what they claim to be the world’s best OS, yada yada yada, and if I were Jobs, I would NOT want to jeopardize that. He is not stupid. At all.

\* Now Apple will have to support two platforms and two OS’s and possibly two suites of apps. Yup. Pain? Yup. Some people get screwed? Probably. Will I? Nah. My G4 laptop is my office, now. What we all care about at the end of the day is interoperability. My Word or PPT: anyone can read them in most (even Linux) environments. The HW and OS are independent of making file formats interoperable. Not bad guys! Not bad at all. And this is largely Microsoft (for you bashers...)

\* What about old-time users? I don’t know Apple’s policies on that, but from what I gather, there is a certain arrogance the company exudes and some customers get the shaft. (iPOD battery fiasco?) I don’t defend or attack Apple. I don’t care except that I WANT good service. So do you. I want good service for you, but there’s not a damned thing I can do about that.

What about security? Here are my best guesses.

1. Apple will tightly integrate the already proven OS to the hardware – at first. (More later.) If they do this the same way they did the PowerPC and OS X, I would hope and indeed expect them not to screw the pooch. Do it right. Will there be an oops? Sure. Catastrophic? No.
2. The single vendor integration of HW/SW is still superior to multi-vendor specsmanship and home users turning their boxes into doorstops. I stand by that, even though I still use WinTel for some applications. Mac is not everything and not perfect.

In Mad As Hell Part VII, some absolutely, 100% sure fire predictions for 2007.

**Mad As Hell: Part VII - MacTel vs WinTel (2007)**

## Mad As Hell: Part VII - MacTel vs WinTel - 2007

IMHO, 2007 will be a hugely significant year for the evolution, or perhaps devolution, of the PC industry.

Three dramatic events will occur.

Longhorn, or some version thereof, is sorta scheduled to be out. It has all sorts of promises with it, but over its development, many of the promised features have been removed. Understandable! Complexity breeds complexity and this is the last thing the Enterprise desktop or Ma&Pa needs. I really think Microsoft has it all wrong here.

They are adding more features. Color me skeptical. Longhorn is a major rewrite. Adding features to a new underpinning only complicates a trouble free roll out. I don't think it will be trouble free at all.

They are changing the look/feel in many ways; users and Ma&Pa will be learning from close to scratch.

They say they are improving security. Beware of complexity and management issues. In the government, the old 'B' ratings were applied to 'secure' machines, appropriately tested by the NSA. This level was called MAC, or Mandatory Access Control. Each object is 'labeled' (Secret, Top Secret, or Public, Sales, HR) to create isolation between objects and subjects (users). Very cool. Works well. Multi-level security though is VERY hard to manage. You think it's tough now? Hah! Try managing just hundreds of people in a few dozen departments in a half dozen locations, with a bunch of servers, custom applications and hundreds of thousands of files. It's a bitch! A real bitch! Not for the faint of heart. SNAFUs wait at every turn.

While MS is making radical changes to their OS, they could be making existing OS's more robust without SP2 disasters.

Better yet, how about an MS KISS SOS? (Microsoft Keep it Simple Stupid Simple Operation System.) Small kernel. Interoperable office suite applications, an integrated reader that can handle every file format we all use. Sounds like OS X to me, but I think MS could do the same thing – and should.

According to Apple, MacTels will be gushing forth in vast numbers by 2007. I figure it will be an integrated HW/SW approach with more spectacular industrial engineering.

WinTel watch out: Your price advantage just evaporated. If it were me, I would charge somewhat more for the MacTels because Apple could afford to provide the kind of support and service we want. Security and reliability with Apple history? MS has a rep to overcome.

No horrendous security implications for Apple or MacTel users.

I also expect that Apple will release an open architecture version of OS X (et al) in 2007 and tell the Intel PC community, "Go for it" and issue a serious challenge to Longhorn as an OEM OS.

Security ramifications of low-cost MacTel clones? The underlying OS is well tuned and security is built in. Will HW vendors mess it up? How much they mess it up will depend upon the amount of review and technical control (Read Certification) Apple will require. (Read Profit Center). They could well want to have substantial quality control over its partners and the products they produce. Tread carefully.

2007 Event Three: LinTel and some Office Suite become ready for prime time. I know, I know: Linux is God. OO.o is perfect. IMHO, it isn't quite there. LinTel needs to have more experience and a few more major deployments at the desktop.

Given that LinTel is making major inroads to the appliance server market, a strong technical foothold is being built. But that's the geeks. To make it out of the NOC into Ma&Pa's kitchen, though, LinTel still needs maturity, another couple of generations of tweaking and true home user simplification.

The adaptation of LinTel is going to happen. Someone with \$ is going to open this market opportunity with a BaNG!

Stay with me here. My prognostication says, "In 2007, Enterprise and Ma&Pa will have three different viable, interoperable environments from which to choose."

Now, if you'd like, you can argue with me here, but (with no sound basis by which to defend this position) I predict the following desktop market shares for 31 December 2007:

WinTel72%

MacTel16%

LinTel12%

What do you think?

Bottom Line:

What really matters today (and in 2007) is two and only two things!

Security of the platform, its application, its OS, including Availability, reliability and Cost of Ownership. Don't just think crypto and hacking as security. There's plenty more to worry about.

Seamless data transfer between WinTel, MacTel and LinTel. If the data is usable in all of these environments, managers can look beyond the alleged monopolistics and design their environment from a simpler, more appliance oriented and operational viewpoint.

Next in the Mad As Hell Series:

### **The New Security Triad**

Winn Schwartau

[The Security Awareness Company](#)

[Security Awareness Blog](#)

[Trusted Learning](#)

[Infowar.com](#)

### **Mad As Hell VIII: Appliance Versus Theory of Everything**

It's been a while. I have no excuse. Except, my Mac works.

I have not spent one minute (well maybe one) worrying about viruses, spyware or ANY of the usual WinTel crap. I have saved, I figger, in 10 weeks, at least 20 hours of time, not including crashes which means multiples of days.

Last night, in a hotel in Vancouver, I doubled checked my stealthiness, and all is good.

I have been to no less than 2 dozen networks in the last couple of weeks, and I have never needed to configure to them. I have saved at least 6-10 hours of time.

I have lost a few seconds here and there because my fingers still 'think' Windows commands, but that is my ancient brain rewiring itself. I have not used my PC in three weeks.

My PC-worry factor is now next to nil, and that is a strange feeling, indeed! It takes a while to get used to the fact that things just work.

Many of the Linux adapters have it right, IMHO.

Here again underscores the increasing problems with WinTel platforms. As a culture we have been promised that our PCs will do everything for us. They will solve all of our problems, do anything we ask and just keep piling on the functions you want. It will be all right. Trust us. We are geeks.

BS.

We have a tendency to think adding more technology is the answer to solving our technology problems. From a systems and control view of the world this is sheer insanity. It is an especially foolish approach when the vast majority of your customers have just recently conquered push button phones and their VCR/DVDs still flash 12:00.

(BTW: In the security world, vendors are forever saying, “Our new blue widget will solve all of your security problems.” Bull. Remember PKI? \$5M+ and for what? Fortezza? Expanding headers = non scalable. Or the infamous, “Add a firewall. That’ll protect us.” Then they get Sally in shipping to configure it. It IS people, people!)

Let’s say you own your own business. Or, better yet, let’s say I do, which I do: a security company. (Which if you remember, is why I began this long series of rants on why WinTel is a national security threat and a danger to your company)

If I were a one man shop, I would have to do almost everything myself... or, outsourced those things where I am not expert. As a larger company, I hire people who specialize in various disciplines. My HTML is good, but I can’t design graphics beyond stick figures. I can write, but our marketing and PR is done by people who specialize in that. My geek factor gets lower by the week as new technology is impossible to stay on top of, so I have a great team of engineers. I need a lawyer, an accountant... and so it goes.

But these damn computers! Think how much we pile on them to do. Everything.

One of security’s mantras is SPF – Single Point of Failure. If I concentrate too much workload and expectance of functionality in one place, when things fail (which by now you realize will happen) it all fails. At the desktop we add application after application, and expect the WinTel to perform perfectly. It can’t and it won’t.

We add patches to fix old problems. We build perimeters of security and embed them in applications and O/Ss. And all we end up doing is making the system more complex and ultimately, less reliable. It is inevitable.

How are Ma & Pa supposed to deal with this? They can’t and there is no reason that the computer industry should expect them to.

There is plenty of academic support for the thesis that WinTel will continue to fail as long as the current entropic thinking is maintained.

BILL BASH: The other day (mid May 2005) Gates said something like, (paraphrase) “iPod is a fad. Smart phones will take over and iPod will die.” This is the same philosophy of putting everything under one roof, or in one box, that is driving everyone nuts. It’s too much.

I like appliances. I have a phone that works like a phone. No pix. I have a camera for that. No IM. I have a computer for that. If one appliance dies (which they will) I am not SOL. I don’t like being SOL.

## **Mad as Hell IX - Back to Simple**

### **Back to Simple**

The Linux folks say, “hardware is cheap. Build a box to do ‘A’ and another box to do ‘B’ and network them.” I like that. It’s simple, doesn’t require an SPF, and when something fails, I don’t lose all of my functionality.

That’s what was so cool about DOS, too. It was simple, and we got the job done. However, look where we are now! We have added incredible complexity into a basic desktop system that really, simply, is just supposed to do a few things. Microsoft ships with most of its security features turned off. They do this for a very smart reason: it’s easier for them. As we all know, security can all too often hamper functionality. So Ma & Pa could easily think that something doesn’t work, when in fact, a well-intentioned security feature is hindering them from doing what they want to do.

Microsoft is doing the smart thing – profit-wise, and ease of use for Ma & Pa wise, but their decision is one of the great O/S security blunders of all time.

SUGGESTION: Microsoft keeps making their O/S more and more complex to make it capable of doing more and more of the arcane tasks people want to do. Why not define a “SOS” or Simple Operating System that meets the needs of the vast majority of people who buy PCs for simple every day tasks. Get rid of the infinite complexity, and therefore (systems engineering hat on) simplify the interface between SOS, BIOS and hardware.

KISS. You know what it means. KISS SOS. I like that.

Winn Schwartau

[TheSecurityAwarenessCompany](#)

[TrustedLearning](#)

[Infowar.Com](#)

Office: 727.393.6600

## **Mad as Hell X - Security History, Systems & the Failure of Wintel**

The basic security principles of standalone devices (mainframes or PCs) was first published in 1983 (finalized in 1985). Called the Orange Book (TCSEC, Trusted Computer Security Evaluation Criteria), it set the standards by which we need to look at the security of any computing environment, be it an Enterprise or a single box. For my purposes here, though, I will just look at the PC and ignore the network for a while (because IP stacks are pretty darned reliable. God-bless Open Source.)

Although the Orange book is ancient, the current version is called Common Criteria, it is still based upon... well, the Basics... something all too often ignored by the WinTel world, despite their protestations to the contrary.

The Orange Book (et al) created a set of guideline criteria by which security could be evaluated. One of the most basic principles of evaluated security is that once an application, O/S or piece of hardware has been evaluated to a specific degree of security performance, there can be no changes at all. The vendor cannot change so much as one byte of code without having to go through a long and costly security evaluation process again.

Therefore, by definition, every change implies some unknown degradation of the security of the system unless it has been re-evaluated properly. Security patches are often considered a joke because they introduce more problems than they solve. Application upgrades all too often create additional vulnerabilities.

The American approach to security evaluation was superseded in the late 1980s by a European effort called ITSEC (Information Technology Security Evaluation Criteria). They introduced a key concept called TOE, or Target of Evaluation. They recognized that a prime failure of the American TCSEC was that it considered each component of a system (O/S, application, crypto, etc.) in isolation and not as a homogeneous whole. (After all, I am a systems engineer.) In my mind this was a breakthrough that has escaped the attention of PC manufacturers today, thereby **exacerbating** the security problems we face today.

The TOE approach (now included in the modern Common Criteria approach to security evaluation) says to look at the system as a whole; as an integrated unit, with all of the operational pieces glued together as designed for a particular application. Good. I like that.

However, computer manufacturers who integrate O/Ss, applications, utilities, drivers, patches, hardware, protocols, BIOS and more are expected to produce a system that works reliably.

For the life of me, though, I cannot see how they are reasonably expected to produce anything that functions according to my initial specifications in **How I (And Most Everyone) Works**. It's too hard. There are too many variables. And we wonder why we don't have better security and why WinTel fails?

Most of us accept that security and functionality are inversely proportional ( $S=1/F$ ). The answer is intuitively obvious: remove some of the unneeded complexities and give us back some sense of security, particularly availability.

We are only going to compound our errors and make things worse, I chagrin. My cell phone makes and receives calls. It does not GPS, SMS, AES, PDA, POS or anything else that will turn it into a guaranteed failure.

**Mad as Hell XI - Time Based Security**

In 1995 I came up with [Time Based Security](#) as a solid math derivative of an earlier PDR model by Robert Ayers. One of the key assets of TBS was the ability to quantify security with well known metrics and easy to test methodology.

By taking TBS and applying it to the classic infosec CIA triad of Confidentiality, Integrity and Availability, security vendors and security practitioners are using this model as the means to quantify risk using time as the metric.

When any computer fails (in this case I am looking at WinTel), it must be repaired if Availability is to be returned. There are two ways to examine this quantifiably.

1. The amount of time I have lost as a user. If I am the only person using the box, then it is only my time wasted.

a. As a home user this might be your hobby and repairing broken computers is your personal psycho-therapy. (Some of us might just call it psycho, but it's your life.) Or maybe you just want the damned thing to work as it's supposed to. Then you can measure the amount of downtime (D, in time) multiplied by frustration factor (Fr, in # of curse words per minute) to arrive at your personal IQ (I Quit)  
( $D \times Fr = IQ$ )]

b. If you run your own small business, a dead PC can mean a dead business. You might not have the budget for redundancy. Or you are so busy you just want the damned thing to work as it's supposed to. (Sound familiar?) In this case downtime  $\times$  \$/Hr = Total Loss. ( $D \times \$ = TL$ ) Easy to calculate. Make sure you include the amount of time it takes to wait on the phone with New Delli and rebuild the sucker, too. More on that later.

c. Only you can determine this value threshold and then add it to the  $(D \times Fr) + TL = IQ$ . Either way, from frustration or financial loss, you need to determine your own IQ point.

2. The amount of time it takes someone to repair the box.

a. You lose some amount of time and productivity, even if they just to swap out the box.

b. Your company has to either repair it (Time and materials = \$) or send it back to whomever made it, get another and redeploy it. (More time and materials and expenses.)

c. You need to decide your Corporate IQ point. I can't do that for you.

All I can tell you is, during the week of April 18, my IQ point was reached. My wife's IQ point was reached. Our CTO's IQ point was reached. IQ-ism is contagious and self reinforcing.

We all have the same problems. I have tolerated them for entirely too long. I have spent too many hundreds of hours on the phone to Dell Helli. I have installed more O/Ss than I would ever wish on anyone, even John Ashcroft.

## **Mad as Hell: XII**

### **IPv6**

OK, this is sort of geekish, but I will do my best.

The Internet uses a protocol (a common language so computers can talk to each other) call IP or Internet Protocol. Don't even think about getting under the sheets of that one; suffice it to say that over the years there have been many variations of Internet Protocol as it has matured. Today IPv4 (Version 4) is what makes it all work.

The 'new' standard is IPv6 (no one knows what happened to V5, so let dead dogs lie). IPv6 has a whole lot of cool features and security built into it, unlike the naked as a jaybird IPv4. It also has 'an expanded address space'.

#### **GEEK SPEAK:**

An IP address looks like this: 169.131.122.201 and every one is a unique number or address, just like your street, building and apartment number. There are only 4,294,967,296 different addresses in IPv4. In IPv6 there are about 340 trillion, trillion, trillion unique addresses. Loosely translated, that's a whole lot. More than humanity could ever use.

#### **END OF GEEK SPEAK:**

At the end of the day, Ma & Pa don't care about IPv4/6. They only that it fricking works.

The reason I mention it though, is to underscore that the OS X folks do a lot of Future Think about security and I consider that to be a good thing. (In addition to the security features that have been in Unix-like O/Ss for over two decades!) IPv6 is already there, so, IMHO, when IPv6 devices start showing up in homes, cars, appliances, Mac users will just have to plug in a USB cable and forget about it. (READ: The Toaster Rebellion of '08. (GREG: SEE ATTACHED)

No new drivers! No downtime. High availability. No geeking.

Bottom Line: Forget about it unless you really need IPv6 for some arcane reason in the next few years. I was just geeking a bit.

## **Mad as Hell: XIII REPRISE.**

### **Hypothesis: WinTel Has To Fail**

(Some of the bits of this appeared in the NWW article, but this is more detailed as I don't have Susan editing me to 700 words, but after three months, I have found out just how many people agree.)

Why does WinTel have all of the problems it does?

Enquiring minds want to know.

I have seen and heard all sorts of explanations, from both WinTel and Mac fanatics, and I am neither. Regardless, I don't truly subscribe to any of them because the vast majority of what I have seen is evangelistically 'rantish' or the writer has absolutely no clue about security.

Therefore, I had to come up with my own (hopefully rational) reasons as to why WinTel will fail – and has to fail.<sup>1</sup> Worse yet, we have built a society and our national defense upon systems that we know are going to religiously fail for countless reasons; nonetheless I will try.

ALL ABOUT ME: (in brief)

I grew up as a systems engineer in the recording and television industry. That's analogue and digital. Needed to know both. We had both signal and control paths to contend with and they tended to interfere with each other.

We designed, built, installed and maintained incredibly complex systems. Tens upon tens of thousands of color coded wires had to be properly phased and terminated; low level audio, line level audio, speaker level power, video, digital paths, single and three phase mains, and different RF signals had to have proper electromagnetic isolation and filtering. Keeping 20Hz and 200KHz and 2MHz and 200MHz signals from messing with each other is a bitch. Trust me. I missed my honeymoon because the Blues Brothers had a hum in their original recordings due to a British manufacturing problem.

Much of what we had to deal with on a systems level was the subjective beliefs of very famous people like John Lennon, Jimi Hendrix, Led Zeppelin, Liza Minnelli, Chicago and Paul Simon to name a few. If they could 'hear' something wrong, my crews and I had would have to diagnose these complex systems without a reliable technical reference point. "It just doesn't sound right." Our job was to fix it.

Systems infrastructure is easy by comparison. We have measurement tools that simply do exist in the world of pure sight and sound.

So, I tend to look at the world with a systems approach. The answers I am coming up with about endpoint PC security have surprised me.

---

<sup>1</sup> Forget it. I am not going on an anti-Redmond rant.

Let's look at WinTel from that perspective.

1. Windows. Forget about Win2K or XP or Service Pack this or that. Take a look under 'About Windows' and notice that there is a Build number. This means that there are constant refinements to the O/S as part of its evolution. Some small, some large. Which one you get though, is not up to Microsoft; it's up to Dell, IBM, Sony, Moo, or whoever. They pick the version and Build that goes with your machine.
2. Windows. All O/S's are betas. How can I say that? I remember Microsoft saying something like, "We have spent 500 man years testing Win2K..." and that sounds impressive. Except. A new O/S sees, say something like 25 million new users in the first year. There is no comparison between 500 man years of testing with 25,000,000 man years of use and testing. This is not an indictment of MS – it's just a reality. They cannot possibly test every conceivable permutation and
3. combination of hardware, software and configurations... even if it is performed in a constant known and stable hardware environment. It's mathematically impossible, so they have to pick a reasonable point to call it quits and start generating revenue. Real life.
4. When MS releases a new O/S or service pack, there are tons of changes to the functionality. Some of them are intentional fixes and others are upgrade problems. Each release is subject to the same systems problems as above.
5. BIOS. WinTel machines have a BIOS chip that controls some of the basic functions of the machine. There are several manufacturers of BIOS, whom compete with each other. They all try to design to Windows' specifications, but because copyright infringement laws are pretty strong, there has to be different implementations. Ergo: are they all equal? No. Do they all have the same level of compatibility? No, they can't. How much testing can they go through? BIOS firms don't have gazillions in the bank. It's a crap shoot between them and the various incarnations of Windows as to what will happen with the new this driver or that application. Works a lot of the time, but not enough for me anymore.
6. BIOS upgrades. Which version of the BIOS does your machine have and what are the known problems? Who knows. Why does your WinTel crash? Getting the idea here? Systems-wise that is. The user becomes the integrator after the cheap-as-all-hell WinTel PC vendor puts his bits together.
7. Software Applications. Are they well written or do they cheat and take short cuts? Short cuts may work in some environments, but not all, and ultimately the consumer pays in lost time, availability and productivity. Does Buffer Overflow sound familiar? Some of the OS X problems I am documenting run into the same programming glitches.

8. Software Clues. Windows source code is not generally available to the world to poke around in. Microsoft wants to keep its secrets, and therefore (as the subject of many lawsuits) 3<sup>rd</sup> party software developers do not necessarily get the same “under the hood” view or have the experience on call as MS application developers. Try designing a house when you have no idea what the ground is like. The OS X suite is a sweet.
9. Hardware. How many WinTel ‘compatible’ motherboards are there? I have no earthly idea, am not going to spend the energy to find out, but I know it’s in the hundreds if not thousands. They all claim to be better than the next one. Whatever. Some are going to be designed better, with more engineering reliancy than others. Designing to the edge of performance is fine for tweekers and geeks, not Ma&Pa. They want it to work. All of the time
10. Hard drives in any space will fail at near the MTBF: Mean Time Between Failure. Cheap ones fail more.
11. Memory. Not all RAM is equal for either hardware space. There is really good RAM that has clean square waves with minimal ringing (also a motherboard issue) and is specced honestly. Then there is the cheap-ass RAM. It operates at the bleeding edge of reliability and is often the agent responsible for systemic problems in WinTel machines,, but the blame falls to Microsoft. Use decent RAM no matter what.

People blame Windows for everything when it is much more accurate to view the problem as one of systems engineering. What is the best way to glue complex parts together?

- A. Test them individually in as many real-life scenarios as you can. The simpler the system or sub-system, the less that can go wrong and the easier it is to test thoroughly.
- B. Define an integrated system baseline. In the PC Magazine et al, laboratories, multiple performance comparison tests are done using baseline performance specification. This is good. But all we hear in the WinTel world is “Pentium X at Gazillion GHz and SoMuch RAM”. What I don’t see is what concerns me most.
  - i. I have no doubt that OS vendors have a reasonable idea of how their software behaves in certain hardware environments. But what are those idealized set ups? I would like to know. How is cache handled and what the performance hits for RAM, L1/2 cache? I would like to know how that affects reliability.
  - ii. What RAM is used, and how close to the edge is it? The Blue Screen of Death is often lousy hardware blaming Windows.

- iii. The infinity of customizability spawns a virtual infinity of problems or potential failures. No way around that. Simple is as Simple does. Complexity breeds failure and that is why I have become appliance minded. Let TCP/IP do the comm. Work.
  - iv. Real life performance: Software suites, Internet connections, sharing settings, security, etc. We are the guinea pigs by necessity.
  - v. Startup is a nightmare. Every software and hardware vendor is convinced that you want their icons on your task bar, your desktop and sitting in RAM. This is crazy. They have control of your machine and install drivers and TSR programs without your knowledge. That's permission controls gone to hell and a handbasket. If you permit an install, you give up control and your startup
- C. I find it almost amusing that the myriad WinTel vendors out there expect Ma&Pa to be the Systems Integrator. They claim to test. They do. A suite of generalized tests that do not and cannot take into account most of the real world.

Putting on my 'systems integrator quasi-geek' hat is the same as you calling for Customer Service to New Delli or SONY.

"My computer crashed."

"It's Windows, reinstall." And lose data and a full day.

"It's the hard drive. Send it in." And lose data and two weeks.

"It's the motherboard." Send back and wait.

The supposed interoperable open-architecture is the problem! The number of design variables is simply too many to create a long term stable desktop environment. Finger pointing is rampant (blame is always easy to assign; less so to accept).

100 million lines of code to run Office, Email and Firefox is insane. 98% of humanity would be happy with 1 million lines of code that work.

End rant.

**The Ugly About "The Move" – MAH XIV**

1. PC fluent fingers are going to have to learn to walk all over again.

All of those <CTRL> <ALT> commands we are used to are different. Some are the same, but you get an extra <CMD> button so once you get it, there are tons of fast short cuts.

From a security standpoint, this means you will need to be more aware than usual because your finger-memory may do things that do something unintended. I haven't seen a 'bad' thing happen yet, but it is possible. Just a sanity FYI.

Occasionally you will have to sit back, take a breath and spend 5 minutes learning what keys do what when you want to do something fast that is PC second nature to you. What I have found is that once I learn the OSX way, I am pleased... because the method is so bloody intuitive.

2. You will need to think simply.

All of this intuitiveness is non-WinTel. Things happen that make sense.

In the WinTel world I spent endless hours (availability loss) trying to find files, file associations and where things are put. So far, OS X is smart enough to know where the bits and pieces are.

Stop thinking in terms of directories in the PC sense and think of logical data organization from the way you work! I love it.

3. Some things are just frankly different.

“Better” is religion. Different is physics. So far, so good.

I liken it to speaking English, French, Greek and Latin. My brain needs to learn the OS X way of thinking (or the Unix/Linux underbelly and be able to switch back and forth. This is a distinctly non-American way of thinking; after all “We Rule The World” but most global citizens have several languages under their belts. I speak several, and now I have several OS's. Fluency requires use. No surprise.

Same thing with OS X. The context based intuitiveness needs to be programmed into your neurons by use. Believe me, it is so worth the effort.

**Mad As Hell: XV  
PENTINENCE AND CONFESSION – Next to last**

Wow.

I know nothing about Macs and I got invited to speak at the Tampa Bay Mac Users yady yady... and had a great time.

I kept my hair long,, didn't shave and wore an offensive hacker t-shirt that discussed jpgs and a girlfriend. My wife didn't approve but she didn't go, so she lost.

This was really an honor and I started out like this.

"I am too stupid to use Macs.

The other day I was trying to do some music moving with my kids. <Click> nothing. Poked here and there ... nothing. Thought about rebooting (a PC owners knee jerk reaction to anything going wrong, or even if you merely suspect a problem, or if you think you might have a problem sometime in the coming week. Reboot.) But I resisted the urge, under the eternally optimistic experimenter's belief that I would not need to. (This is an experiment after all.)

Instead I closed the app and reopened it. Nothing. Network. Open, reset, close, open, reset, re—enter, advanced, do it over again. Arrghh. Automatically I cursed. "Stupid Mac," and regretted my choice of words.

Got into terminal. Looking for IP packet problems, stack problems, traffic monitoring... and found nothing wrong. So, as a good ex-PC user, I did it all again. I guess I am into this almost 2 hours now and I was really getting annoyed despite the tense smile on my face.

My son walked by. He doesn't even own a Mac. He thinks I am an idiot. He is fourteen. You decide. I asked him if he had any clue what was wrong? The router tables? Firewall restrictions? Port forwarding? I am running the gamut here.

He comes over to my Mac, clicks a couple clicks and checks the "Share iTunes" box.

So who's the idiot? Yeah.

And the point I made to this great audience of senior citizens (and the 82 year old Porn widow), a handful of geeks, some corp types, school board and... yep! Some Apple reps who wanted to see how crazy I was... Oh yeah, the point I made: After battling the WinTel world for 15 years (DOS used to work before that!) I am still overthinking my computer usage and that is a sin.

So in front of the world, I confess my newly recognized sins.

1. I assume the computer is going to fail. There are so many problems, my first reaction is the technology has failed yet again. I confess to this sin.
2. The network is to blame. Other than a lightening strike the other day which did in fact fry the main router, our network is highly reliable. (Yes! I do have UPS and surge protection, but shit happens, OK?) So why do I blame the network? Some WinTel wireless and LAN and dialup networking configurations are a nightmare (read: less than automatic). For some unknown reason I could never decipher, DHCP and other Advanced networking configurations get changed by the office Poltergeist. He seems to have gone away since we switched to Mac. (Saves a bunch of time, I'll tell you!)
3. I have not run anti-virus in over 3 months.
4. I have not run any spyware software in 3 months.
5. I have not defragged.
6. I have only checked the integrity of my firewall 3 or 4 times.

7. I forget that there is an easier way than I am used to. Somewhere, there is a simple button to do 99% of what I need.
8. I still use a PC but will defend it all day long. It doesn't connect to the Internet though, and Sharing is controlled carefully. Sorry folks! I also still use Linux as I watch it prepare for its Prime Time appearance in 2007.
9. I curse the one button mouse, use a Microsoft Mouse and begged the Apple reps at the meeting for free Mighty Mice. They look cool. I also despise the standard Mac desktop keyboard. Boy did I hear about that.
10. We're good now. Mac is my office.

## **MAD AS HELL: XVI – FINAL MAH**

**“It does not take 50 million lines of code to do e-mail, browse the net and write a letter.”**

Winn Schwartau, to the Tampa Bay Mac Users Group, 10 August 2005.

So, at this Mac meeting, we came to a nice conclusion that most of them agreed with: “You Mac people need to calm way the hell down! You are too enthusiastic!” It's like the ex-drug addict who somehow got a prescription for an infinite supply of “I'm Too Happy Pills,” or that former sinning friend who suddenly found religion and just won't shut up!

Mac people, Chill! It's only a computer, and it's only a tool. If you are anthropomorphizing it, you need help. Yes, PCs are good. They have their space, too, so get relax. There is also room for your brother Linux. Get a grip.

Then we talked about “What do you really need a computer for” and other than the octogenarian group-sex and porn addicts, it came down to three things:

1. Email the grandkids and get pictures back.
2. Surf the net for porn and shopping.
3. Word for writing.

That is 95% (ok, pick your own large number) of the world.

**CAVEAT:** “It does not take 50 million lines of code to do e-mail, browse the net or write a letter.”

And I chastise myself for espousing simplicity yet allowing my autonomic reaction to look for the hardest possible solution.

The transition from WinTel to Mac is going to be a lot harder for people with years of PC experience than for newbies. My daughter made the transition in about an hour. Me? I still enter Win codes with my left hand. Gonna take a while and I accept that. Reprogramming the keys to emulate Win hotkeys might be heresy, but it's my box and my life.

**CAVEAT:** Unless specifically compelled otherwise for legitimate and extenuating reasons, all new computer users should buy a Mac. It makes all of our lives easier. (Read: less customer support from geeks to users.)

I am not going Mac religious on you. I am happy and that is what matters to me. But, I get extra thrills and Bonus Points at Heaven's Gate if I try to do good and make decent, well thought out recommendations to the Generally Clueless. (No offense, of course.) Then the selfish part is I receive less tech support calls, so it's not all altruism.

So, I guess I am going to wind down the Mad As Hell series. I had planned to do a lot more, but I am not Mad As Hell anymore. I am Pleased As Punch for all of the reasons I have discussed.

I do hereby declare my experiment a success.

Technically, I will now begin my tweaking of my Mac. I have run native (except Firefox and an FTP client) and will now get more under the hood (WinTel thinking) and see what damage I can do. I will ask for help from the Mac experts out there as I fumble through.

My first goal was to determine if the Mac switch was worth it, and yet, it was unquestionably one of the smartest things I have ever done, albeit late. My tech-stress level is way down. Things just work they way they should. My productivity is way the hell up! I don't have to waste time trouble shooting.

Done. Nuf said.

I have one more major component in the Mad As Hell series that I hope to get out in the next couple weeks.

Total Cost of Ownership. TCO.

I am finishing up a study of the WinTel/Mac TCO and will be publishing it shortly. It will be my analysis plus some tools to let you perform your own TCO, cost-benefit analysis when considering a WinTel or Mac (future MacTel).

Comparative value for Ma&Pa = one set of equations.

Comparative value for SOHO, branch offices = one set of equations.

Comparative value for SME = more equations.

Hope to have them up soon. I am moving my daughter to Paris to attend the Sorbonne, and wife threatened me with the best thing a wife can threaten, that I had better disconnect for at least a week. Will do, honey. Promise.

So figger the week after the week of Labor Day and I'll have the WinTel/Mac TCO Analysis ready for Prime Time.

Adieu!