2007-06
Which User Platform?

Introduction:

It may be obvious, but Windows is for too insecure to be usable by most folks in terms of pragmatic risks to the average user today. So then if we don't run Windows, what do we run? Mac's OSX does a great job, but it's really designed for consumers more than businesses, and Linux, as nice as it is for geeks, doesn't have the full compliment of Windows applications. For most users, there are no other real choices because of the problem of getting support, the ability to run almost anything they find from wherever they find it, and the need to do so at reasonable cost.

Tradeoffs

Risk management is about tradeoffs. We trade other utility, like ease of use, cost, and performance, against safety all the time. Just like we don't build doors for out houses the same as bank vaults, we don't use the highest quality security products for the average user. And just as most city folks have locks on their doors and lock them most of the time, most Internet computer users should have some security measures in place on their computers and use them most of the time. None of the security measures make you “safe” or “secure”, but all of them trade utility of use for utility of safety.

What are user platform tradeoffs today?

Today, the tradeoffs of utility in the form of ease of use, availability of support, and cost leave most users with three choices. Windows (Microsoft), OS-X (Apple), or Linux (lots of them). Here are the basic issues with each of them:

- Windows is so insecure that most normal users cannot realistically use it for more than a few days on the Internet without it being broken into and exploited repeatedly by malicious attackers. It crashes a lot, is hard to configure and use, and it is the most popular environment on the planet.
- Linux is relatively safe in that it is rarely broken into in normal user uses, but configuration is a nightmare, ease of use is poor, and support is complicated. It almost never crashes, but it is not very popular or consumer friendly.
- OS-X is almost never broken into in normal user use, it is relatively easy to use and very easy to configure, it almost never crashes, but you have to reboot for most updates, and it is well supported.

It seems like an easy decision – and it is!

I am not dogmatic about technology. I have no religious ties to any company or operating system, and my views have changed over the years as the operating environments have changed. Nobody is paying me or otherwise remunerating me for my point of view. If you would have asked me two years ago, I would have told you something quite different, and in two years things are likely to change again as will my opinion based on those changes. Furthermore, I am giving you the same advice I give to my wife and children, who are pretty much average computer users today.

> ***Apple running OS-X is the clear operating environment of choice today, especially for notebook computers.***

I want to be clear on this, so I will take a bit more space. Apple is not more secure than Linux or Windows in the sense that it is harder to break into. With roughly the same amount of effort, I can break into any of them. But it is easier to secure from essentially all of the things that actually happen today as you roam the Internet.

The most important reason for Apple's relative safety is that it is less popular. If you are a professional criminal, which most computer attackers today are, and you have so many dollars to spend on attacks, would you spend them attacking 1/20th of all the computers in the world when you can get 90% of the computers in the world by attacking Windows? You wouldn't, and they don't. OSX is not popular enough to get heavily attacked yet, and this makes it safer for those that go there – for now.

The relatively low density of Apple computers in the global computing population also makes them harder to sustain computer viruses and worms. Individually, they are all susceptible, but because of their lower population density, the epidemic threshold for infectious diseases is higher and it is harder to write a successful worm or virus for OSX. The time to cure will generally not need to be as fast as it is for Windows in order to prevent epidemics, which means that as users you don't have to work as hard to win most of the time.

Conclusions:

Most users who care about security should buy Apple instead of Windows for their normal use. Most security professionals today likely use Apple when they can.

To configure it more safely, you might go to all.net and look at the article on how to configure and use it securely.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 97, section 36.1.2 we present:

"People tend to reciprocate any gifts"

> *"...even a meaningless gift will create an obligation... biases them subconsciously."*

No matter how honest you are, and no matter how small the gift, some level of obligation is present. But interestingly, the refusal to take a gift in return will cause resentment. Thus the exchange of gifts when a gift is given is not only a social pleasantry, it is necessary in order to stay on an even keel. This newsletter is free, and we will not offend you by refusing any business you send our way to achieve social parity.

Section 6.3.1.3.1 (page 186), "Say no politely – buy flowers instead" tells us:

> *"... You can say no politely..."*

Actually this section is about a different issue, but it still applies to gifts and reciprocation. You can either reciprocate with a pleasant gift of similar value, or you can politely refuse the gift. When I used to work for government, I told people that as a government worker it was against the law for me to accept gifts. As an analyst I can't lean on regulation, but I do refuse even the smallest gifts from those I review.

Chet's Corner

I am finally starting to come to believe that, in the long run, security is a hopeless cause. We all die.

> *"Nobody gets out of here alive!"*

So security is not about the long run, it's about the short run - or the medium run? Somehow the notion of long-term security strategy seems senseless. Yet, the Chinese and Japanese have multi-generational views of the world. So those with a short-term view of security fail in the long run, but win in the short run? Hmmm... I think I have to think it out again.

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's our vendor consulting practice:

You might think that it is controversial for supposedly independent experts to work for vendors in the space they give independent opinions about. It is. But most so-called independent experts do it. And so do we. But we also take precautions to make certain that we are not influenced, even indirectly, by the fact that these companies pay us. Just to be clear:

> Apple has never paid me in anything and we don't have any other such arrangements.

What we do for vendors is give them confidential independent outside opinions, review their marketing and sales material from the viewpoint of analysts, executives, and users, and provide custom research and development services. They don't always like what we have to tell them, but they pay us to be honest and confidential, not to tell them what they want to hear.

As an example, one major vendor had a new release they were going to put out that would have affected tens of millions of computers all over the world. They had spent tens of millions of dollars in development and were coming up on deployment when they decided to ask us to evaluate the safety of what they were about to do. At the end of the day, they decided to not deploy this new innovation because the risks exceeded the rewards. They wished the results were different, but at the end of the day, they agreed with them and made the tough business decision.

Mollie gets the last word in

I'm going to South America for six months soon, and my dad insists that I get a security briefing. So he goes to the CIA Web site to get the really scary stuff, and comes at me with a spiral bound 25 page book on the specific countries and cities I Will be visiting!

Now, I know that my dad loves me, and I appreciate that he is watching out for me, but is the CIA really going to post it on their Web site if they are planning an overthrow?