

- There will be increased disruption of personal computer operations. Already office conversations contain talk about apparently abnormal events on home computers. At one time these events were attributed to plain bugs. Now the conversation is likely to blame the problem on a “virus”. As our home computers become more important the fear of being “virused” will increase.
- There will be more disclosures of previously private information from our own personal computers and those that are owned by doctors, hospitals, schools, and governments. The protections today are minimal. With a bit of social engineering as discussed by Mitnick one can obtain a password that divulges almost all that is a key to an individual’s identity.
- Systems that report on the shipment of packages will be violated and information provided to thieves.
- Credit card systems will be disrupted to the point that they are not trusted.
- Cell phone digital and voice messages will be intercepted.
- Cell phones will become targets for SPAM.
- Networks and systems used to operate the public infrastructure will be disrupted.

As these events and more begin to happen there are a couple of possibilities in my opinion.

- One possibility is anarchy among governing bodies. For instance the state of California recently enacted laws against SPAM that look like they cover all SPAM in the world. However, California does not have authority all over the world and indeed California is in a deep budget and political crises. The California laws should likely be national.
- Another possibility is that national leadership could arise and start a program much like the Apollo project that led us to the moon. We could recognize that the production and deployment of quality software is as important as the auto safety or airline safety efforts.

**Is there a technical problem?** Can computers and networks be secured? This is a research topic today. It is clear that networks and even individual computers can be attacked. Most of us can name ways of attack computer systems. These ways range from sophisticated worms and viruses to plain old social engineering which was the subject of a book by Kevin Mitnick (reference).. What we cannot discuss because we do not know is the barrier that will prevent attacks with any degree of certainty.

Computers are in fact more vulnerable than people to biological viruses. Even the most devastating biological virus will not attack 100% of the people. Over time, without any intervention some number of people will be immune to attack and over time vaccines are routinely developed that spread immunity. Computer viruses and worms will be able to infect and harm 100% of the vulnerable systems that are exposed.

The technical problem might be able to be attacked, but there are social barriers:

- Schools need to offer a modern and fast changing curriculum, but processes to change the educational plans are slow. For instance, changing the catalog within a department can take 1.5 years and changing courses across departments can take several years.
- Even if schools could change plans fast training tenured faculty and getting them to keep up with fast technology changes is difficult.
- Our observation is that the best software houses often build product for themselves. Those that build software products are often driven by unreasonable schedules that compromise quality and testing. Note that the largest software suppliers tend to have many updates to correct vulnerabilities. Recently Apple Computer withdrew a release due to flaws that were apparently not caught during pre-release testing.
- The battle between Microsoft and Open Source advocates may be destructive. Microsoft likely has the funds to make significant strides in building better software and the Open Source advocates may be among the best constructive critics, if the sides chose to talk.
- Those schools with the best programs are technically elite and likely superior. The problem is that much of the world's software is developed by people who do not attend these programs...
- The ACM has taken a position against licensing software engineers as professional engineers. However, the ACM has not suggested a better program. The position of the ACM will likely delay any software developer qualification program.
- UCITA, or the uniform computer information transfers act, the set of rules that govern software sales limits the liability of software vendors. UCITA removes many of the financial incentives for producing quality software.

With software becoming more important and the forces that could create better software teams in disarray the likelihood is that the problem faced by society will become worse before it is better. What are some of things that are likely to happen?

## Clouds on the Horizon for Computer & Network Security

Almost every week or perhaps daily there are new stories of hackers wrecking havoc with some computerized service. The number of attacks measure in the hundreds of thousands and the damage is considered to be many tens of billions. The trouble with the picture is that the problem of computer security or lack thereof is not peaking, but rather getting worse.

**What's happening?** Is the computer virus really a biological virus that is taking over the world faster than the plague? I contend that the problem is even worse than the plague that devastated cities and geographic areas.

Computers and networks of computers have become as essential to human activity as electric power. Recently much of the East Coast of the US was without power for up to 120 hours or the better part of 5 days. During this time much commercial life in the areas affected just stopped. If the nation's computer grids were down for a week much commercial life and even civilian life would go back to the dark ages. I don't even remember the last time I purchased gas with cash or even with a credit card that was handled manually.

Some months ago I was in a major grocery store when the credit card processing system failed. There was no paper backup. A loud speaker blared out that credit card purchases were not being processed until further notice. My guess is that if this problem lasted long that between 50% and 80% of sales would be lost.

**How big is the problem?** At this moment each virus or hacker attack gets attributions in the millions or billions depending upon the side effects considered by the publisher of the incident (add some quotes to this). The risk is actually much greater than spreadsheet numbers. If you remember back to the gas crises of 1974, the US was for a few months paralyzed. US citizens are used to a free flow of gasoline at fairly low prices compared to the rest of the world. Most of us do not think twice about driving from place to place. Suddenly after the beginning of the oil shock of 1974 gas lines were long. There were restrictions on purchasing gas depending upon your plate number. What had been expected to be always available was suddenly absent. The effect of the gas crises was a change of life style that lasted years.

Today in the US and indeed in most of the developed world we are more dependent upon computer networks than we are upon gasoline. Power, water, airplanes, goods of all types, money movement, identity checking, and about every facet of modern life is dependent upon computer to computer interaction. If our computers and networks suddenly become clogged for any considerable time then our current life style would be disrupted. Banks no longer have sufficient teller staffs to hand out money. There are no longer sufficient gas attendants to take cash. Manual credit card verification systems are no longer trusted or available.