

Crusts, Patches, and Soft Spots

By Stephen Cobb, CISSP

We at Volkswagen believe that on the road of life
there are passengers and there are drivers.
Drivers Wanted.

It would be nice to think that, as this seminar-to-end-all-seminars comes to a close, I could come up with a set of wise and accurate predictions about the future of information assurance. However, in the past I have been burned by predictions. Don't get me wrong, I have actually predicted a number of things that have come to pass, but very few of them came to pass within the timeframe that I predicted. As Will Shakespeare, my historical neighbor¹ from the old country would say, therein lies the rub. To be of serious value, security predictions have to get the timing right or they are about as useful as me telling my wife, about a year ago, that the stock she inherited is bound to go up soon. One day it might, but right now she's still waiting for "soon" to arrive.

The Privacy Driver

One of my more successful predictions was that privacy would emerge as a driving force in computer security. At the end of 1999 I wrote an article titled "Today's Security Drivers" in which I suggested that this was already happening.² Over the next 18 months privacy started to make the front page of most major business and



¹ Shakespeare grew up in Stratford-on-Avon which is 18 miles from Coventry, where I was born and raised. In the sixteenth century, Coventry, with its powerful merchant guilds and massive city walls, which had an impressive twelve gates, was the closest big city to Stratford. There is even a rumor that Will was caught poaching on the grounds of my alma mater, King Henry VIII School.

² Cobb, S (March 2000). "Today's Security Drivers" Business Security Advisor Magazine, archived at <http://2cobbs.com/help/art-secdrivers.htm>.

consumer publications (this was well before the shocking events of 9/11/01, the government's response to which led to even wider debate over privacy and privacy rights).

In the summer of 2001, the Federal Trade Commission brought this prophecy to very real fruition when it chose to act on a complaint lodged by the ACLU against pharmaceutical giant Eli Lilly for revealing, in June 2001, the email addresses of people receiving email from prozac.com.³ As it turns out, I was one of the experts to whom the FTC turned when it tried to decide if this incident was a security breach. Based on the evidence, much of which was made public, I argued that it was. I also proposed some of the remedial measures that the FTC imposed in its settlement with Lilly in January of 2002.

When a number of parties complained to the FTC in 2001 that Microsoft's claim that its Passport identity service offered superior security, I was not involved in the FTC's deliberations. However, the remedial measures imposed on Microsoft were patterned upon those in the Eli Lilly case.⁴ The same was true of the Guess case, in which it was alleged that Guess did not use reasonable or appropriate measures to protect consumer's personal information against "commonly known attacks."⁵

Predictions and Arguments

Journalists love to get experts to predict the future. Over the years I have learned, rather sadly, that grim predictions are the best bet for a security expert, at least in terms of coming true. Nobody wants to be the expert who said, in any given year, including 2003, that the virus threat will soon diminish. So I have tended to stick with a tired but trusted line: "It is probably going to get worse before it gets better." I think I said that about boot sector viruses in 1992, about macro viruses in 1995, Java exploits in 1996, spam in 2002, and so on.

So when Dr. Peter Tippet stepped up to the plate and agreed to write the final chapter of *Computer Security Handbook, 4th Edition*, he had my sympathies. I had faced a similar challenge in 1996, when I came to write the final chapter of what was then called the *NCSA Guide to PC & LAN Security*.⁶ Of course, that is the same NCSA that became ICSA then TruSecure, of which Dr. Peter Tippet is CTO. Indeed, for a period of time back then, Dr. Tippet was my boss. So it is somewhat fitting that I now draw attention to one of Dr. Tippet's earlier ideas, an idea with which I took issue in that final chapter.⁷

³ See <http://www.ftc.gov/opa/2002/01/elililly.htm>.

⁴ See <http://www.ftc.gov/opa/2002/08/microsoft.htm>.

⁵ See <http://www.ftc.gov/opa/2003/06/guess.htm>.

⁶ Cobb, S (1996). *NCSA Guide to PC & LAN Security*. McGraw Hill (ISBN 0079121683).

⁷ Cobb, S (2001). *Cobb's Guide to PC and LAN Security*. iUniverse (ISBN 0595181503). Chapter 15 is available online and free of charge at <http://cobb.com/pclan/pclan15.pdf>

In 1996, Dr. Tippet was looking forward to the day when computer security would be taken care of by persons/agents other than the owners/operators of the computers. This approach has a lot of merit and we have seen a big surge in recent years in both “managed security” and “self-healing systems.” However, one of the most important lessons I have learned about developing information security products and solutions is that timing is everything. I wrote my original security book in the late eighties and back then it seemed that diskless workstations were, from a security and system management perspective, a great idea. The book came out in 1992. The product that I had highlighted as an example of a diskless workstation disappeared. Then Oracle’s CEO, Larry Ellison, announced the thin client network station about the time that the 1996 edition of the book was coming together.⁸ How could I go wrong this time? I was sure the security advantages of this approach would eventually gain traction.

However, perhaps aware that the remotely managed, easy-to-use, appliance-style workstation would take some time to emerge, I took issue with Dr. Tippet’s assertion that users should not have to worry about security. I was concerned that too many computer users, and owners, were abdicating responsibility, rather like people who drive without checking the tread on their tires. I was, and still am, keen to get across the notion that a computer user is a computer operator, and things might have gone better if ‘user’ had never replaced ‘operator.’ Indeed, it is my recollection that ‘user’ was coined for users of dumb terminals, as opposed to the people who operated the computers that fed the data to the terminals (as someone once observed, computer companies and drug traffickers are the only two categories of retailer that routinely refer to their customers as ‘users’).

If the hundreds of millions of people who today “operate” powerful and autonomous computer systems were actually using terminals then we’d all be a lot safer. But the fact is we have hyper-threaded, multi-gigahertz systems selling for less than \$1,000, often packed with hundreds of megabytes of RAM, tens or even hundreds of gigabytes of storage, sitting on megabit-per-second connections to the global network, operated by Junior, who, at 11 years of age, probably lacks a fully developed sense of personal responsibility.

This is like letting teenagers drive without lessons or a permit. And the automotive analogies don’t end there. I’m not sure how far back your memory of cars goes, but back in the fifties, when my father went to work in the mornings, the probability that the car would start was a lot lower than it is when I head out of the door today. This does not just reflect the fact that I grew up in England. My wife tells me that her father, just like mine, would take the family car to the shop for service before any long trip. Recently, I watched my daughter get in her car and head off on a 2,000 mile round trip without even thinking of lifting the hood.

My point here is that over the last half century cars have steadily moved closer to a reality that was talked about as long ago as the fifties, a car so ‘maintenance-free’ that it frees the driver of

⁸ “Oracle unveiled its Network Computing Architecture for the “thin client” concept today with support from over 40 companies.” CNET, October 1, 1996, see: http://news.com.com/2100-1001_3-233603.html.

any mechanical responsibilities. Sadly, the maintenance-free, care-free computer has not yet arrived. And even though cars today have warning lamps to tell us when a lamp is burned out, or a tire is low, it is still the responsibility of the driver not to drive unless all lamps are working properly and all tires are properly inflated. In the world of information systems we have not yet reached the point when we can relieve the individual of the responsibility of proactively protecting systems from abuse. While conceding to Dr. Tippet that managed security is a worthy goal, I did, and still, assert that we are not there yet.

People and Products

The future of information assurance rests with people and products. I've talked about products, but what about the people? Like many of my colleagues I believe that the human race needs a massive dose of computer ethics training. We need to start the computer ethics education early and repeat often. And we must continually endeavor to counter the still too common misconception that system abuse is cool.

Sadly, corporate America makes ethics education difficult to discuss with a chorus of derisive laughter. The moral example set by over-paid C-level executives is appalling. I'm not just talking about the theft and fraud and slimy accounting, but the moral tone. When a company is convicted, under the laws of the land in which it is incorporated, of being a monopoly, it is unseemly to find it arguing overseas, several years later, that it is not (yes, that is a reference to Microsoft). The rampant absence of shame and contrition in the corporate world makes the task of teaching Junior to respect the intellectual property and cyber-space of others that much more challenging.

Also hard on information assurance, and hard to swallow, is the established fact of a computing monoculture. The emergence of any monoculture would be a risk factor, but fact that the one we have is riddled with holes and drowning in patches only makes it worse. So, in late 2003, we have the ironic situation of the world's leading operating system and application vendor making a public admission that it cannot keep its software secure, and as a result is looking to perimeter security to save the day,⁹ while other business leaders are calling for the de-perimeterization of networks.¹⁰ This echoes the concerns raised in the early days of firewalls, when it was feared by some (such as Simson Garfinkel) that firewalls would be an excuse for not making networks as secure as they could, or needed, to be.

⁹ "A growing feeling among security experts at the software giant is that a new strategy of better securing the edges of networks might ultimately better protect the numerous Windows systems found within those networks. This strategy, called "Securing the Perimeter," is now a core tenet of Microsoft's wider Trustworthy Computing initiative, and it will affect all IT administrators and decision makers that use Microsoft products." Windows and .Net Magazine, October 21. See <http://www.winnetmag.com/Windows/Article/ArticleID/40590/40590.html>.

¹⁰ "Users needed to build borderless global networks where security was built into the network, rather than just at the interface between the internal network and the outside world. This technique, known as de-perimeterisation, said Simmonds, "promises to reduce cost and aid business." From the article "IT chiefs call for security rethink." Computer Weekly, Tuesday 28 October 2003. Article announces a call to industry by Paul Simmonds, global information security director at chemical firm ICI and David Lacey, head of information security and governance at Royal Mail, to move beyond the limitations of network perimeter security, at the RSA 2003 security conference in Amsterdam. See <http://www.computerweekly.com/articles/article.asp?liArticleID=126003&liFlavourID=1>

Mr. Garfinkel's fears appear well-founded when you consider the way many people think about firewalls: as network security. In fact, almost all firewalls currently deployed provide inter-network security, and most of them, Internet security. In a conversation back in 1996, Mr. Garfinkel argued that workstations, and the connections between them on a network, could be configured securely, such that an outsider, coming from an untrusted network (i.e. the Internet) would find no resources or services open to abuse. This might have been true when most networks were running UNIX or Novell under the control of a savvy sysadmin, but those days are long gone (if they ever existed). People have been putting in firewalls while overlooking internal controls, leading to the "crusty on the outside, soft on the inside" state of much system security today.

Conclusions

I am duty bound to end on a note of hope, the possibility that advances will be made in information assurance, at least at the product level. Let me return to the automotive analogy. Studies have found that slowing traffic down from 80 mph to 30 mph for ten minutes is far better for overall traffic throughput than bringing all traffic to a halt for even 30 seconds. So consider what happens when you take to the motorways of the UK and some other EU countries. On a good day, in the right place, you have multiple lanes of fast moving traffic, all of it monitored by camera from command centers. When something goes wrong, the emergency response is often under way before anyone on the scene has called it in. And traffic flow control signals immediately begin slowing down the traffic to avoid it coming to a standstill. Central monitoring of traffic flow, combined with appropriate application of flow controls, helps traffic keep moving even when some things go wrong.

A couple of technologies that appears to be a step in this direction are TCP/IP traffic shaping and sFlow. In simple terms sFlow is an emerging standard for network traffic sampling and analysis.¹¹ An international, multi-vendor and end-user forum called sFlow.org is promoting the benefits of sFlow sampling technology for monitoring and managing traffic in complex networks. The positive security potential is considerable.¹² Quite independently, my former colleagues at what is now TurnTide arrived at traffic sampling, coupled with traffic shaping, as a means of combating spam and other email threats. While this technology operates at the perimeter, it could also operate both internally within a network, and externally, on a backbone. It turns out that sampling traffic and analyzing the sample "out-of-band" is more efficient, and can even be more accurate, than making message-by-message or packet-by-packet decisions about what is good or bad network traffic. When bad traffic can be identified, and its use of resources controlled, the effect is to suppress bad actors while clearing a path for good actors.

¹¹ See <http://www.sflow.org>.

¹² Reves, J. and Panchen, S. (2002). "Traffic Monitoring with Packet-Based Sampling for Defense against Security Threats." See <http://www.sflow.org/SamplingforSecurity.pdf>.

So is there hope for information assurance? Here is the final paragraph from that final chapter I wrote back in 1996:

“How can you summarize a subject this diverse, in a world that changes so fast, in a paragraph that needs to be kept short? At the end of the day, I am optimistic that honest people, armed with good intentions, bright ideas, and a prodigious amount of useful information, eventually will prevail in the struggle to keep computer-based information as secure as it needs to be. However, it will be a struggle.”

Note the optimism, plus the careful hedging of bets in that very vague word: eventually.