

# Ten years in the wilderness, part III: Diogenes on the threshing floor



Richard Power

Dario Forte

By Dario Forte and Richard Power

The Greek philosopher, Diogenes, walked the streets of Athens, carrying a lit lamp in broad daylight. He said he was looking for an honest man. But, of course, Diogenes wasn't really just looking for an honest man; he was offering truths that only an honest man could embrace. Diogenes belonged to the Cynic school. They taught by example and used their own lives like lamps that radiated meaning. Well, on assignment at the 15<sup>th</sup> annual RSA Conference, traversing the exhibit hall, pacing the back of the hall during the general sessions and trolling the conference rooms during the break out sessions, we saw a lot of people who should know more about the product they're selling, and a lot of other people who should know more about the product they're shopping for. But we also saw some truth-sayers, who like Diogenes, are looking for someone honest enough to embrace the truth about cyber security.

## E-commerce disguise

It is poignant that the last movement of our three-part retrospective on the past decade (1996-2006) should be focused on the RSA Conference. A decade ago, the RSA Conference was only one of numerous cyber security conferences. It started as a small gathering of cryptographers and was very technical in nature. Over the years, it developed into an E-commerce show disguised as a security conference. But now, by attrition in the marketplace, and its own natural evolution, the RSA Conference has become the main event. Its exhibit hall is the industry's threshing floor.

How many of these exhibitors, we wondered, would be here again next year? How many of them were here two years ago? Except for four or five giants (their banners hang the highest, and their booths have the best positions), there seems to be little continuity from year to year.

Meanwhile, some of the brightest minds and strongest voices are still

crying out in the wilderness – moving from caravan to caravan, and leaping from one stepping stone to another just before it disappears beneath their feet.

This month, in the final installment of our retrospective, we will share our experience at RSA with you, and ask three big questions of some very knowledgeable colleagues we bumped into, wandering like Diogenes on the threshing floor.

## Man of the year (again?)

It was disorientating to see Bill Gates up on the big screen at the opening general session of the 15<sup>th</sup> annual RSA Conference, held recently in the heart of Silicone Valley. Had we stumbled into the wrong event? Then we remembered, "Oh yes, he has done it for three years in a row." Here are four truths about Bill Gates and Microsoft:

- Microsoft perceives its customer to be the developer, Apple perceives its customer to be the end user.

The difference in philosophies is profound, and results in profoundly different products.

- Only one US corporation that existed in the year 1900 still existed in year 2000: General Electric (GE). But in the year 3000, there will be two still standing: GE and Microsoft.
- Bill Gates belongs on the cover of TIME Magazine - "Man of The Year" issue for 2006, standing alongside his wife and rock star Bono, honored for humanitarian efforts throughout the world
- Bill Gates does not belong in the role of keynote speaker at a major cyber security conference. Certainly not for three years in a row.

We would have been more impressed if we had found Gates and his numerous development teams in the front rows madly scribbling notes and listening to people who really have something to say about cyber security. So we ask some of our colleagues, astute and experienced cyber security professionals, what they would say if they had a microphone and Gates and his team were, indeed, sitting before them in rapt attention.

Their responses proved insightful.

## Microsoft

### Rik Farrow

Rik Farrow ([www.spirit.com](http://www.spirit.com)) has been a leading Internet consultant and trainer for many years. He is also one of the best writers on the cyber security beat.

This is what he would tell Bill Gates. "Windows, like most current operating systems, suffers from insecurity in

depth. The operating system itself is enormous, and executes with privileges that make it easy to exploit. The next version of Windows (Vista) will deal with a small part of this issue by moving some device drivers out of the kernel. But that still leaves a huge body of code at the mercy of ever more sophisticated attacks and rootkits. The other aspect of insecurity in depth comes from Microsoft's legacy code. The recent Windows Meta File (WMF) patches dealt with code written over a decade ago as part of Windows 95. While Microsoft has done much better writing new code, and has performed automatic checks on old code, the majority of the code in current systems was not written with security in mind. Most applications use libraries that include this old code. And with most desktop users working with Administrative privileges, any exploit of this code results in a system exploit. Thus, the trusted code base includes the myriad DLLs and software libraries included in today's applications, producing insecurity in depth.

Unless and until Microsoft redesigns their operating systems to support the execution of insecure code, we can expect to see the same routine of critical patches to Windows code. I don't expect Microsoft to give up over a decade's worth of legacy code, so they must learn how to execute old code, and third party code, securely."

### Gene Schultz

Gene Schultz, who is now Chief Technology Office for High Tower ([www.high-tower.com](http://www.high-tower.com)), founded the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) and, while at Lawrence Livermore National Laboratories, he co-founded the Forum of Incident Response and Security Teams (FIRST). He also taught at Purdue University's CERIAS (Center for Education and Research in Information Assurance and Security) and at the University of California at Berkeley.

Here is what he would tell Bill Gates: "I'd tell him that although Microsoft products have gotten quite a bit better over time when it comes to security, Microsoft still has a long way to go. Microsoft's Trusted Computing Initiative (TCI) was a giant step forward, something that has earned a great deal of respect among security professionals such as myself. At the same time, however, too many security-related vulnerabilities, many of them serious, in Microsoft products keep emerging. And despite new solutions such as the Windows Update Server, keeping Microsoft systems properly patched is still too hard because of the sheer number of vulnerabilities, the need to boot after patching in most cases, and the fact that some of hot fixes are not as stable as advertised.

### Fred Cohen

Fred Cohen ([www.all.net](http://www.all.net)), formerly of Sandia National Laboratories, and currently a senior analyst with the Burton Group, has been an innovator in computer virus defenses, information assurance and deception.

"The fundamental problems with Windows security stem from the business model at Microsoft. The approach is to give the gift that keeps on giving - or in the case of Microsoft - sell the software you have to keep on buying. Security takes time and focused effort. When you keep changing the architecture, you keep rewriting code, and you have an increasing code base that, among other things, fails to use the same routines to do the same things in all places. For example, file creation in Microsoft sets a wide range of different file creation dates, presumably because each routine chooses a different initial date. This may seem like a minor issue, but it means that a program that looks at file subsystem dates and times within an OLE file to rebuild a routine (like the make command does) ends up with date and time stamps that yield the wrong dependency relationships and can

result in an improperly built routine. This is quite subtle and may only have an impact under some strange condition that is rarely encountered or not anticipated by the people who write the program analysis engines that do compilation. In order to have a secure environment, you need to also have a mature environment. Mature code bases can improve with age, and well thought out detailed designs with consistency in mind are necessary for a higher surety level result. This is directly at odds with how Microsoft makes money, which is by selling the operating system to its user base year after year. It would be foolish of Microsoft to give up the revenue stream, and security weaknesses are unavoidable in this context.

"The other important thing to understand about the Microsoft environment is that the more established team members have spent their careers taking short cuts and not doing things in a sound and secure manner. This is reflected clearly in the writings they produce to tell the world how to do it better. For example, "Writing Secure Code (version 2)" tells us that inside Microsoft, a typical decision of how to determine whether denial of services could be used against an Internet interface is to run more random vectors through code to test how long it might end up running rather than to analyze the complexity of the algorithm. In practice, they think that more testing can replace better analysis, but attackers have historically been willing to analyze the complexity of algorithms to determine the worst-case input sequence. When they do so, unless the testing happened across it, which is highly unlikely, the operating system will grind to a halt. It is endemic within Microsoft that the most senior people are not well educated in the issues they need to understand to address security concerns, and that starts at the top. We all know that Gates himself is chief architect and never graduated from college. While the wild and woolly days of the

80s and 90s were important to the creation of the current computer industry, the long term goal has to be stability and reliability rather than ever increasing and rarely used, poorly designed, and not fully tested or analyzed components racing to win the time to market challenge. As areas mature, deeper knowledge is the only path to success. Until the whole organization comes to embrace in-depth knowledge and well thought out design, Microsoft will never produce a secure anything. “

### Keith Rhodes

Keith Rhodes is Chief Technologist for the US General Accountability Office (GAO), and has directed some of the U.S. federal government's most important studies of critical infrastructure vulnerabilities and other security risks produced over the last decade.

Here is what he would tell Bill Gates.

“I would say to Bill that Microsoft Press publishes the works of Steve McConnell, who, I think, is one of the finer observers of the foibles of software development. I would suggest that everyone in Microsoft have all of Steve's books in their personal library and that they read them and that they manage their software to the suggestions he makes in those texts. I think that if Bill and his team were to clearly see themselves through the lens of McConnell's guides, they would either have to start writing good code, including testing it prior to release; or they would have to be willing to announce to the world that they do not really care if it works or not, as they view the person who buys their code as being a developer of their product, and, therefore, subject to all the flaws and miscues that go with product release. I would think that if one is the market (e.g., Microsoft), they could pause for a moment and decide to build some code the right way — even if it is a side development in parallel to the main product line. I would also clarify for Bill that there is a difference between asking a buyer for

suggested improvements to a product and making the buyer fix a broken product.”

### One step forward, two steps back?

The next question we asked this fearsome foursome concerned progress over the last decade, vis-à-vis the technical dimensions of cyber security: one step forward, two steps back? Is there forward momentum or are we backsliding?

### Rik Farrow

According to Farrow, it isn't as if cyber security is backsliding, it is more like it is sliding forward into the muck.

The biggest change in the last 10 years, in Farrow's view, is the shift from attacking servers to attacking client software.

“Ten years ago, you used firewalls to limit attacks to particular services on servers. But, today, the method of choice to get inside an organization is to send emails that will exploit a user's mail-tool. Today's attackers will compromise a Web server and install exploits that will be downloaded onto vulnerable Web browsers (WMF again). So while public facing servers still get exploited, the bulk of exploits are against client systems.

“One reason for this change is that client systems often have great bandwidth, lots of processing power, and poor administration, making them useful to the owner's of botnets. As recently as 2001, DDoS attackers targeted UNIX systems, because they were fast and well-connected. But advances in technology have made desktop systems better targets, and security of the desktops has not kept pace. Virus writers build on past viruses, creating ever more complex and harder to detect viruses. Payloads have become better at hiding as well. And exploiting desktop systems today produces real ‘rewards,’ in terms of theft of passwords, credit card numbers, and identity information.

“A large part of the security industry focuses on band-aids —firewalls, virus scanning, and various intrusion detection schemes. The worst of these are virus scanners, as they are an admission that today's desktop systems cannot be made secure. Microsoft has decided to cash in on their own inability to produce secure systems by selling anti-virus support. Microsoft has admitted that their bestselling software cannot be made secure, and will be taxing users for band-aids to keep the desktops limping along.

“Walking the exhibit hall at RSA 2005, I was impressed by cool new hardware designed to work at ever faster network speeds, blocking the old, well-known attacks, while attempting to filter out new attacks, often unsuccessfully. The attacker has the advantage over the defender, when current operating systems are fertile ground for infection. “

Why? Farrow faults computer industry as a whole, not just the security segment.

“Our current model of computing was born back in the late 60's, when timesharing became popular. In that model, programmers designed operating systems to protect users from each other, and the operating system from users. Today, users must be protected from software that the user herself runs (the mail-tool or Web browser, for example), and that same user will often have sufficient privileges to both patch and compromise the operating system. This model stopped serving us more than 10 years ago, when single user computers were becoming the norm. Today, the vast majority of systems have single users, and most servers function with just a handful of user identities.”

### Gene Shultz

Gene Schultz has a positive view of progress over the last ten years. “Over the last decade the practice of information security has improved somewhat— we have definitely made some progress. Back in 1996, for

example, firewalls were new and were often looked upon with suspicion. Firewalls are now commonplace. The same can be said for intrusion detection systems and other useful tools. Laws such as SoX, HIPAA, Gramm-Leach-Bliley, and FISMA have forced organizations to take their security practices more seriously. Vendors such as Microsoft have had a definite shift with respect to how serious they take security. I'd also be willing to bet that if someone looked at the International Security Forum benchmark data over the last decade, there would be a marked improvement in the use of security countermeasures and practices. So, overall, despite the fact that it doesn't come easy in the information security field, there has definitely been some progress over the last decade.

### Fred Cohen

Fred Cohen's assessment of technology trends is somewhat less encouraging. "Over the last 10 years, the vendor community has embraced the eternal fees perspective on selling security stuff, while the industry is calling out for more secure software rather than more security software, as Phil Venables once said. 'The sell it first, fix it later approach has continued to avoid the liability issues that led long ago to government imposed safety mandates and the implied warranty of sale for automobiles. But this situation cannot continue forever.'

### Keith Rhodes

Keith Rhodes questions people's grasp of the task at hand. "I do not think that people understand defense. Defense doesn't show; it isn't headline news. Thus, it is hard to make the work attractive; it is hard to even make thinking about the work attractive. For Rhodes, there is too much focus on product and not enough on the fundamental building blocks of security itself.

"People don't seem to understand that security is based on vigilance and

diligence, not on a product or standard or vendor suite. You have to be aware of what you are protecting, and you have to know what you are protecting it against. You have to know how long you have to protect it, and at what cost. Vendors don't offer that kind of knowledge; it's not off-the-shelf. We have lost ground relative to people thinking about their own roles in security. Otherwise, we would not outsource everything for off-shore development."

Rhodes also emphasizes the interpenetrating challenges of securing both the physical and virtual worlds.

"There are no boundaries in a virtual world, but the physical world still has demographics and battle lines. I do not think that we are ready for the marriage of the physical and virtual worlds. In the film 'Being There,' Peter Sellers points his TV remote control at a young gang member and tries to change the channel. When will we know that it is no longer impossible? What will security mean then?"

## Trends in security technology

Where are we going? What new trends in security technology show promise? What new trends in security technology spell trouble?

### Rik Farrow

According to Farrow: in the future, we will see faster, smaller, and better connected devices.

"Cell phones already have wireless connectivity and immense processing power. But the security of cell phones today relies on closed systems — something that has failed spectacularly. Wireless networking has already made it difficult to secure an organization's perimeter, but portable wireless devices will make this increasingly impossible to secure. Your Windows laptop will automatically connect to any AP that it finds, especially if it has a SSID it has seen before (Linksys anyone?). As we move forward, with more

network-enabled devices, this will only get worse.

Farrow believes we need a new paradigm for moving forward securely.

"The old method of using firewalls to protect the soft and chewy internal network has little meaning as networks become ever more interconnected, and wireless access becomes both simpler and faster. If you examine the past 10 years, you can see that we are still using passwords, and our networking technology still revolves around just getting things to work (DHCP for IP addresses, DNS without digital signatures). Given the inertia I see today, it is hard to imagine the industry, and not just the security industry moving forward. If anything, we have a large special interest group who would lose money and market share if things do get better. But there are signs that this will change. What will begin forcing the change is the number of people who have stopped using the Internet, as they get tired of paying for anti-virus software that doesn't stop infection, animated pornography advertisements and spyware. This is beginning to happen now. The time for band-aids has past. We need a new paradigm for computing, one that makes good on the promise of the now-ancient Orange Book — that a trusted system can securely run untrusted software. We are working on this problem today, and with any luck, we may once again have computers that are both secure and fun to use. "

### Gene Shultz

Schultz sees both good and bad on the horizon.

"On the good side, I am confident that regulation and compliance considerations will continue to have a very positive effect on the practice of information security. Identity management technology is particularly hot at this time; it will not be long before a large percentage of organizations adopt some kind of identity management solution. Intrusion prevention technology will get considerably better over

the next few years, leading a growing number of organizations to adopt this very potentially useful technology.

On the dark side, however, it will only get darker. Watch for malware that 'does it all,' i.e., requires no intervention from perpetrators and hides even better than today's malware. Watch for new, previously unimagined financial rip-off schemes.

Unfortunately, many users who thought they had learned their lesson when they fell for previous schemes will prove otherwise by falling for these new schemes. We have seen only the tip of the iceberg when it comes to unauthorized access into databases that store personal and financial information.

### Keith Rhodes

According to Rhodes, we are going towards total integration and device convergence.

"The only limiting factor at the moment is the need for a screen and keyboard, but once the virtual screen is deliverable and the voice-control is working acceptably, then you will

become the device. With smart fabrics (not network fabrics, but clothing fabrics), there will be nothing that is not connected; we will all be the podcast. What worries me is the same old security trend of putting bandages on the wounded operating system or database or application. As we converge the devices and the applications, many more cracks will appear in the wall, and the attacker will be just water finding a way through the small cracks."

Rhodes stresses the importance of awareness and education.

"Security education is the only one thing that I see that will help us now, or in the future. People will have to understand that most of what is emailed to them is junk, just like on television, or in their physical mailbox. They will also have to get clear on becoming more and more part of the mesh, or the grid, as we accelerate toward the ever-present, all-pervading network."

### Fred Cohen

And Cohen sees progress in terms of awareness and education.

"The inattention to security education is starting to reverse – more and more funding to universities is being applied to improve security education.

Although there is still a long way to go, it is starting to head the right direction. In 25 years, we will reap the real benefits of this positive trend." Ten years in the wilderness. Two steps forward one step back. Where will we be in another 10 years? It is up to you. Be like Diogenes. Embrace the hard truths, and you will shed light wherever you go.

### About the authors:

*Richard Power (www.wordsofpower.net) is an internationally recognized authority on cyber crime, terrorism, espionage, and so on. He speaks and consults worldwide. Power created the CSI/FBI Survey and his book Tangled Web is considered a must.*

*Dario Forte (www.dflabs.com) is one of the world's leading experts on Incident Management and Digital Forensic. Former Police Officer, he was Keynote at BlackHat briefing and lecturer in many Worldwide recognized conferences. He's also Professor at Milan University at Crema.*

# The convergence of physical and electronic security

Dr. Andy Jones, Security Research Centre, BT, Adjunct, Edith Cowan University



Dr. Andy Jones

**People have always been concerned with their physical security. But security of information is a more recent phenomenon. Both types of security have been traditionally disparate. But with physical security moving towards electronic mechanisms - surely both can be converged? Dr Andy Jones discusses.**

We are constantly being told of the benefits and problems that have been associated with the convergence of computing and telecommunications technologies. The 'new' technologies are increasingly giving both the individual and organizations the

opportunity to achieve greater efficiency, to achieve what had previously been thought to be unachievable and to enjoy a better quality of life.

One side effect of this technological evolution and the growing maturity of

the information technology security industry may be seen in the convergence of physical and electronic security, in relation to the technologies that are used and the way that they are utilised and the disciplines and procedures that are implemented.

### Separate

The measures taken to achieve physical and electronic security have, historically, in the main, always been treated separately. Physical security, which includes the protection of buildings, equipment, people and information has been undertaken throughout recorded history and there is a great deal of experience and knowledge as to the best way to carry it out. In addition to this, physical security is ubiquitous and affects us all in every environment, from our home to our