Foreword

It is my privilege to say a few words about this book, words I mean more as an aperitif rather than a tasting sample.

Financial services firms were the first non-military sector to pay attention to information security. They have long been, and are likely to remain, the avatar for all other civilian sectors. If you look at finance, you can generally see the future. There are several reasons why this is so.

While the first is the most pertinent it is perhaps the least relevant banks are where the money is. But money does not make money unless it moves, and so move it does. The bigger the bank, the greater the percentage of its business is done with other banks, an oddity not found in other industries (Ford does not buy and sell GM cars) with the minor exception of some small parts of the energy market. The chief trading partners for major financial houses are other major financial houses, thus predisposing banks to take digital security seriously their counterparties are also their competitors.

What banks buy and sell is risk, which likewise predisposes them to understand risk or, more correctly, to engage in risk management. Risk management is inherently forward looking, as best said by Borge: "The purpose of risk management is to change the future, not to explain the past." Changing the future is hard, but somebody has to do it and, as always, two things help -- a prepared mind and good cash flow. Banks have both.

Finally, banks have and do pay attention to digital security because they don't actually make widgets or even stockpile widgets; they move bits. While bits are bits, some bits are more important than others and bits are not naturally self-protecting. When the system is digital, its failures are binary.

Paleobiologists like Gould see evolution as "punctuated equilibria" which is to say long periods of stability interrupted by short periods of rapid change. Evolution, as they describe it, is not some steady upslope at 8% grade, but rather the unexpected when least expected and then a flurry of change that will eventually damp itself out enough to be called progress, as if anything that brought us to where we are must have been progress since this is the best world yet made.

The risk management we need might therefore be understood as (1)the ability to maximize the damping effects of stable periods of risk and (2) to be prepared to handle the punctuating events of the definitively unpredictable, the latter being what Taleb famously called a "black swan."

Can we look back and see a few of these sorts of episodic catharses? Of course we can. Every transformation of the computing world has been a surprise, one that removed the reason for existence upon which its predecessor depended

and which was later superseded in like manner whatever followed. The first computers were rare, expensive, and they made redundant legions of folks who once worked out tables of logarithms to nine digits by hand. Time share destroyed the market for stand-alone behemoths, and desktop PCs destroyed the market for time share. Today, software as a service (SaaS) looks poised to destroy the desktop PC. At each stage, the best X ever produced was also the last X ever produced as it was itself rendered irrelevant by the leading edge of the next phase. As the son of an accountant, I saw this first hand; my father had the finest Frieden mechanical desk calculator made, it was mechanically programmable -- a thing of beauty -- and yet the lousy Bowmar Brain made mechanical desk calculators irrelevant. You can surely name example after example of the same phenomenon -- that of a kind of equilibrium punctuated by the end of the environment on which the most evolved members of that environment depended.

To the biome, to the occupier of a niche that was here yesterday and will be gone tomorrow, change is a surprise. No tree can say "Time to move" and no salamander can think "I need to evolve." Evolutionary change depends on this unpredictability; otherwise yesterday's winners are tomorrow's winners, yesterday's dominant species only get more dominant tomorrow. As Grove said, only the paranoid survive.

Note that "change" is not a synonym for "disaster." Just as some pines have cones that only open after they've been burned in a forest fire, opportunism as a counter to disaster is something we can see in our world -- today and every day -- in that for every backdoor some worm or virus installs, you can bet your paycheck some other bit of malware is soon searching for the self-same backdoor for its own purposes. A backdoor unused is like a biological niche unoccupied; Nature, both biologic and digital, abhors a vacuum -- that backdoor will get used, the only question being by whom or what.

In the natural world, a high presence of attack pressure must and does result in a high rate of mutation. What part of your body suffers the most daily insults and thus mutates all day, every day? The E. coli in your gut. Their mutation rate rises and falls in relation to stress since if things are going well a mutation is likely to be deleterious whereas if things are going badly it may well be a last chance and, in any case, reproductive fidelity is more metabolically expensive than producing mutations. A withering digital attack ought to provoke some adaptive mutations in the target whether we are talking of a single executable or an industrial sector. Put differently, if you are losing a game you cannot afford to lose, try changing the rules.

I define complexity as the density of feedback loops. A lot of people say that complexity is the enemy of security -- I'm one of them -- but at the same time I am here to argue that we have to learn from Nature precisely because Nature is the most complex "thing" we will ever see. Nature is an existence proof that complexity is not the enemy of life, but complexity is the enemy of stasis. Our problem is that we've pretty much equated security with stasis, and it is slowly getting us into trouble. Take forest fires -- if you always quench them, such as to

protect vacation homes and tourist dollars, then you necessarily build up the supply of unburned fuel wood in the ecosystem and someday you get a much bigger fire. If you let any and every fire burn, someone who can vote will lose. If you prevent any and every fire, you look smart and life goes on, and predictably so... until it doesn't.

If we look at Nature in the form of the equations of ecology, we see two alternative games for survival, r-selection and K-selection. R-selected species produce many offspring, each of whom has a relatively low probability of surviving to adulthood. By contrast, K-selected species are strong competitors in crowded niches, and invest more heavily in much fewer offspring, each of whom has a relatively high probability of surviving to adulthood. If we change the term from "produce many offspring" to "re-image frequently" you now have precisely the advice Microsoft's D'Anseglio gave when he said, "[In] dealing with rootkits and advanced spyware programs, the only solution is to rebuild from scratch. In some cases, there really is no way to recover without nuking the systems from orbit." This brilliant remark is a direct, if inadvertent, suggestion that desktop machines need to be r-selected, i.e., they need to die and be re-born often. If you are of a mind to invest in virtual machines, you may get r-selection as a side effect to whatever it is that you are trying to do with VMs.

I trace the security industry as we know it today to one of Gould's punctuations appearing as one of Taleb's black swan events, but one in relatively slow motion compared to, say, the Witty worm. Specifically, I trace the birth of the industry in which most readers earn your keep to Microsoft's introduction of a TCP/IP stack as a freebie in the Windows platform. Besides putting FTP Software out of business, a tactic followed so many times that I have literally lost count, the TCP/IP stack took an OS designed for a single owner/operator on a private net, if networked at all, and connected it to the world. Once that stack was installed by default, every sociopath became your next door neighbor and, as such, we can point to that event as the birth of our industry, confirmed by a sudden, one-time-only, wholly dramatic spike in that second derivative of the rate of attacks reported to the CERT immediately following that appearance of a TCP/IP stack on Windows. Note that I said a spike in the second derivative; nothing much else happened for a bit but, similarly, lighting the solid fuel on the Space Shuttle doesn't have any instantaneously visible effect either.

The second of these equilibrium punctuating moments occurred, as far as I can tell, some time around 24 months ago. Like the first, it was no thunderbolt, more like a glacier finishing its slide across a river bed and thus "suddenly" damming the waters. This moment was when our principal opponents changed over from adventurers and braggarts to professionals. In a sense, professionalization of the attack class is akin to virulence in that the increasing immunity of computer systems forced an upgrade in the ability of the attacker to attack, i.e., finding vulnerabilities and exploiting them is now hard enough that it has moved out of the realm of being a hobby and into the realm of being a job. This changes several things, notably that hobbyists confirm their successes with public kills and share their findings so as to claim the bragging rights in which they

are paid, whereas professionals do not share and are paid in something more liquid than fame. Speaking biologically, a mutation (toward strength) on the part of the prey was matched by a mutation (also toward strength) on the part of the predator. As a side effect, the fraction of all vulnerabilities that are unknown has risen and will continue to rise.

We have yet to reach the post-punctuation equilibrium in this cycle. The mutation toward strength represented by professionalization of the attack class was not a simple, compensating match for the increasing self-protection in merchant operating systems. It went further and it did so because, at least for the first world, the digital arena is now clearly where the opportunities are, such as that when robbing banks it is the amateur who uses a hand gun and the professional who uses a bot.

In the fall of 2006, I did some back of the envelope calculations that resulted in a guess that 15-30% of all desktops had some degree of external control present. I got a bit of hate mail over that, but in the intervening months Cerf said 20-40%,Microsoft said 66%, and IDG said 75%. It doesn't matter which is right; what matters is that this changes a core feature of the ecosystem -- and changing a core feature is the very definition of a punctuating event.

In this case, it actually was not standing up a professional class of attackers any more than in the first go 'round it was a spike in the second derivative of the reported attack rate. What it was, was that a fundamental assumption of network security has now been breached and there is no putting it back together again.

Ever since we did Kerberos, the idea has been "I'm OK and you're OK, but the network between us cannot be trusted for a second." Authentication, authorization, and accountability all begin with authentication and that, in turn, begins by asking the Operating System the name of the user. What has really changed is that it is no longer true that "I'm OK and you're OK" since it is entirely likely that the counterparty to whom you are connecting is already compromised. A secure network connection? Who cares if the other end is hosed? Spafford was right but early when he likened network security to hiring an armored car to deliver gold bars from someone living in a cardboard box to someone sleeping on a park bench.

That is the new security situation you and we are facing -- what to do about 0wned counterparties. This is a today issue, not a tomorrow issue; the November 2006 10-Q filing for E-Trade included a material loss due to exactly this problem, the first SEC filing of this sort to my knowledge. 0wned machines mean key loggers and key loggers mean opponents who can get you to help them in the pump phase of a pump & dump stock fraud, whether you like it or not. If and when you ever bother to call your broker to complain that this or that purchase was not one you did, the broker has two choices: "You are an idiot." or "We'll make it up to you." Such a situation is untenable, and indicative of the need to evolve.

If, by chance, you think the professionals aren't winning, just consider that

they now value stealth over persistence, i.e., they find it so easy to 0wn machines that they make no effort to survive reboot, preferring instead to hide in-core only. Consider this the equivalent of gene therapy as prescribed by Dr. Faustus.

At the end of the day, however, we are facing a much bigger, more metaphysical question than the few so far posed. The bigger question is this: How much security do we want?

How much security do we want is the real question, and while Nature can give us more clues than we can ever use to improving what we puny humans can do, we are fast closing on a point where the question we must ask is whether we wish to turn over our security to sentient machines. Within the career lifetime of nearly everyone reading this Foreword, computers will be smarter than we are. Security is already the most difficult intellectual profession on the planet. The core knowledge base has reached the point where new recruits can no longer hope to be competent generalists, serial specialization is the only broad option available to them. Computers will soon be called upon to do what we cannot, and that is to protect us from other computers, and to ask no permission in so doing. Every practitioner can tell some story where an insane affection for convenience caused people for whom you were nominally responsible to create, or at least tolerate, insecurity and to be offended if you endeavored to make them see that light.

The next punctuation of the equilibrium will therefore be the effective end of the general purpose computer as a consumer durable -- as presaged by Apple dropping the word "Computer" from its name or leading Wall Street trading firms already going back to displays only on the desktop and no PCs at all. Software as a Service, or temporary periods of invasive remote-control of the client-side machine by the server-side counterparty,or apps on hand-helds that only run because they are perpetually connected to back-end processing -- all of these are the leading edge of the next equilibrium punctuatum. Yet, if you do not have a general purpose computer, with which, to paraphrase Felten, you have the freedom to tinker, then I ask you what kind of security will that be?

Karlos Krinklebine, in inviting me to write this Foreword, proves Gibson's idea that the future is already here, just unevenly distributed. Krinklebine shows you that the second epoch of information security is over and he and his colleagues are well into the third. The tour of the combination battlefield and sausage factory which follows this Foreword asks many of the questions that are part of this next moment of punctuation, the ones that derivatively follow professionalization of the opponents and which will soon endeavor to make the general purpose computer less general. He is a front-line soldier in the war, and war is hell. He knows what he is talking about and, which is more, he, too, hates the circumstances that make the distasteful necessary and the necessary distasteful.

Much more than myself, he is showing you how the sausage is made. He is walking the perimeter of the financial services network world with you so that you can judge not so much the how of what must now come but rather the why. "Why" is the only real source of power, without it we are powerless, and you would

be well advised to pay attention. Lamport's witticism, that "A distributed system is one on which I cannot get any work done because some machine I have never heard of has crashed" is even more true of that most distributed of all digital systems, financial services. Though Krinklebine apologizes for the occasional technicality
he must describe, no apology is needed unless, of course, you don't want to know "why" or even "how," you only want to be protected. That has never been a good bargain for a sentient being, but then again only a sentient being will likely read this book, or want to. My compliments to you for getting this far.

Daniel E. Geer, Jr., Sc.D.
April 2008