Why tolerate mediocrity?

anonymous

November 18, 2007

This essay examines the reasons why mediocre security products beat the good ones in the marketplace. We review the conventional economic wisdom regarding why this might happen, then discuss what is special about the market for security products. We then show that, (a) consumers are conservative, not irrational, and (b) the situation with security products is not unique. Next, we propose an explanatory model for the security products market that takes hidden variables and inertia into account to provide a coherent view of the seemingly contradictory market behavior. Finally, we analyze the impact of this model on producers and consumers in this sector and give suggestions for how efficiency can be increased overall.

The conventional basic assumptions of economics are that producers and consumers are rational and they act to optimize their own interests. Producers are free to determine how they produce, what they produce, and what they charge. Consumers are free to choose what they buy and from whom they buy it. Everyone knows everything and products are valued accordingly. Producers and consumers converge on the parameters of their deal, and business takes place.

In the simplest model, producers understand what their customers want and what they will pay, and consumers know exactly what they want and can easily assess whether the item being sold to them will satisfy their needs. This is far from reality when it comes to selecting security products.

The real-world market for security products deviates significantly from the simplistic ideal market model. The consumer does not usually have a clear specification of what he or she needs and producers often do not provide a complete description of what can be expected of their product. There is often a long delay during which a product appears to be effective, only to fail later. Indeed, there is somewhat of an adversarial, or at least distrustful,
relationship between the producer and the consumer. The consumer is typically not given the opportunity to view the source code of the product. This results in a situation where a black box is offered for sale, take it or leave it. The fact that security is difficult to measure has a profound effect on the market for security products.

Consumers might seem irrational, given that they continue to buy products with poor performance when better-performing products are available for the same money. Generally they are not irrational, but are acting rationally when three relevant factors are considered. First, experimentation has cost. Trying an new product requires taking time to learn about the product and how to integrate it with the existing system. Second, experimentation involves risk. Unless an isolated testbed is available for product evaluation and testing, the new product will be tested on a live system. If things go wrong, real data, real processes, and real people will be affected. Third, since consumers lack a clear specification of what they expect from a product, they will not feel confident in the new product even if it performs well during testing. They can never be sure that they have tested all of the functionality they will be depending on later. In a nutshell, when dealing with security, it is rational to be conservative, even when it appears almost superstitious to an outside observer.

In many cases a free, open-source product appears on the market after a commercial product already exists and has a foothold. Typically the open-source product will be touted as being more secure in addition to being free. Customers, particularly military and financial ones, are not overly eager to switch to the open-source product. The reason is that they are risk-averse. They might be fully aware of the mediocrity of the product they are using, but it is a known quantity, a not a source of uncertainty. It is like a mountain climber choosing his rope. One rope will hold 500 pounds for sure, and the other rope might hold 1500 pounds but it also might break with 400 pounds. Most climbers will take the first rope. Risk-averse decision making exits in many areas. Millions of individuals choose to pay for health insurance even though the expected payout on any given year is much less than their insurance premium. The decision does not revolve around the expected cost/benefit ratio, but rather the worst case cost/benefit ratio. To summarize, consumers in many areas will accept a mediocre product if they feel that it shields them from uncertainty. This is really nothing more than saying that a bird in hand is worth two in the bush.

To explain why mediocre products are successful in the market, a model
is needed that accounts for inertia and aversion to risk. We assume that the consumer is rational, and understands that his knowledge is limited, both of terms of his needs and in terms of the efficacy of the products on the market. He must maintain “functional coverage” which is to say that choosing not to consume is not an option. For example, a firewall is considered necessary functionality for a corporate network. There is freedom to choose which firewall, but there is no freedom in whether some firewall will be used. Our model states that the consumer acts to minimize surprise. This can be viewed mathematically in terms of a decision tree. The consumer makes his choices today to minimize the expected surprise tomorrow.

The market for security products is in a bleak state. Very little standardization has taken place, with crypto algorithms being the one notable exception. (Of course information security is much, much more than just cryptography.) Advancement in technology is normally motivated by the prospect of economic rewards, but becomes frustrated when the market prefers inferior technology. Fear, uncertainty, and doubt is a technique that is usually used by producers in the technology sector to scare their customers away from exploring alternatives. Ironically, in this same sector, fear, uncertainty, and doubt has overtaken many security technology producers. The sector has become conservative, making only incremental improvements on existing products, and devoting more energy to locking in their existing customers than to attracting new customers by developing radical innovations. Customers need better security. Engineers and researchers have new ideas, but many of these new ideas don’t get to market because of producers cannot predict how the new product will be received. It is a loss for everybody.

To improve the performance of the security market, standards are the first step. For example, a core set of PC antivirus functionality could be standardized. When standards are in place, security can be measured objectively in terms of compliance. When security can be measured objectively, innovative products can distinguish themselves based on other attributes like convenience and performance. Consumers can know what they are shopping for in terms of which set of standard functionality it provides. Producers can be reasonably assured that if they provide the standard functionality at a good price, they have a good chance of achieving market acceptance. This would be a win for everybody.