How Secure Are Lemons?

Since hackers have evolved into such sophisticated creatures over the years, there has been an upsurge of security products in the market. These products range from antivirus, firewalls, and intrusion detection software. Of all these products, how many of them are effective? How can end users determine the effectiveness? Why are so many mediocre security products outselling the ones that seem to work better? The general problem seems be the fact that there’s a lack of perception as to where the security risks actually lie by users and manufacturers alike.

At the bottom corner of many e-commerce websites there is a logo stating that they are protecting their customers with 128-bit encryption. When most individuals are asked what does 128-bit encryption mean they might say “I don’t know it’s more than what I can count with my fingers.” In any case, having that logo on the webpage makes the customer feel safe when shopping online. Data security is still an unknown territory for many consumers big and small. When purchasing a security product, the consumer falls victim to trusting what the product promises to do and what features it might have without being given information how the product works internally. However, the amount of time, effort and money needed to fully test this product is usually more trouble than what it is worth. Despite this, the company selling the product should be held accountable for the quality of the service that they provide rather than relying on the consumer to understand the product. Unfortunately in the corporate world of security software, companies are pressured into rolling out their latest and greatest faster than their competitors. This leads to poor design and a lack of risk analysis.

The goal is to roll out with the technology first then try and make improvements later. Regrettably, these improvements seldom happen because technology is constantly gaining on
itself and before improvements can be made something new comes along. To add to this pile of
lemons, some of these security software companies themselves aren’t even hiring the qualified
individuals to produce their products. A great example is when Tweakers.net broke Secustick’s
security in their widely used USB flash drive product line. For a company to mass release and
advertise a security product without implementing encryption is simply absurd. To make matters
worse, Secustick’s response to Tweakers.net’s findings was that “…not everyone has the
technical expertise that you have”. The “security” implementation on Secustick’s flash drive
was so basic that anyone with basic technical experience would have little trouble breaking into
the device.

The lack of security standards and thorough tests on the part of manufacturers leads to a
series of incorrect perceptions on of what security products must provide. These misconceptions
are not only on the part of users but also manufacturers who concentrate on first stage protection
rather than planning for the initial breech and creating multiple levels of protection. The breech
of one step protection is inevitable because there will always be advancements in the
sophistication of malicious software. By putting personal data under multiple levels of
protection hackers would be further deterred.

Generally, consumers invest in products that are produced by large, widely trusted
companies, as opposed to smaller companies that might have better products but lack of market
recognition. It’s not wrong to trust big companies but consumers shouldn’t have to rely on trust
and reputation alone. Most of the time, these companies rely on having the implementation of
their security software proprietary. Their perception is that by keeping their software
proprietary, it will reduce or prevent the hackers from discovering loop holes. With the many
ways that technical individuals can reverse engineer software products, secrecy is definitely not
the best policy. At the end, the only services that these companies provide are ease of use and the “features” that their product may have. Often, the ease of installation and use wins over the consumer regardless of how well the product performs. Consumers buy into these features and if by chance they don’t experience having their data compromised they naturally assume the product they purchased is protecting them and/or their company. There is not necessarily a correlation between not having sensitive information stolen and the security product(s) being used. On top of that, consumers take the features that one product provides and assumes it is their one-stop shop solution in protecting their entire system. In reality, it is a combination of several security products that will maximize data theft prevention.

The Magnuson-Moss Warranty Act is a federal law that enforces quality control on consumer goods. Unlike these tangible consumer goods, security software is not subject to the Magnuson-Moss Warranty Act. Therefore, there is no sure way of judging the quality of a security product. Instead of defining quality, what the information security industry should focus on is standardization. Standardization means having a set of rules which security products must follow. The absence of standardization is driving software companies into defining what security means to them without any overarching guidelines. Security is not about setting the maximum number of password retries or having the user verifying other personal information. Security is about making data theft and corruption difficult enough so that it won’t be worth the effort of a typical hacker. Encryption, depending on the chosen algorithm, can be standardized as step in providing more reliable security software.

Ultimately, the problem is cumulative since it involves both how the industry defines security and also how the users perceive the product as being dependable. In the case of the software manufacturers there must be some kind of standard for applying cryptographic methods
in protecting personal data. As the trend is now, with mediocre security applications, the quality of security software will eventually decline as malignant software catches up. This will lead even brand name manufacturers to lose their credibility, leaving users vulnerable to further exposure on any system. In today’s world, where technology is constantly moving at Moore’s law, the industry has to be cautious of marketing software that is incomplete in order to meet consumer demands.