Economics

Rohit Sinha

December 12, 2011

1 Economics and Security

1.1 Mac vs. PC

Are Macs inherently secure? Maybe macs are not inherently secure, but attacking PCs has a higher payoff because PCs have much higher market share.

Observed windows malware to mac malware ratio is nearly 1000:1, much higher than the market share ratio.

Lets model this as a very simple game. The model consists of an enterprise with 90 PCs and 10 Macs, which is roughly the market share. There are two players in this game: attacker and defender. The attacker chooses to attack either PCs or Macs located in the enterprise. The defender is the IT security team at the enterprise, with some limited budget. In other words, they can either defend PCs or Macs, but not both. There are two assumptions here:

- If the attacker attacks an undefended platform, then attack is guaranteed to be successful. For example, if the attacker attacks PCs and the defender defends Macs, then the attacker gains 90 machines.
- If an attacker attacks a platform that is also defended by the enterprise, then the attack fails. For example, if the attacker attacks PCs and the defender defends PCs, then the attacker gains 0 machines.

Table 1.1 illustrates the payoff matrix under these assumptions.

	defend PC	defend Mac
attack PC	0	90
attack Mac	10	0

This is a zero-sum game, meaning the number of machines gained by the attacker equals the number of machines lost by the enterprise to the attack. The optimal strategy for this payoff matrix is:

Attacker: attack PC 90% of the time, and Mac 10% of the time.
Defender: defend PC 90% of the time, and Mac 10% of the time.

This should predict that 90% of attacks should be on PCs, and 10% of attacks on Macs. However, in reality, almost 99% of attack traffic is directed towards PCs. This model does, however, suggest that even without assumptions on Mac vs. PC OS level security, the attack traffic is proportional to market share.

Let's add another assumption to our model.

- Macs are more secure than PCs. Inherently, Mac OS comes with security protection which is able to protect it on x % of the attacks (without any enterprise effort). PCs have no security and they are able to protect themselves in 0 % of the attacks.

Table 1.1 illustrates the payoff matrix for x = 50%.

	defend PC	defend Mac
attack PC	0	90
attack Mac	5	0

The optimal strategy for this payoff matrix is:

Attacker: attack PC 95% of the time, and Mac 5% of the time.
Defender: defend PC 95% of the time, and Mac 5% of the time.

This result may indicate that Macs are really more secure than PCs.
Let's add a different assumption to the original model where Macs and PCs are equally secure.

- Defenses are not perfect. Approximately y % of the defenses fail.

Table 3 illustrates the payoff matrix for y = 50%.

	defend PC	defend Mac
attack PC	45	90
attack Mac	10	5

The optimal strategy for this payoff matrix is:

Attacker: attack PC 100% of the time, and Mac 0% of the time.
Defender: defend PC 100% of the time, and Mac 0% of the time.

This reflects the real attack traffic fairly closely.

2 Externality

Economics definition: Cost or benefit that is not reflected in the market price. A third party incurs a portion of the cost or enjoys a portion of the benefits of some action.

A good example is a factory which creates pollution, but does not have to pay for the environmental damage. This allows them to create more products than they would if they were made to pay for the damages. The cost is undertaken by the general public. Similarly, buying a phone service not only benefits the customer, but the customer's friends as well. This is also known as the network effect.

2.1 Externality and Security

Spammers don't necessarily compromise machines to get access to sensitive data since most of the victims are home users. A common motivation for spammers is to recruit these machines as botnets for spamming attacks.

So, who should really pay for security? Home users or the corporations like Amazon and Microsoft getting attacked (via DDOS for example)? There is an externality here. There is some cost to an end user in getting their machine hacked for data or identity theft, but there is almost

no cost to the user in getting their machine hacked and used as a jumping off point for attacking corporations.

Ross Anderson's paper on banking fraud proposes that the cost of security should fall under those who can create defenses against the attacks. For instance, it is incumbent upon the banks to secure their customers against ATM fraudulence. By that analogy, if Microsoft wants to protect itself from botnet attacks, then it should provide free antivirus software to its users. There have been efforts to encourage OS developers to write more secure code. For instance, Microsoft was pressured by the industry to make security a higher priority. To that end, Microsoft enforced mandatory security training for all its Software developers. Some have suggested that ISPs should be made responsible for analyzing their traffic for DOS attacks and other spams. However, ISPs want to stay away from this because there is always risk of false positives. These false positives imply that a fraction of customers face problems in internet access, which leads to expensive customer care calls.

3 Market for Lemons

Market for lemons occurs when the buyers do not have perfect information about the quality of products. If the buyers and sellers have perfect information, economics theory suggests that they should converge to an effiicent market governed by supply and demand. The matrix below illustrates the different scenarios in this context.

	buyer knows	buyer doesn't know
seller knows	efficient market	market for lemons
seller doesn't know	market for limes	ignorance

It is undesirable for a seller to be in a market for limes. Examples of this are health insurance providers and antique item sellers. A health insurance provider, for instance, does not have access to complete information on a person's health before selling insurance. The insurance providers get around this issue by issuing a contract with the client.

3.1 Market for lemons in Security

Examples of markets for lemons in the security world include services which require personal information. For instance, an online Playstation gamer trusts Sony to protect his or her information. This protection is an indirect service being sold to the customer. However, the customer typically does not know the quality of protection being offered, thus making it a market for lemons. There are several techniques that sellers use to deal with lemon markets.

3.2 Signaling

Signaling addresses a market for lemons. Sellers use signaling to differentiate themselves from other sellers. The idea is to demonstrate ability to do something that the competitors cannot do.

For instance, banks spend a lot of money on their storefront to give their customers a sense of confidence that the bank is stable. Similarly, female peacocks signal health by showing off a healthy tail. Although it serves no useful purpose, the tail demonstrates the male peacock's ability to spend extra energy on beauty, which is a signal for health.