Malware and Market Share

Daniel G. Arce
Ashbel Smith Professor of Economics
University of Texas at Dallas
800 W. Campbell Rd.
Richardson, TX 75080
darce@utdallas.edu

Abstract

This paper presents a game theoretic analysis of the relationship between an information technology platform's market share, its level of security, and the extent to which malware creators (hackers) target a platform in order to proliferate via the platform's network externalities. In equilibrium, a platform's market share is shown to be the square root of the ratio of its competitor's vulnerability to its own vulnerability. This implies that in order to maintain market share, platform leaders must make increasing investments in cybersecurity, thereby decreasing the platform's vulnerability.

Introduction

Malware, a term that combines malicious with software, refers to a computer infection program designed to compromise, damage, or infiltrate a computer, server or network without the user's knowledge or consent, often for profitable gain. Examples of self-replicating malware include viruses and worms. The potential for malware has been recognized since the dawn of personal computing itself. Hiltzik (1999) recounts a 1978 episode at Xerox's revolutionary PARC research facility where an employee created a worm whose code became corrupted and caused scores of desktop computers connected to PARC's Ethernet to repeatedly crash. According to a joint study by International Data Corporation and National Singapore University, for 2014 the annual cost of malware was expected to be over $491 billion a year (Robinson 2014). In addition, consumers would spend 1.2 billion hours dealing with the aftereffects of malware. The direct cost alone would rank malware as the 26th largest country in the world in terms of GDP. In such a high stakes environment it is necessary to understand the strategic incentives facing those who provide security for information technology platforms (e.g., PCs, tablets, smartphones), users who select this technology, and malware that targets users through platforms.

As the famous bank robber Willie Sutton reportedly explained, he robbed banks, "because that's where the money is." Similarly, hackers write malware to target where users are, and this is determined by the market share of a platform. Everything else held equal, hackers prefer a platform with a larger installed base (Honeynet Project 2004). This paper provides a game theoretic characterization of the relationship between market share, quality (security) of a platform, and the relative degree to which malware creators (hackers) target a platform.[1] Two of the three of these variables: market share and the distribution of malware across platforms, are

[11] The use of the term "platform" is widespread in the literature on the economics of two-sided markets, where a platform allows distinct user groups to interface, thereby providing each other with network benefits, often based on economies of scale. Technological devices or systems are quintessential examples of economic platforms because they create network externalities by matching users and application providers.

derived endogenously. For a given level of platform security, users choose between two platforms and hackers choose their target. Malware both compromises and takes advantage of the network externalities associated with information technology markets. Within this context, the focus here is on how malware constitutes a negative externality for users, thereby determining market share within an existing duopolistic platform market. In equilibrium, a platform's market share is shown to be the square root of the ratio of its competitor's vulnerability to its own vulnerability. This leads to a never-ending battle in which security increases a platform's market share while malware targets platforms with greater market share.

Related Literature

This analysis combines three strands of literature. The first pertains to market dualism, referring to the phenomenon that different firms in the same market follow distinct strategies. For example, in the U.S. all major domestic airlines charge for checked baggage with the exception of Southwest, the largest domestic carrier within the U.S. Another example is that some grocery chains provide discounts to identifiable customers with shopper/rewards cards whereas for other chains discounts are uniformly available to all customers (e.g., rollbacks at Walmart). In this paper duality takes place with respect to the platforms associated with devices such as personal computers, laptops, smartphones and tablets.

These platform markets are characterized by direct and indirect network externalities. Users experience direct network externalities when the benefits of a platform increase with the number of users. In addition, direct externalities are augmented by indirect externalities such as the variety of software and app producers, which is determined by and determines a platform's market share. The process by which pricing and innovation interact to determine the outcome of platform competition is taken as given. Instead, the focus is on how the resultant network externalities both influences users' selection of a platform and facilitates malware's exploitation of a platform's market share.

In order to capture the existence of direct and indirect externalities, users' network benefits of a platform are assumed to be determined by a platform's *relative* market share. That is, for users there are demand-side economies of scale that might otherwise result in one platform. Specifically, if s is the market share of the dominant platform and $1-s$ is the market share of the minority platform then the combined network externalities associated with the dominant platform are $s/(1-s) > 1$; indicating the complementary benefits of having the larger network of users. By contrast, the network externalities associated with the minority platform are $(1-s)/s < 1$.

Several reasons exist for why platform competition that exhibits these demand-side economies of scale need not end in a winner-take-all outcome. Cennamo and Santalo (2013) show that when rival platforms engage in 'get big fast' strategies by locking in both users and applications providers, thereby undermining rival platforms that do the same, then the resulting market segmentation precludes any platform from being able to capture the whole market. In the same way, when platforms offer contracts to firms that are contingent on the number of firms that join the platform, excessive competition in the presence of network externalities can lead to a split market (Lee 2014). Another possibility is that a minority platform successfully caters to a niche market (e.g., arts and academia) by providing proprietary segment-specific benefits.

In addition, the ability to access network benefits is limited by the extent that malware targets a platform. For users the selection of a platform by others constitutes a positive externality, but the targeting of the platform by malware creates a negative externality. Hence, differences in network benefits and platform security contribute to market dualism. Consequently, platform competition is not winner-take-all and is instead taken to be bifurcated, consistent with the current reality for PCs, laptops, smartphones and tablets. According to NetMarketShare.com, Windows currently holds approximately 91% of the PC market with Mac's OS second at 7.5%.[2] For smartphones and tablets the breakdown is Android with 41% and iOS with 32%.[3]

Given that most malware is designed to exploit operating system holes (vulnerabilities) and bugs (Karyotis and Khouzani 2016), market share matters. As such, the second strand of literature considered is the mixed strategy approach to explaining market structure, where the mixed strategy for users in the associated game characterizes the proportion of users that select a given platform, thereby endogenously deriving a platform's market share. A mixed strategy Nash equilibrium (hereafter, MSNE) allows the equilibrium choice of platform to be bifurcated whereas a pure strategy equilibrium corresponds to a winner-take-all outcome. Similarly, the mixed strategy for hackers characterizes the proportion of malware targeting a given platform. Perhaps the first use of mixed strategies to formally characterize market structure in this way was given by Cornell and Roll (1981), who used the MSNE of a securities trading game to derive the proportion of analysts and non-analysts that is consistent with the efficient market hypothesis. Jacquemin (1991) notes that in industrial organization a MSNE allows for the existence of market dualism.

More generally, the perspective taken here employs the '*mass action*' interpretation of MSNE, originally given in Nash's (1950: 21-22) dissertation. In the mass action interpretation a MSNE constitutes a cross-sectional distribution over a population of players' strategies, with a mixture's value corresponding to the frequency of a strategy within that population. Hence, for the malware-platform game introduced in the following section we focus on the MSNE, with the mass action interpretation of the MSNE characterizing both the market share of each platform and the proportion of malware that targets a platform.

[2] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0. Accessed 18 April 2016.
[3] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1. Accessed 18 April 2016.

The third strand of literature considered pertains to the game theoretics of information technology security and malware. O'Donnell (2008) shows that if a platform's market share is particularly large, then it may be a dominant strategy for hackers to exclusively target the prevalent platform. He gives the following example: suppose that the Mac OS platform has 4% of the PC and laptop market whereas Windows has 85%. Furthermore, suppose that the Apple OS platform is 80% secure whereas Windows products are *p*% secure. So long as the expected number of Windows users whose security is breached exceeds that of OS users: $(1-p)\times85 > (1-.8)\times4 \Rightarrow 99\% > p$, then hackers will exclusively target Windows-based PCs. In this example the Windows platform can be much more secure than the OS platform and yet malware exclusively concentrates on the Windows platform owing to Windows' enormous market share. Windows' domination makes it the "hackers' target of choice" (Berghel 2003).

A major difference between O'Donnell's (2008) game theoretic model and the present analysis is that in O'Donnell market share is taken as given and users select which platform to *protect* whereas here users decide which platform to *select*. This allows market share to be endogenously determined from a MSNE that characterizes the cross-sectional distribution of platforms selected by users. This not possible in O'Donnell because users' payoffs are not specified; consequently, no equilibrium strategy for users is derived.[4] Finally, O'Donnell's assumption of equal quality (security) across platforms is relaxed.

Garcia et al. (2014) consider a differential game of platform competition where platforms possess positive network externalities that are offset by the negative externalities associated with malware. Both externalities enter linearly into a user's payoff function. They show that the long-run platform market structure depends on hackers' sensitivity to market share asymmetries. Platform providers with lower market share compete by providing higher security at lower

[4] This is because his focus is on the existence of a dominant strategy for hackers, which by definition is independent of users' actions.

prices. In the present model malware exploits a platform's direct network externalities through the platform's market share. The ability to do so; however, is determined by a platform's security. Hence, hackers' preferences for a platform are sensitive to the combination of a platform's market share and security. Moreover, users' positive network externalities and negative malware externalities are multiplicative rather than linear, owing to the role that security plays as a gateway for achieving network effects.

Finally, Florencio and Herley (2013) examine a game in which hackers' efforts do not focus on the network effects produced by a weakness in a platform's structure. Instead, hackers employ *en masse* attempts to breach each *individual* user's weaknesses (e.g., passwords). This produces the novel result that a probability of hacker success is a function of the summation of each user's security effort. The distinction between their model and the present one lies in the difference between spreading and propagative processes of malware diffusion (Karyotis and Khouzani 2016). Florencio and Herley is a spreading model of hacking, in which the transfer of malware takes place between two individual and distinct nodes – malicious and noninfected – where there is a population of each type of node. Our focus here is not on an individual user's weakest link, but a weakness in the platform that is common to all users of that platform. In terms of diffusion, the resulting game employs a propagation externality because both the original malicious nodes and infected nodes are able to contaminate noninfected nodes.

The Model

The model introduced in this section is deceptively simple but has rich implications for the interplay between malware and market share. It is based on the recognition that information technology markets are often bifurcated into two platforms such as Windows and Macs for personal computers or Android and iOS for smartphones. As discussed above, among other factors the presence of malware creates a friction that allows for a bifurcated platform market where standards that produce network externalities might otherwise lead to one platform. Malware is a negative externality in the market for platforms that offsets the network benefits of a common platform. At the same time, the greater a platform's market share, the more benefit a hacker receives from creating malware that exploits it. Users, on the other hand, receive benefits from the direct and indirect network externalities associated with a platform. These network externalities are captured by the relative market share of a platform, as explained above. By the nature of direct (same-side) network externalities, users of a platform receive benefits that increase with the number of users of the platform. In addition, indirect externalities exist in that proportionally more software and apps will be written for the dominant platform. The positive network externalities of a platform are offset by the likelihood of malware compromising the platform, as measured by the platform's security. Users' network benefits are only realized if the platform is not compromised.

Within this context, the payoffs for users and hackers associated with a particular platform are determined by (relative) market share, and the platform's security. Specifically, let:

$s \in (0,1)$ ≡ *market share* of platform 1 with $(1-s)$ ≡ market share of platform 2.

$p \in (0,1)$ ≡ *security* (quality) of platform 1; denoting the probability that an attack on platform is 1 unsuccessful, with $1-p$ denoting platform 1's *vulnerability*.

$q \in (0,1)$ ≡ *security* (quality) of platform 2 (the probability of successful deterrence), with $1-q$ denoting platform 2's *vulnerability*.

To foreshadow, in equilibrium the effect of malware on market share is determined by the ratios of these variables. As defined above, the *relative market share* of platform 1 is $s/(1-s)$ and that of platform 2 is $(1-s)/s$. In addition, the *vulnerability ratio* of platform 1 is defined as $v_1 = (1-p)/(1-q)$ for platform 1 and $v_2 = (1-q)/(1-p)$ for platform 2.

The associated game is given in strategic form in Figure 1, where a hacker's strategy is which platform to target and a user's strategy is which platform to select. Hackers' payoffs are determined by the market share of a platform, s or $1-s$, thereby exploiting the platform's direct network effects. Recall the quote by the famous bank robber Willie Sutton given in the introduction. The ability to compromise a particular platform is given by the probabilities $1-p$ and $1-q$. From Figure 1, a hacker that targets platform 1 has an expected payoff of $(1-p)s$ and attacking platform 2 instead yields an expected payoff of $(1-q)(1-s)$. By definition, if $p > q$ then it is more difficult to attack platform 1 and if $p < q$ it is more difficult to target platform 2. If a hacker targets a platform that is not selected by any user then the hacker's payoff is normalized to zero, corresponding to the hacker's off-diagonal payoffs.

In selecting a platform, users realize that a platform's security determines their ability to benefit from the platform's network externalities, as measured by the platform's relative market share. Given that p is the security of platform 1 and $s/(1-s)$ is its relative market share, if a hacker targets platform 1 a user of platform 1 receives an expected payoff of $p\times[s/(1-s)] + (1-p)\times 0 = p\times[s/(1-s)]$, where the users' network benefits of platform 1 are attained only if the platform successfully deters the hack (deterrence occurs with probability p). One can alternatively think of $p\times[s/(1-s)]$ as the reduced network externalities experienced by users of platform 1 when platform 1 is targeted by hackers. By comparison, a platform 1 user's payoff is $s/(1-s)$ if hackers instead target platform 2. The (expected) payoffs for users of platform 2 are similarly defined for level of security q and relative market share $(1-s)/s$.

Equilibrium and Characterization

As foreshadowed above, the focus is on the mixed strategy Nash equilibrium (MSNE) of this game because a pure strategy equilibrium on the part of users would imply a winner-take-all outcome, and such an outcome is not observed for the platform markets under study. Within this context, the interpretation of MSNE is as given by Nash's (1950) concept of mass action: cross-sectional distributions of users and hackers over the platforms, respectively; rather than the probability that an individual user or hacker selects a particular platform. As such, let:

$\sigma \in (0,1)$ ≡ mixed strategy distribution of users *selecting* platform 1;

$1 - \sigma \equiv$ mixed strategy distribution of users selecting platform 2;

$\tau \in (0,1)$ ≡ mixed strategy distribution of malware hackers *targeting* platform 1; and

$1 - \tau \equiv$ mixed strategy distribution of malware hackers targeting platform 2.

In a mixed strategy Nash equilibrium, σ has the property that it makes malware hackers indifferent between attacking platforms 1 and 2. Referring to Figure 1:

(1) $(1-p)s \times \sigma = (1-q)(1-s) \times (1-\sigma)$.

Under the mass action interpretation of MSNE, σ and $1-\sigma$ represent the cross sectional distribution of users selecting platforms 1 and 2. As in Garcia et al. (2014), in equilibrium hackers' expectations of the market share of each platform are required to be fulfilled. Consequently, in equilibrium it is required that:

(2) $\sigma = s$.

That is, under the mass action interpretation of MSNE, the equilibrium mixed strategy for a user's platform choice is equal to that platform's market share. Hackers' expectations of a platform's market share are thereby fulfilled. Substituting (2) into (1), platform 1's relative market share is:

(3) $s/(1-s) = \sqrt{(1-q)/(1-p)}$.

Similarly, platform 2’s relative market share is $(1-s)/s = \sqrt{(1-p)/(1-q)}$.

From these derivations, one can see that a platform’s relative market share is determined by the inverse of its *vulnerability ratio*, defined above as $v_1 = (1-p)/(1-q)$ for platform 1 and $v_2 = (1-q)/(1-p)$ for platform 2. Specifically:

RESULT: In bifurcated platform competition, a platform’s relative market share is equal to the square root of the inverse of its vulnerability ratio, $\sqrt{1/v_i}$, $i \in \{1,2\}$.

This result establishes a theoretical building block for cybersecurity that is also consistent with the longstanding empirical folk wisdom that platform leaders must make increasing investments into cybersecurity in order to maintain market share. As such, the result has several novel implications. First, $p = q \Rightarrow s = ½$. Equal quality (in terms of security) leads to equal market share. Second, a platform creator must make increasingly greater investments in security; otherwise, its market share will erode. For example, for platform 1 increasing p increases $(1-q)/(1-p)$, but relative market share, $s/(1-s) = \sqrt{(1-q)/(1-p)}$, grows much more slowly than does $(1-q)/(1-p)$. Empirically, power law predictions for relative market share (also known as ‘share ratios’) are quite common (Kohli and Sah 2006). The present analysis provides a theoretical foundation for this phenomenon.

Third, the comparative statics of relative market share are: $\partial\left(s/(1-s)\right)/\partial p > 0$ and $\partial\left(s/(1-s)\right)/\partial q < 0$. In equilibrium, platform 1’s relative market share is increasing in its security (p) and decreasing in the security of platform 2 (q). Indeed, this result is a strategic extension of Hirschman’s (1970) analysis of consumer exit and quality deterioration. Specifically, platform 1’s relative market share is decreasing in its *lapse* in security (vulnerability), 1–*p*, and increasing in platform 2's *lapse* in security (vulnerability), 1–*q*. Similar comparative statics hold for platform 2's relative market share, (1–*s*)/*s*. This is illustrated in Figure 2. When a dominant platform's security initially deteriorates, its relative market share initially decreases at a slow rate. If this deterioration persists, then the exodus of users leads to a rapid decrease in relative market share.

Fourth, given $s/(1-s)=\sqrt{(1-q)/(1-p)}$ and $(1-s)/s=\sqrt{(1-p)/(1-q)}$, it follows that when malware targets platform 1, the payoff for users of platform 1, $p\left[s/(1-s)\right]$, in Figure 1 can now be expressed as $p\sqrt{(1-q)/(1-p)}$, and the payoff for users of platform 2, $(1-s)/s$, is $\sqrt{(1-p)/(1-q)}$. Similarly, when malware instead targets platform 2, the payoff for users of platform 1, $s/(1-s)$, in Figure 1 can be expressed as $\sqrt{(1-q)/(1-p)}$, and the payoff for users of platform 2, $q\left[(1-s)/s\right]$, is $q\sqrt{(1-p)/(1-q)}$. Given these expressions of the payoffs, the following assumption guarantees that the game in Figure 1 has a unique mixed strategy equilibrium (i.e., a clockwise sequence of best replies for the players) and therefore allows for market dualism rather than winner-take-all platform competition:

ASSUMPTION: $1-p>p(1-q)$ and $1-q>q(1-p)$.

These inequalities imply $(1-p)+(1-q)>\ q(1-p)+p(1-q)$, which holds for $p,q\in(0,1)$.

In deriving the cross-sectional distribution of malware hackers, the associated MSNE has the property that targeting mixture τ makes users indifferent between the two platforms. As the users' payoffs in Figure 1 can be re-expressed in terms of *p* and *q*, τ satisfies the indifference property for users when:

$$\tau\times p\sqrt{\frac{1-q}{1-p}}+(1-\tau)\times\sqrt{\frac{1-q}{1-p}}=\tau\times\sqrt{\frac{1-p}{1-q}}+(1-\tau)\times q\sqrt{\frac{1-p}{1-q}}.$$

Solving for τ:

(4) $$\tau = \frac{(1-q)-q(1-p)}{2(1-p)(1-q)} = \frac{1}{2(1-p)} - \frac{q}{2(1-q)}.$$

Note that $\tau > 0$ when $q(1-p) < 1-q$, which holds by assumption. Also $\tau < 1$ when

$(1-q)-(1-p)q < 2(1-p)(1-q)$, which reduces to $p(1-q) < 1-p$ and holds by assumption.

The comparative statics for malware targeting are $\partial\tau/\partial p > 0$ and $\partial\tau/\partial q < 0$, which are somewhat counterintuitive until one considers the network effects on the market structure of malware. An increase in security, p, increases platform 1's relative market share, $s/(1-s)$, which thereby increases malware's targeting of platform 1, τ. This is because the only way that $s/(1-s)$ can increase is if s increases and s enters directly into the payoff of malware that targets platform 1. Indeed, the market share-malware-targeting nexus identified here is also observed in the market for information technology security. It is well-known that hackers write malware to specifically breach products from Intel Security (McAfee) and Symantec (Norton) rather than freeware security products, because it pays to breach these commercial products given their large market share. Conversely, minority platform users' presumption of superior security may instead be an illusion related to low hacker targeting owing to low market share. By contrast, an increase in platform 2's security, q, decreases platform 1's relative market share, $s/(1-s)$, which thereby decreases the extent that malware targets platform 1, τ.

Conclusion

In medicine, the foremost principle for diagnosis is known as Sutton's Law: consider the obvious. This paper does the same for cybersecurity by presenting a game-theoretic analysis of the relationship between a platform's market share, its level of malware security, and malware hackers' decisions to target one platform over another. It is shown that when the network effects of an information technology platform can be hijacked by malware, then the relative market share of the platform is the square root of the ratio of its competitor's vulnerability to its own vulnerability. In terms of Sutton's Law, as a platform's security increases, malware hackers *increase* their targeting of the platform, owing to the way that security increases a platform's market share. This suggests that the very maintenance of a platform's market share requires greater and greater investment in security, as hackers leverage a platform's market share to further their own intentions. The market share-malware nexus is a never-ending battle.

References

Berghel, H. 2003. Malware Month. *Communications of the ACM* 46(12) 15-19.

Cennamo, Carmelo and Juan Santalo 2013. Platform Competition: Strategic Tradeoffs in Platform Markets. *Strategic Management Journal* 34(11) 1331-1350.

Cornell, Bradford and Richard Roll 1981. Strategies for Pairwise Competitions in Markets and Organizations. *Bell Journal of Economics* 12(1) 20-213.

Florencio, Dinei and Cormac Herly 2013. Where Do All the Attacks Go? In Bruce Shneier (ed.), *Economics of Information Security and Privacy III*, New York: Springer, pp.13-33.

Garcia, Alfredo, Yue Sun and Joseph Shen 2014. Dynamic Platform Competition with Malicious Users. *Dynamic Games and Applications* 4(3) 209-308.

Hiltzik, Michael 1999. *Dealers of Lightning*. *Xerox PARC and the Dawn of the Computer Age*. New York: HarperCollins.

Hirschman, Albert O. 1970. *Exit, Voice and Loyalty*. Cambridge, MA: Harvard University Press.

Honeynet Project 2004. *Know Your Enemy: Learning About Security Threats*, Second Edition. Indianapolis: Addison-Wesley Professional.

Jaquemin, Alexis 1991. *The New Industrial Organization*. Cambridge: MIT Press.

Karyotis, Vasileos and M.H.R. Khouzani 2016. *Malware Diffusion Models for Modern Complex Networks*. *Theory and Applications*. Cambridge, MA: Morgan Kaufman.

Kohli, Rajeev and Raaj Sah 2006. Some Empirical Regularities in Market Shares. *Management Science* 52(11) 1792-1798.

Lee, Robin S. 2014. Competing Platforms. *Journal of Economics & Management Strategy* 23(3) 507-526.

Nash, John 1950. Non-Cooperative Games. PhD Disseration, Princeton University Department of Mathematics. In H.W. Kuhn and S. Nasar (eds.), *The Essential John Nash*, Princeton University: Princeton University Press, pp.53-84.

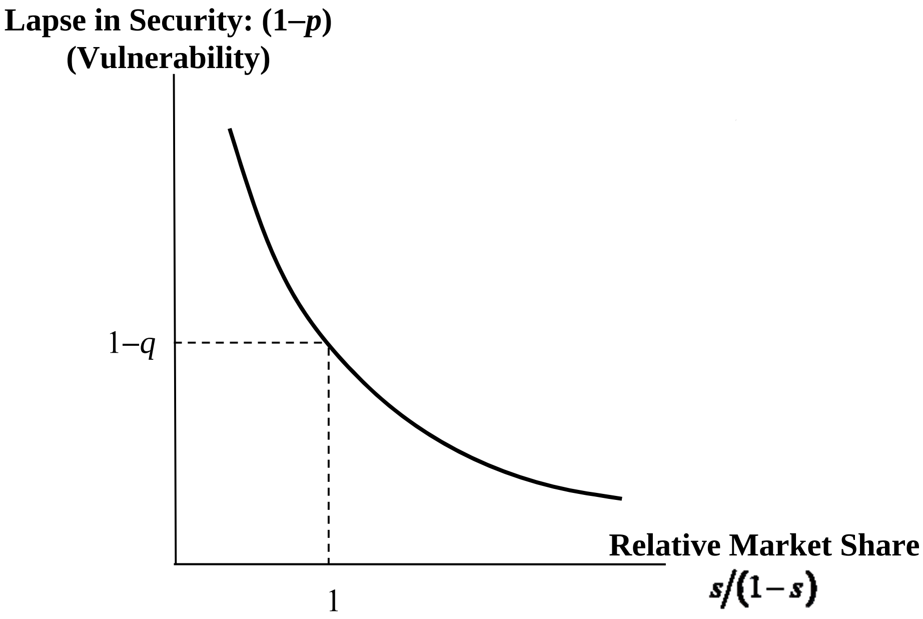
O'Donnell, Adam 2008. When Malware Attacks (Anything But Windows). *IEEE Security & Privacy* May/June 68-70.

Robinson, Teri 2014. Breaches, Malware to Cost $491 Billion in 2014, Study Says. *SC Info Security Magazine*, 20 March.

Figure 1: The Malware Game with Bifurcated Platforms
[*s* ≡ Market Share of Platform 1]

Hackers Target Malware on	Users Select	
	Platform 1	**Platform 2**
Platform 1	$(1-p)s, p\frac{s}{1-s}$	$0, \frac{1-s}{s}$
Platform 2	$0, \frac{s}{1-s}$	$(1-q)(1-s), q\frac{1-s}{s}$

Figure 2: Market Share and Security


Lapse in Security: $(1–p)$
(Vulnerability)
$1–q$
Relative Market Share
$s/(1-s)$