Cybersecurity and Platform Competition

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

Abstract

Operating systems, microprocessors, and cloud computing services are examples of platform providers in the classic sense of the economics of two-sided markets. This is because indirect externalities arise from connecting users with developers of complementary products or services. The premise investigated here is that platform security is subject to the same rigors of platform competition that shape a platform's pricing and market structure. This paper demonstrates how cybersecurity shapes platform competition and platform competition shapes cybersecurity. In particular, cybersecurity is shown to be a user-side phenomenon with characteristics that can lead to platform coexistence rather than monopoly. In addition, a platform's switching costs are shown to be the ratio of users' potential malware-induced losses for each platform.

1. Introduction

Information systems platforms are technological architectures or ecosystems that connect users with developers of complementary products or services, thereby reducing search costs for users and increasing transaction opportunities for developers. Examples include the Windows operating system for PCs/laptops and Apple's OS for Macs, as well Android and iOS for tablets and mobile devices. In this case, users buy apps that are developed for the platform by third parties as well as the platform itself. Similarly, Intel, ARM, and AMD microprocessors are competing hardware platforms for PC systems. Historically, growth in the PC and laptop markets is largely driven by innovations in microprocessor architecture and Moore's law. This increase in performance affects innovation and compatibility across ecosystem complementors (e.g. operating systems, motherboards, peripherals, software, etc.).[1] A further example is cloud computing, particularly software-as-a-service (SaaS), in which applications can be made available on demand to users via the Internet. SaaS platforms include G Suite by Google, Adobe Creative Cloud, Microsoft Azure, and Salesforce.com.

In facilitating exchange between both sides of the market, a platform creates *indirect externalities* in that the value of the platform for those on one side of the market rises with increased participation on the other side of the market. For example, application developers benefit if there are many users that adopt the operating system running their applications. Similarly, users benefit from an operating system with many apps to choose from. For this reason, information system platforms were motivating examples at the genesis of the economic analysis of two-sided markets.[2]

At the same time, information system platforms differ from the classic analysis of two-sided markets in at least two significant ways. First, two-sided markets are often characterized by winner-take-all (WTA) competition among platforms, thereby leading to a monopoly provider. Following Anderson (2001), the three conditions that, in combination, are likely to lead to a WTA outcome are (i) direct network externalities, where users' benefits from their side of the platform increase with the number of users on the same side of the platform, (ii) technology with high fixed costs and low variable costs per user, and (iii) large switching costs from one platform technology to the other. Owing to the prevalence of these conditions, the literature on platform pricing decisions and

[1] Gawer (2014) suggests using the term 'complementor' for the firms/applications developers/services on the opposite side of users in IT platforms and this convention is continued here.
[2] See Gawer and Cusumano (2002), Rochet and Tirole (2003), and Parker and van Alstyne (2005).

strategy largely adopts the assumption of platform-as-monopoly (e.g. Parker, Van Altstyne, and Choudary 2016, Evans and Schmalensee 2016, and McAfee and Brynjolfsson 2017), with the resulting analyses being dependent upon this assumption.

In spite of this, not one of the standard examples of an information technology platform given above is a monopoly. Apple OS coexists alongside Microsoft Windows (and Linux) as operating systems for desktops and laptops. Similarly, Android and iOS coexist as mobile and tablet platforms. Multiple cloud providers are available for SaaS. Recognizing this, the platform markets analyzed here have the potential to be (imperfectly) competitive. Consequently, in this paper no assumption about platform market structure is made. Instead, a platform's market structure is determined endogenously even though the WTA conditions continue to hold.

Second, information technology platforms are often plagued by miscreants seeking to co-opt the technology for their own interests, often to the detriment of users, platform providers, and complementors. This is, of course, a reference to malware. Hence, in addition to successfully connecting both sides of the market, platform providers must consider their information security investments in terms of malware's effects on the (in)direct benefits of the platform. Indeed, with respect to cloud platforms, "hosts such as Amazon, Google, and Salesforce.com generally guarantee security for their hosting customers through detailed service level agreements" (Cusumano 2010, p.28). Hence, platform security provision is as well conducted under the rigors of platform competition.

This paper examines the provision of platform security through the lens of platform competition. To date, much of the focus of platform competition is on the structure of prices, as competition may lead to one side of the market receiving subsidized prices in order to generate membership that produces indirect externalities benefiting the other side of the market. For example, platforms often provide application developers with development toolkits recognizing the effect that the proliferation of apps has on the adoption of the platform by users. Similarly, Intel interfaces with its complementors through its Intel Architecture Lab (IAL) in order to coordinate innovation activity. These actions are akin to a platform providing a subsidy to complementors.

Yet it is generally something other than the pricing structure that leads to the coexistence of platforms. Examples on the complementor/developer side include strategies such as app exclusivity agreements and app variety. Indeed, the vast majority of the literature on platform coexistence focuses on platform strategies for the complementor/developer side of the market. At the same time,

a market can sustain multiple platforms only if coexistence also holds on the user side.

For this reason the focus here is on the user side and the platform strategy of providing user security. Malware exploits vulnerabilities and bugs in a platform, thereby diminishing the value of the platform to the user. The contention here is that security is subject to the same disciplinary forces of platform competition that shape a platform's pricing structure and other strategies, such as whether to make the platform feature-rich versus minimalist, or the choice between open-source versus proprietary. For example, platform coexistence requires that that no users will switch from one platform to another. Platform security that satisfies the 'no-switching' requirement is consistent with platform coexistence.

Consequently, one contribution of this paper is demonstrating how cybersecurity shapes platform competition and platform competition shapes cybersecurity. In particular, cybersecurity is primarily a user-side concern. Additionally, from the perspective of platform competition, monopoly is regarded as a 'corner' solution and platform coexistence as an 'interior' solution or market structure. By identifying the conditions on platform security that lead to an interior market structure, this study characterizes platform security in terms of the process of platform competition and economics of information security.

The analysis proceeds as follows. Section 2 provides a brief review of the literatures on platform security and platform coexistence. Section 3 presents a model of platform competition on security for the user side of the market. Section 4 derives the criteria for determining when the market structure is interior and characterizes platform security in terms of these criteria. A discussion of the economic and information security interpretations of this characterization occurs in Section 5. Section 6 consists of a brief conclusion.

2. Related Literature

This section focuses on those contributions to the literatures on platform security and platform coexistence that are closely related to the analysis at hand. In so doing, the differences between the present and preceding analyses are delineated in order to foreshadow the model described in the next section.

In a WTA outcome there is little incentive for the dominant platform to further complicate its relationship with developers via increased security standards (Anderson 2001). Initially at least, user security creates little value-added between a platform and potentially adopting developers.

Moreover, a negative externality is present, as the consequences of insecurity fall primarily on users, whereas the platform provides users' security, which is costly for the platform to do. If malware diffuses between users (i.e. contagion) this as well provides a rationale for a monopoly platform to provide a minimal level of security (Lelarge 2009). Specifically, for low quality contagion protection, the demand for security will be high because of direct network externalities; users protect themselves owing to the high possibility of contagion. For high quality contagion protection, the demand will be lower because of the free rider effect; a user relies on a neighbor's protection to protect themselves from contagion. Consequently, a profit-maximizing monopoly takes advantage of the increased demand stemming from the direct externalities induced by low-security protection.

If the market structure is instead imperfectly competitive, the characterization of security substantially changes. Assuming two or more competing firms engaged in e-commerce, Liao and Chen (2014) characterize three phases of security. First, surviving the initial phase of competition allows for greater claims on total market profits in the future. As investments in security increase, the commensurate likelihood that a firm will survive (assuming users abandon demonstrably insecure firms) implies that security investment is akin to a first-mover advantage. In the second stage, the number of security-investing firms reaches a critical mass that allows for free riding. In this stage further investment in security only occurs in reaction to the publication of firm-specific vulnerabilities by a third party. In the third and final stage security matures to the point that the survival claim on profits sufficiently offsets the incentive to free ride. The conclusion to be reached here is that the character of security is sensitive to economic incentives that are a function of the structure of the market. Security is characterized differently for monopoly verses oligopoly.

These analyses are not set explicitly within an environment of platform competition and its associated incentives. By contrast, Sen, Guerin, and Hosanagar (2011) examine a monopolist serving a two-sided market and the decision whether to make its platform functionally-rich, which is expensive for the platform but lowers development costs for potential complementors; or minimalist, which places the burden of developing application programming interfaces (APIs) on complementors. Furthermore, they assume a monopolistic market with no direct externalities among users. In their model, small changes in the rate of change of a platform's fixed cost (as a function of the number of features) can result in large changes in the number of features that is optimal for the platform to provide. Hence, even though high fixed costs are consistent with a WTA outcome, the monopoly's provision of features – which can include security – is highly

sensitive to (i) the character of fixed costs, and (ii) the two-sided nature of the platform. Once again, the economic incentives and market share matter for the provision of security.

One can take this a step further by recognizing that the *strategic* incentives inherent in two-sided markets also affect security. That is, the actions of competitors matter as well. For example, Garcia, Sun, and Shen (2014) consider a two platform model in which the security level of a platform is defined as the probability that a randomly-selected hacker targets the other platform, i.e. security-as-deterrence.[3] This probability enters negatively as a separable component in the other platform's payoff. Given this environment, they show that the long-run platform market structure depends on hackers' sensitivity to market share asymmetries. Furthermore, platform providers with lower market share compete by providing higher security at lower prices.

When the platform is the problem, that is, when malware is designed to exploit holes or vulnerabilities in the platform itself, as is usually the case (Karyotis and Khouzani 2016), then malware directly diminishes the utility that users derive from the platform. Platform insecurity can result in a class break in that the entire class of users of the platform are vulnerable, as may be their associated systems once users are compromised (Schneier 2000). In other words, the standard – here, the platform – becomes part of the threat. Consequently, malware interacts with the (in)direct externalities associated with the platform in a non-separable way. For this reason, the current analysis considers an entirely different definition of platform security than that analyzed in Garcia, Sun, and Shen (2014). Owing to the interaction between security and a platform's (in)direct externalities, platform security is defined as the probability that a malware attack is unsuccessful rather than the degree to which it causes malware writers to target an alternative platform. The criteria for establishing the coexistence of competing platforms is commensurately different as well. The coexistence criteria involve (i) no-switching constraints for the users of the platform, (ii) a platform's provision of security that is incentive compatible for the cross-platform distribution of users, and (iii) a no-loss (participation) constraint for each platform.

Lee (2014) invokes these coexistence criteria for the complementor side of platforms, showing that platforms can coexist if each offers a menu of participation-contingent contracts, that is, transfers to complementors that depend on the number of complementors that ultimately join the platform. An example is app exclusivity, where high quality applications are developed and

[3] Their security level is initially defined as the probability that a randomly selected hacker does not attack the platform. As it is assumed that all hackers attack one of the two platforms, the two interpretations are equivalent.

reserved for the platform, with the platform providing a contingent transfer to the complementor. These transfers are regarded as the outcome of multilateral bargaining between the platform and complementors. Such a practice lends itself to the coexistence of platforms because on the complementor side of the platform the direct network externalities need not be positive, as an increase in the number of complementors often translates into increased competition. Hence, Lee shows that contingent transfers allow competing platforms to coexist without appealing to congestion effects, coordination problems, or multiple platforms that employ a portfolio of winner-take-all strategies (e.g. early entry, exclusive licensing, penetration pricing, and app variety).

By contrast, contingent transfers are rare on the user side of the market. The need to create indirect network effects for complementors by increasing the user base through prices that are discounted, subsidized, or equal to zero (i.e. free) is a recognized potentiality. But these low prices are generally not a function of the number of users or result from multilateral contracting between platforms and users. Users are too numerous to justify the transactions cost associated with such a process. Alternatively, platform security *is* related to a platform's market share of users. This can lead to a multi-platform outcome on the user sider, as is shown below. This is novel because the nascent literature on competing platforms has largely focused on the conditions for producing non-monopolistic outcomes on the complementor side, but platform competition cannot truly be non-monopolistic unless coexistence is similarly established on the user side.

Another example of the security-market share nexus is provided by Arce (2018). He considers a game where users' direct externalities from a platform stem from the platform's market share and malware creators target a platform based on its market share as well.[4] In terms of the model to come, given N users in total, n users of platform 1, and exogenous security levels p and q for platforms 1 and 2, respectively, Arce characterizes the Nash equilibrium relationship between a platform's relative market share and relative security as $n/(N-n) = \sqrt{(1-q)/(1-p)}$. This characterization holds regardless of the functional form used to express users' direct network externalities. By contrast, in this study the security levels are endogenous and determined by the process of platform competition. Moreover, the structure of the user side of the market (one or two platforms) is endogenous as well.

[4] An analogy can be made between hackers and market share and bank robbers and banks. As the famous bank robber Willie Sutton explained, he robbed banks, "because that's where the money is."

3. Description of the Model

A platform facilitates a two-sided market, one involving complementors (e.g. application developers) and the other involving users. The focus here is on the interplay between platform security and users. There are two potential platforms, with a set of potential users, $\mathbf{N} = \{1, 2, \ldots, N\}$, each of which can select platform $i \in \{1, 2\}$. The number of users choosing platform 1 is $n \in \mathbf{N}$, and the number of those choosing platform 2 is $N - n$. Users cannot multi-home (choose more than one platform). Allowing for multi-homing would on its own weaken the competition between the two platforms, thereby decreasing the likelihood of monopoly. This is because, by definition, multi-homing violates the WTA condition of prohibitive switching costs.

The (probabilistic) *security* of platforms 1 and 2 are $p(n)$ and $q(n)$, respectively, which are interpreted as the probability of a successful defense against malware attacks. Similarly, the *vulnerability* of platform 1 is $1 - p(n)$, and platform 2's vulnerability is $1 - q(n)$. Specifying a platform's security or vulnerability in this way is consistent with Littlewood et al.'s (1993, pp. 7, 22) appeal for a, "probability-based framework for operational security" that is, "conditional on upon the effort process" of the attacking adversaries. A simple software measure in this vein can be based on the number of defects per lines of code (Vaughn, Henning, and Siraj 2003). A more involved measure that is appropriate for networks is Jha, Sheyner, and Wing's (2002) reliability metric, which estimates the probability of an adversary not succeeding in an attack. Ramos et al. (2017) provide a survey of techniques for generating these probabilities via state-space stochastic models, attack graphs, Bayesian networks, conversion of common vulnerability scoring system (CVSS) scores, or information theory. Finally, the game theoretics of generating effort-based probabilities as a function of the interaction between attacker and defender are addressed in Sallhammer, Helvik and Knapskog (2006a, b).

Security probabilities $p(n)$ and $q(n)$ are functions of n of because of the possibility of social engineering as well as malware targeting based on market share. Under social engineering, the attack surface of a platform is a function of the total number of users of the platform (i.e. through email) and/or the number of user devices connected to the platform (Miller 2011, Krombholz et al. 2015). This specification is consistent with a WTA environment because the condition that the cost of extending security to an additional user, Δn, is negligible can hold even though the level of security itself is a function of the size of a platform's user base, n, and its associated attack surface.

Finally, vulnerability, as represented by $1-p(n)$ and $1-q(n)$, differs from congestion because congestion is a physical property of the platform that may be the outcome of a malware attack (e.g. DDoS) but is not in itself an attack surface to be exploited by malware.

The platforms are differentiated in that users' expected utility can differ across platforms for a given number of users, but it is assumed that users' (reservation) utility is identical within a platform for the same number of users. A user's expected utility for selecting platform 1 is denoted as $U_1(p,n)$ and that for selecting platform 2 as $U_2(q,n)$. Given the number of users of platform 1, $n, U_1(p,n)$ is assumed to be increasing in n and $U_2(q,n)$ decreasing in n. This for two reasons. First, users experience positive direct network externalities on the user side of the platform, meaning that users' benefit from a platform is increasing in the number of users of the platform. This is characteristic of WTA competition. No further assumption is made as to whether the rate of change is increasing, decreasing, or constant. Second, owing to indirect externalities, the number of complementors on the other side of the platform is influenced by and influences n.

An important assumption is that, in addition to direct and indirect network effects, the reservation utility component of $U_i(\cdot,n)$, $U_i(n)$, captures all net benefits associated with platform i other than its security/vulnerability. This includes user-side platform differentiation such as direct network effects, pricing, ease of use, and compatibility; and complementor-side differentiation such as indirect network effects, the number of complementors, number and variety of applications offered, and degree of competition among complementors. Lee (2014) makes a similar aggregating assumption for the payoffs of complementors in order to focus on how contracting between the platform and complementors can lead to platform coexistence. He does not, however, address the user side of the market or the security decision undertaken by platforms. Instead, his is a model of multilateral contracting between the platform and complementors. In the present analysis, no bargaining or contracting takes place between the platform and users, as is explained in the literature review. The aggregate nature of $U_i(n)$ facilitates a focus on security via the analysis of $U_1(p,n)$ and $U_2(q,n)$. An additional assumption is that $U_1(0)=U_2(N)=0$.

Malware negatively affects the utility of users. In particular, if a successful malware attack occurs owing to vulnerabilities in the platform, then – from the users' perspective – the platform is part of the problem. As such, users receive diminished utility from the platform and its associated

network externalities. This diminished utility from platform 1 is given by $\hat{U}_1(n)$ where $0 \le \hat{U}_1(n) \le U_1(n)$, with the second inequality being strict for $n \neq 0$. To wit, if platform 1 suffers a successful malware attack, a user's associated loss is $U_1(n) - \hat{U}_1(n)$. Similarly, the diminished utility from a successful malware attack on platform 2 is $\hat{U}_2(n)$ where $0 \le \hat{U}_2(n) < U_2(n)$, with the second inequality being strict for $n \neq N$. A user's loss associated with a successful malware attack on platform 2 is $U_2(n) - \hat{U}_2(n)$.

In this way, the effect of platform security is two-fold. First, security acts as the gatekeeper for user access to everything else that differentiates the platform in that it determines the expected value of using the platform based on $p(n)$ or $q(n)$. Second, security is not merely another dimension of product differentiation. Insecurity determines the degree to which all other dimensions of platform differentiation are degraded under a breach via $\hat{U}_i(n)$. That is, insecurity is an argument within the expected value. To see this, the expected payoffs for using a platform are

$$U_1(p,n) = p(n)U_1(n) + (1 - p(n))\hat{U}_1(n), \text{ and}$$

$$U_2(q,n) = q(n)U_2(n) + (1 - q(n))\hat{U}_2(n).$$

No participation constraints are needed for users because, by definition, $U_i(n) \ge \hat{U}_i(n) \ge 0,\ i = 1,2.$ Finally, it is also assumed that platform 1 breaks all ties. That is, if $U_1(p,n) = U_2(q,n)$, then users select platform 1.

In specifying a platform's cost structure of security it is helpful to distinguish between the case where the units of measurement are per user values versus the case of providing a level security across a platform's user base. Specifically, the marginal cost of producing security for an additional user is negligible, which is as well consistent with WTA competition. For example, in the case of software the marginal cost of producing an additional unit for an additional user is effectively zero. Nevertheless, increasing the level of security for the user base comes at a constant marginal cost, $c_1, c_2 > 0$, for each respective platform. The term $c_1 p(n)$ is platform 1's total cost for providing level of security $p(n)$ across 1's user base, and $c_2 q(n)$ is platform 2's total cost of security level $q(n)$ for 2's user base. Consequently, there is a marginal (incremental) cost for increasing platform1's level of security from $\tilde{p}(n)$ to $p(n)$, where $p(n) > \tilde{p}(n)$. A similar

argument holds for platform 2 and $q(n)$. Once again, c_i is not the marginal cost of security for an additional user of platform *i*. It is the marginal cost of increasing security for all users of the associated platform. If interpreted instead on a marginal cost per user basis, $c_1 p(n)$ and $c_2 q(n)$ are each platform's respective fixed costs. This is again consistent with WTO competition.

As is standard in platform economics, each platform has a component in its payoff, specified here as $\Pi_1(n)$ and $\Pi_2(n)$, that is a function of its number of users. Similar to the specification of $U_i(n)$ for users, $\Pi_i(n)$ captures all non-security aspects of platform *i*'s payoff, including the number of participants, pricing, and profits the platform earns on the complementor side of the market. The platform's profits are also a function of its security, the cost structure of which is discussed above. In addition, $p(n), q(n) \in [0,1)$. That is, no platform is perfectly secure, $p(N), q(0) \neq 1$, and a platform has no incentive to invest in security if it has no users, $p(0), q(N) = 0$. It follows that each platform's payoff is

$$\Pi_1(p,n) = \Pi_1(n) - c_1 p(n), \text{ and}$$

$$\Pi_2(p,n) = \Pi_2(n) - c_2 q(n)$$

Without security, $p(n) = q(n) = 0 \; \forall n \in \mathbf{N}$, and the outcome of platform competition is a monopoly. Specifically, platform 1 will be the monopoly if $U_1(0,N) \geq U_2(0,0)$, and platform 2 will be the monopoly if $U_1(0,0) < U_2(0,N)$. This is in keeping with the literature on monopoly provision of a minimal level of security within a WTA environment. What remains to be determined is whether or not differences in security among platforms can sustain multi-platform competition rather than monopoly. This is the subject of the next section.

4. Cybersecurity and Platform Competition

Given the properties of users and platforms established above, this section describes and derives the conditions on platform security such that the platform structure is *interior* in *n*. By 'interior' it is meant that the two-sided platform is bifurcated (duopolistic). This is the simplest example of a multi-platform two-sided market, also known as *market-splitting* or *platform coexistence*. In particular, an interior solution should have the following three properties. First, in order that platform competition does not degenerate into a winner-take-all contest, it must be the case that

platform 1 users do not want to switch to platform 2 and vice-versa. Second, no platform will find it profitable to add any users from the present pool of potential users, *N*.[5] Finally, a platform must make a profit (or at least break even) given its number of users. The effect of each of these properties on the provision of security for a platform's user base, $p(n)$ and $q(n)$, is now considered in turn.

In an interior solution, each platform sets its level of security such that no user will switch to the other platform. That is, platform *i* must satisfy a *no-switching constraint*, NS_i, $\forall i \in \{1,2\}$. For the number of users of platform 1 to be interior, $n \in (0, N)$, this constraint specifies that it must be the case that the expected payoff for using platform 1 is at least that for switching to platform 2: $U_1(p,n) \geq U_2(q,n-1)$. [If a user of platform 1 switches to platform 2, there are $n-1$ remaining users of platform 1.] This implies

(NS_1) $\quad p(n)U_1(n) + (1-p(n))\hat{U}_1(n) \geq q(n-1)U_2(n-1) + (1-q(n-1))\hat{U}_2(n-1).$

It is useful to simplify this expression and solve for $q(n-1)$:

$$(1) \qquad p(n)\frac{U_1(n)-\hat{U}_1(n)}{U_2(n-1)-\hat{U}_2(n-1)} + \frac{\hat{U}_1(n)-\hat{U}_2(n-1)}{U_2(n-1)-\hat{U}_2(n-1)} \geq q(n-1).$$

Similarly, if there are currently n users of platform 1 and a platform 2 user switches to platform 1, then there are $n+1$ users of platform 1. Consequently, the no-switching condition for platform 2, $U_2(q,n) \geq U_1(p,n+1)$, is

(NS_2) $\quad q(n)U_2(n) + (1-q(n))\hat{U}_2(n) \geq p(n+1)U_1(n+1) + (1-p(n+1))\hat{U}_1(n+1),$

yielding

$$(2) \qquad q(n)\frac{U_2(n)-\hat{U}_2(n)}{U_1(n+1)-\hat{U}_1(n+1)} + \frac{\hat{U}_2(n)-\hat{U}_1(n+1)}{U_1(n+1)-\hat{U}_1(n+1)} \geq p(n+1).$$

Together, (NS_1) and (NS_2) establish the conditions under which platform 1 does not want to change $p(n)$ because its users will not switch to platform 2 and platform 2 will not want to change $q(n)$ because its users will not switch to platform 1.

In addition, it must be the case that under $p(n)$ profits will not increase if platform 1

[5] The model is static in the sense that the set of users, **N**, is fixed. An interesting question is to examine the effect of an expanding **N**.

changes its level of security in order to attract an additional user, and under $q(n)$ platform 2 cannot increase its profits by changing its level of security so as to attract an additional user. That is, for *n* to be interior it must also be the case that each platform's level of security is *incentive compatible*. For platform 1 this implies

(3) $\Pi_1(n) - c_1 p(n) \geq \Pi_1(n+1) - c_1 p(n+1).$

Substituting in the value of $p(n+1)$ from (2) and solving for $p(n)$ derives platform 1's incentive-compatible level of security:

(IC1) $$p(n) = q(n) \cdot \frac{U_2(n) - \hat{U}_2(n)}{U_1(n+1) - \hat{U}_1(n+1)} + \frac{\hat{U}_1(n+1) - \hat{U}_2(n)}{U_1(n+1) - \hat{U}_1(n+1)} - \frac{\Pi_1(n+1) - \Pi_1(n)}{c_1}$$

Similarly, platform 2's incentive compatibility constraint is

(4) $\Pi_2(n) - c_2 q(n) \geq \Pi_2(n-1) - c_2 q(n-1).$

Substituting in the value of $q(n-1)$ from (1) and solving for $q(n)$:

(IC2) $$q(n) = p(n) \cdot \frac{U_1(n) - \hat{U}_1(n)}{U_2(n-1) - \hat{U}_2(n-1)} + \frac{\hat{U}_2(n-1) - \hat{U}_1(n)}{U_2(n-1) - \hat{U}_2(n-1)} - \frac{\Pi_2(n-1) - \Pi_2(n)}{c_2}$$

Finally, each platform must not be making a loss. That is, each will participate in the two-sided market. This is expressed through the following *participation constraints*:

(PC1) $\Pi_1(n) - c_1 p(n) \geq 0,$

(PC2) $\Pi_2(n) - c_2 q(n) \geq 0.$

RESULT: When $p(n)$ and $q(n)$ jointly satisfy (IC1), (IC2), (PC1), and (PC2), then platform competition is interior in *n*; i.e. multiple platforms or market-splitting occurs.

This result is novel for several reasons. It shows that platform markets can be interior based on differences in cybersecurity. That is, a symbiotic relationship exits where *cybersecurity shapes platform competition and platform competition shapes cybersecurity*. Additionally, from the perspective of the analysis of two-sided markets, it is shown that an interior solution can stem from properties of the user (consumer) side of the market, whereas previous analyses of coexistence have been primarily centered on the complementor side of the market (e.g. locking in apps via exclusivity agreements). Finally, the conditions on $p(n)$ and $q(n)$ are expressed in terms of the

primitives of the model, namely, user preferences/utility and platform profits and costs. The economic meanings of this characterization are addressed in the following section, particularly with respect to the WTA condition on switching costs.

5. Characterization

Platform competition shapes cybersecurity in ways that can be characterized. To illustrate this, conditions ($IC_{1'}$) and ($IC_{2'}$) below are restatements of conditions (IC_1) and (IC_1), where the attributes of security levels $p(n)$ and $q(n)$ are identified and expressed in terms of the economics of platform competition and security.

$$(IC_{1'})\ p(n) = q(n)\cdot \overbrace{\frac{U_2(n)-\hat{U}_2(n)}{U_1(n+1)-\hat{U}_1(n+1)}}^{\text{Malware loss ratio for switching from platform 2 to 1.}} + \overbrace{\frac{\hat{U}_1(n+1)-\hat{U}_2(n)}{U_1(n+1)-\hat{U}_1(n+1)}}^{\text{Malware impact of switching from platform 2 to 1.}} - \overbrace{\frac{\Pi_1(n+1)-\Pi_1(n)}{c_1}}^{\text{Platform 1's opportunity cost of forgoing an additional user.}}$$

$$(IC_{2'})\ q(n) = p(n)\cdot \overbrace{\frac{U_1(n-1)-\hat{U}_1(n-1)}{U_2(n-1)-\hat{U}_2(n-1)}}^{\text{Malware loss ratio for switching from platform 1 to 2.}} + \overbrace{\frac{\hat{U}_2(n-1)-\hat{U}_1(n)}{U_2(n-1)-\hat{U}_2(n-1)}}^{\text{Malware impact of switching from platform 1 to 2.}} - \overbrace{\frac{\Pi_2(n-1)-\Pi_2(n)}{c_2}}^{\text{Platform 2's opportunity cost of forgoing an additional user.}}$$

To begin, with reference to the first right-hand term in each equation, $p(n)$ and $q(n)$ are increasing functions of the other platform's security, $q(n)$ and $p(n)$, respectively. This is consistent with the security 'arm's race' to maintain market share found in Arce (2018). Consequently, $q(n)$ and $p(n)$ are strategic complements.[6]

The magnitudes of these security values also determine how likely it is that a platform's participation constraint is satisfied. As $p(n)$ enters negatively into (PC_1) and $q(n)$ enters negatively into (PC_2), the larger $p(n)$ and/or $q(n)$ are, the less likely it is that the associated participation constraint is met, *ceteris paribus*, and therefore the conditions for an interior market structure are violated. From this perspective, the complementarity between $p(n)$ and $q(n)$ raises concerns about

[6] See Eaton and Eswaran (2002) for a characterization of strategies that are pure complements (substitutes) versus strategic complements (substitutes).

the upper bounds on platform security that must be respected in order for the outcome to be interior. From the participation constraints, these upper bounds are given by each platform's profit/average cost ratio, i.e. $p(n) \leq \Pi_1(n)/c_1$ and $q(n) \leq \Pi_2(n)/c_2$.

A WTA outcome is often associated with (i) direct network effects, (ii) high fixed costs and low per user variable cost, and (iii) high switching costs. As laid out in Section 3, the primitives for the users and platforms satisfy properties (i) and (ii). Hence, platform coexistence depends on the relationship between security and switching costs. In what follows, the Result is interpreted in terms of platform 1, understanding that equivalent properties and discussion hold for platform 2.

For users, switching costs are measured in terms of the ratio of marginal utilities (also known as the marginal rate of substitution) between platforms where the unit of change corresponds to the effect of malware on the sustainability and resilience of each platform. The first right-hand term ($IC_{1'}$) is the marginal rate of substitution of a user in platform 2 that is considering a switch to platform 1 *net* of the effect of malware in each platform. According, it can also be thought of as the loss ratio for being in platform 2 versus switching to platform 1. Intuitively, the greater this ratio is, the less likely it is that users will remain in platform 2 or the more likely it is that users will switch to platform 1. From ($IC_{1'}$), an increase in this ratio increases $p(n)$, thereby making it less likely that (PC_1) is met and an interior outcome occurs.

In addition, the effect of the loss ratio for switching is augmented by the relative malware impact of switching, $\hat{U}_2(n) - \hat{U}_1(n+1)$, as given by the second term on the right-hand side of ($IC_{1'}$). Under a successful malware attack, users of platform 2 experience diminished utility $\hat{U}_2(n)$. A user that switches to platform 1 instead experiences $\hat{U}_1(n+1)$ under a successful attack. That is, the status of a platform subsequent to an attack is part of users' calculus of platform selection. Some platforms suffer attacks better than others or face less consequential attacks (Lindorfer et al. 2013). If $\hat{U}_2(n) - \hat{U}_1(n+1) > 0$, platform 1 is preferred under this criterion as well.[7] Once again, from ($IC_{1'}$) this preference for platform 1 increases $p(n)$, thereby making it less likely that (PC_1) is met and an interior outcome occurs.

As an application, suppose that platform 1 is Microsoft or Google. These platforms create significant direct externalities, which is why they are popular. At the same time, a vulnerability in

[7] Note that no assumption has been made as to the relative magnitudes of $U_1(n+1)$ versus $U_2(n)$.

the platform implies a vulnerability for all users of the platform, consequently, the potential for a class break exists under an exploit. This means that the denominator in the first two right-hand terms of ($IC_{1'}$) is large because it represents a negative network externality, thereby reducing $p(n)$ owing to the consistently higher risk and consequence of an attack. A lower value of $p(n)$ makes it more likely that the platform's participation constraint holds. Hence, the potentiality for a class break increases the scope for an interior solution. Applying this logic to ($IC_{2'}$) means that platform 1's less popular rival must compete by increasing its security, $q(n)$. [This is different that requiring that $q(n) > p(n)$]. But the rival's ability to compete on security is bounded by its participation constraint, implying $q(n) \le \Pi_2(n)/c_2$. Should this constraint be violated, then platform 1 will become a monopoly. As an example, given that Apple OS and Linux exist alongside Windows, they need to compete with Windows on the basis of security. However, there is a limit to the degree that they can do so and remain profitable. Consequently, given Linux's nonprofit status, it has greater latitude to compete on security than does Apple OS.

Finally, security is decreasing in the opportunity cost of forgoing an additional user, $\Pi_1(n+1) - \Pi_1(n)$. If $\Pi_1(n+1) - \Pi_1(n)$ is positive, it is the tradeoff of forgoing the initiation of winner-take-all competition. Hence, if $\Pi_1(n+1) - \Pi_1(n)$ is positive, $p(n)$ can take a lower value, meaning that it is more likely that (PC_1) holds and the conditions for an interior solution are met.

6. Conclusion

The premise investigated here is that platform security reflects the rigors of platform competition. Platform security is defined in terms of the probability that a malware attack is unsuccessful. For example, it is well-established that, as monopolies have no competition, they provide minimal security. By extension, if the market shares of platforms are interior, rather than a platform being monopolistic, then security must be consistent with requirements for an interior market structure. This requires security to satisfy no-switching constraints for users and incentive compatibility constraints for the profitability of platform providers.

The resulting characterization shows that a platform's security is an increasing function of the ratio of users' malware-induced losses for their current platform over their potential losses for the alternative platform. That is, the switching costs that determine whether platform competition is

monopolistic or duopolistic are measured in terms of the relative loss ratios for the platforms. For example, the increased vulnerabilities associated with class breaks that capitalize on the substantial direct network externalities present in Windows or Google imply that their rivals need to compete on the basis of security. This means increasing the likelihood that a malware attack is unsuccessful and decreasing the impact of a successful breach. It also implies that a high degree of adoption can work against platform monopoly owing for the potential for a class break.

No relationship between platform security and platform pricing has been investigated. This is intentional, as the characteristics of security have been shown to be a function of users' preferences/utility, which here are quite general in recognition that other attributes, such as (in)direct externalities, are also reflected in a platform's security strategy. Given the cost structure assumed here, it would be simple enough to back out the platform's price from their marginal profits for an additional user. However, this is not the only component of a platform's incentive compatibility constraint that is a function of platform price(s). For example, a user's direct externality from a platform takes a functional form that is proportional to the number of users of the platform, n, under Moore's law, or is proportional to $\log(n)$ for Odlyzko and Tilly's (2005) alternative to Moore's law. At the same time, one must recognize that the number of users of a platform is not simply an integer, but a function whose value is determined by competing platforms' pricing strategies on both sides of the market. This is the intertwined nature of two-sided markets.

This complexity suggests that simulation may be a fruitful tactic for analyzing the interrelation between platform security, pricing, and/or any other platform attribute. For example, Sun and Tse (2007) present a simulation of the evolution of platform coexistence that is primarily focused on the interaction between pricing policies and the degree of multi-homing on either side of a platform's market. It would also be interesting to endogenize the actions of malware creators within the present model.

References

Anderson, Ross 2001. Why Information Security is Hard – An Economic Perspective. *Proceedings of the Seventeenth Annual Computer Security Applications Conference*, IEEE, 358-365.

Arce, Daniel 2018. Malware and Market Share. *Journal of Cybersecurity* 4(1) 1-6.

Cusumano, Michael 2010. Technology Strategy and Management. Cloud Computing and SaaS as New Computing Platforms. *Communications of the ACM* 53(4) 27-29.

Eaton, B. Curtis and Mukesh Eswaran 2002. Noncooperative Equilibria in 1-Shot Games: A Synthesis. In B. Curtis Eaton *Applied Microeconomic Theory*. Northampton, MA: Edward Elgar, pp. 118-149.

Evans, David S. and Richard Schmalensee 2016. *Matchmakers*. Boston: Harvard Business Review Press.

Garcia, Alfredo, Yue Sun, and Joseph Shen 2014. Dynamic Platform Competition with Malicious Users. *Dynamic Games and Applications* 4(3) 290-308.

Gawer, Annabelle 2014. Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework. *Research Policy* 43(7) 1239-1249.

Gawer, Annabelle and Michael A. Cusumano 2002. *Platform Leadership. How Intel. Microsoft, and Cisco Drive Industry Innovation*. Boston: Harvard Business School.

Jha, S., O. Sheyner, and J. Wing (2002). Two Formal Analyses of Attack Graphs. *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, IEE Computer Society.

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

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl 2015. Advanced Social Engineering Attacks. *Journal of Information Security and Attacks* 22: 113-122.

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

Lelarge, Marc 2009. Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives. *47th Allerton House Conference on Communication, Control, and Computing*. University of Illinois at Urbana Champaign: Allerton House, pp.1353-1360.

Liao Chun-Hsiung, and Chun-Wei Chen 2014. Network Externality and Incentive to Invest in Network Security. *Economic Modeling* 36: 398-404.

Lindorfer, Martina, Bernhard Miller, Matthias Neugschwandtner, and Christian Platzer 2013. Take

a Bite – Finding the Worm in the Apple. *Proceedings of the 9th International Conference on Information, Communications & Signals Processing*. IEEE: Tainan, Taiwan.

Littlewood, Bev, Sarah Brocklehurst, Norman Fenton *et al*. 1993. Towards Operational Measures of Computer Security. *Journal of Computer Security* 2(3) 211-229.

McAfee, Andrew and Erik Brynjolfsson 2017. *Machine, Platform, Crowd*. NY: Norton.

Miller, Charlie 2011. Mobil Attacks and Defense. *IEEE Security & Privacy* 9(4) 68-70.

Odlyzko, Andrew and Benjamin Tilly 2005. *A Refutation of Metcalfe's Law and a Better Estimate for the Value of Networks and Network Interconnections*. University of Minnesota: Digital Technology Center.

Parker, Geoffrey G. and Marshall W. Van Alstyne 2005. Two-Sided Network Effects: A Theory of Information Product Design. *Management Science* 51(10) 1494-1504.

Parker, Geoffrey G., Marshall W. Van Altstyne, and Sangeet Paul Choudary 2016. *Platform Revolution*. NY: Norton.

Ramos, Alex, Marcela Lazar, Raimir Holdanda Filho et al. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys & Tutorials* 19(4) 2704-2734.

Rochet, Jean-Charles and Jean Tirole 2003. Platform Competition in Two-Sided Markets. *Journal of the European Economic Association* 1(4) 990-1029.

Schneier, Bruce 2000. *Secrets and Lies*: *Digital Security in a Networked World*. Indianapolis: Wiley.

Sallhammer, Karin, Bjarne E. Helvik, and Svein J. Knapskog (2006a). On Stochastic Modeling for Integrated Security and Dependability Evaluation. *Journal of Networks* 1(5) 31-42.

Sallhammer, Karin, Bjarne E. Helvik, and Svein J. Knapskog (2006b). Towards a Stochastic Model for Integrated Security and Dependability Evaluation. *Proceedings of the First International Conference on Availability, Reliability and Security*, IEEE Computer Society.

Sen, Soumya, Roch Guerin, and Kartik Hosaganar 2011. Functionally-Rich versus Minimalist Platforms: A Two-Sided Market Analysis. *ACM SIGCOMM Computer Communication Review*, 41(5) 36-43.

Sun, Mingchun and Edison Tse 2007. When Does the Winner Take All in Two-Sided Markets? *Review of Network Economics* 6(1) 16-40.

Vaugh, Rayford B., Rhonda Henning, and Ambareen Siraj (2002). Information Assurance

Measures and Metrics – State of Practice and Proposed Taxonomy. In the *Proceedings of the 36th Hawaii International Conference on System Sciences*, IEE Computer Society.